

Linguaggi

18: Semantica della logica del prim'ordine

Claudio Sacerdoti Coen

`<sacerdot@cs.unibo.it>`

Università di Bologna

09/12/2019

Semantica classica della logica del prim'ordine

Al fine di definire la semantica classica di un linguaggio del prim'ordine è necessario prima individuare la forma appropriata per le descrizioni dei mondi.

La semantica classica associa:

- A ogni connotazione proposizionale un valore di verità $\in \{0, 1\}$
- A ogni connotazione che è un termine un **elemento del dominio delle denotazioni per i termini**

Inoltre, come nel caso proposizionale, un mondo **deve fissare esclusivamente la semantica delle “formule atomiche”** (costanti, funzioni, predicati) che verrà **estesa** a ogni formula possibile assegnando una semantica invariabile ai connettivi e ai quantificatori.

Semantica classica della logica del prim'ordine

Definizione: un **mondo o interpretazione** per la logica del prim'ordine è una coppia (A, I) dove A è un insieme **non vuoto** di denotazioni per i termini e I è una **funzione di interpretazione** che associa

- a ogni funzione f^n una funzione il cui dominio è $A^n = A \times \dots \times A$ (n volte) e il cui codominio è A
- Caso particolare: per ogni costante c , $I(c) \in A$
- a ogni predicato P^n una funzione il cui dominio è A^n e il cui codominio è $\{0, 1\}$ o, equivalentemente, un sottoinsieme di A^n
- Caso particolare: per ogni predicato 0-ario P , $I(P) \in \{0, 1\}$ come nel caso della logica proposizionale

Nota: un mondo non è più rappresentabile come una sequenza di booleani e non è più possibile usare tabelle di verità.

Semantica classica della logica del prim'ordine

Siamo già in grado di interpretare in un mondo (A, I) termini e proposizioni in cui non occorrono variabili. (La definizione formale verrà data in seguito).

Esempio:

Sia $A = \mathbb{N}$,

$I(D)$ l'insieme dei numeri pari,

$I(f^1)(n) = n + 1$

$I(c) = 2$.

Allora $\llbracket D(f(c)) \rrbracket^{(A,I)} = 0$.

Ma che semantica diamo a $\forall x.P$ e a $\exists x.P$?

Intuitivamente, $\forall x.P$ è vera quando P è sempre vera **al variare di x** mentre $\exists x.P$ è vera quando P è vera almeno una volta **al variare di x** . La variazione è implicita essere sul dominio A del nostro mondo.

Come catturare la nozione di variazione di x sul dominio A ?

Vediamo prima un paio di modi non corretti:

❶ $\llbracket \forall x.P \rrbracket^{(A,I)} = \min\{\llbracket P[\alpha/x] \rrbracket^{(A,I)} \mid \alpha \in A\}$

Errata in quanto α è una denotazione e non una connotazione! Pertanto $P[\alpha/x]$ non è ammesso dalla sintassi.

❷ $\llbracket \forall x.P \rrbracket^{(A,I)} = \min\{\llbracket P[t/x] \rrbracket^{(A,I)} \mid t \in \text{Term}\}$ dove Ter è l'insieme di tutte le connotazioni per termini nel nostro linguaggio.

Errata in quanto il mio mondo potrebbe avere molte più denotazioni per termini di quelle rappresentabili sintatticamente tramite connotazioni. Esempio: $A = \mathbb{R}$ poichè l'insieme delle connotazioni è sempre enumerabile.

Come catturare la nozione di variazione di x sul dominio A ?

Definizione: dato un mondo (A, I) un **ambiente** ξ è una funzione il cui dominio è l'insieme di tutte le variabili e il cui codominio è A .

Useremo gli ambienti per interpretare le variabili nello stesso modo in cui usiamo I per interpretare le costanti.

Esempio: $\llbracket f^2(c, x) \rrbracket^{(A, I), \xi} = I(f^2)(I(c), \xi(x))$

I **quantificatori universale ed esistenziale** fanno variare gli **ambienti** per assegnare a una variabile x tutti i possibili valori di A .

Semantica classica della logica del prim'ordine

Definizione di **semantica classica della logica del prim'ordine**.

Sia (A, I) un mondo e ξ un ambiente sul mondo. Definiamo per induzione strutturale

$$\llbracket x \rrbracket^{(A, I), \xi} = \xi(x)$$

$$\llbracket f^n(t_1, \dots, t^n) \rrbracket^{(A, I), \xi} = I(f^n)(\llbracket t_1 \rrbracket^{(A, I), \xi}, \dots, \llbracket t^n \rrbracket^{(A, I), \xi})$$

$$\llbracket P^n(t_1, \dots, t^n) \rrbracket^{(A, I), \xi} = I(P^n)(\llbracket t_1 \rrbracket^{(A, I), \xi}, \dots, \llbracket t^n \rrbracket^{(A, I), \xi})$$

$$\llbracket \perp \rrbracket^{(A, I), \xi} = 0$$

$$\llbracket \top \rrbracket^{(A, I), \xi} = 1$$

$$\llbracket \neg P \rrbracket^{(A, I), \xi} = 1 - \llbracket P \rrbracket^{(A, I), \xi}$$

$$\llbracket P_1 \wedge P_2 \rrbracket^{(A, I), \xi} = \min\{\llbracket P_1 \rrbracket^{(A, I), \xi}, \llbracket P_2 \rrbracket^{(A, I), \xi}\}$$

$$\llbracket P_1 \vee P_2 \rrbracket^{(A, I), \xi} = \max\{\llbracket P_1 \rrbracket^{(A, I), \xi}, \llbracket P_2 \rrbracket^{(A, I), \xi}\}$$

$$\llbracket P_1 \Rightarrow P_2 \rrbracket^{(A, I), \xi} = \max\{1 - \llbracket P_1 \rrbracket^{(A, I), \xi}, \llbracket P_2 \rrbracket^{(A, I), \xi}\}$$

$$\llbracket \forall x. P \rrbracket^{(A, I), \xi} = \min\{\llbracket P \rrbracket^{(A, I), \xi[x \mapsto \alpha]} \mid \alpha \in A\}$$

$$\llbracket \exists x. P \rrbracket^{(A, I), \xi} = \max\{\llbracket P \rrbracket^{(A, I), \xi[x \mapsto \alpha]} \mid \alpha \in A\}$$

dove $\xi[x \mapsto \alpha]$ associa α a x e $\xi(y)$ a y .

Tutte le definizioni viste per la logica proposizionale classica che facevano riferimento alle nozioni di mondo e semantica rimangono identiche per la logica del prim'ordine classica con le nuove definizioni di mondo (e ambiente) e semantica.

Esempio: $\Gamma \Vdash G$ quando in ogni mondo (A, I) e ambiente ξ si ha che se $\llbracket F \rrbracket^{(A, I), \xi} = 1$ per ogni $F \in \Gamma$ allora $\llbracket G \rrbracket^{(A, I), \xi} = 1$.

Semantica intuizionista della logica del prim'ordine

Accenniamo qui alla proprietà più importante della semantica intuizionista della logica del prim'ordine:

se

$$\Vdash \forall x. \exists y. P(x, y)$$

allora

$$\vdash \forall x. \exists y. P(x, y)$$

(per il teorema di completezza debole)

e inoltre **vi è (e sappiamo qual'è) un algoritmo f che ad ogni input x associa un output $f(x)$ tale che $P(x, f(x))$**

$P(x, y)$ viene chiamata la **specifica** dell'algoritmo

Semantica intuizionista della logica del prim'ordine

Esempio di specifica per un algoritmo di ordinamento:

$\forall l. \exists l'$.

$(Lista(l) \Rightarrow \exists l'. (Lista(l') \wedge Ordinata(l') \wedge \forall z. (z \in l \iff z \in l'))))$

Da ogni prova intuizionista del precedente enunciato si ricava una funzione che data una lista l restituisce una lista l' assieme a una prova che mostra che l e l' hanno gli stessi elementi e che l' è ordinata.

Una dimostrazione intuizionista corrisponde a dare contemporaneamente un'implementazione e la dimostrazione di correttezza dell'implementazione stessa!

Rimandiamo al corso di Fondamenti Logici dell'Informatica lo studio di questo approccio alla programmazione.

Equivalenze logiche notevoli (caso proposizionale, 1/2)

Commutatività':

$$A \vee B \equiv B \vee A, \quad A \wedge B \equiv B \wedge A$$

Associatività':

$$A \vee (B \vee C) \equiv (A \vee B) \vee C, \quad A \wedge (B \wedge C) \equiv (A \wedge B) \wedge C$$

Idempotenza:

$$A \vee A \equiv A, \quad A \wedge A \equiv A$$

Distributività:

$$A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C), \quad A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$$

Assorbimento:

$$A \vee (A \wedge B) \equiv A, \quad A \wedge (A \vee B) \equiv A$$

Elemento neutro:

$$A \vee \perp \equiv A, \quad A \wedge \top \equiv A$$

Annichilamento:

$$A \vee \top \equiv \top, \quad A \wedge \perp \equiv \perp$$

Equivalenze logiche notevoli (caso proposizionale 2/2)

Doppia negazione:

$$\neg\neg A \equiv A$$

De Morgan:

$$\neg(A \vee B) \equiv \neg A \wedge \neg B, \quad \neg(A \wedge B) \equiv \neg A \vee \neg B, \quad \neg A \vee \neg B \equiv \neg(A \wedge B)$$

Nota: quelle in rosso valgono solo in logica classica, quelle in nero anche in logica intuizionista

Teorema (completezza): siano P e Q due formule della logica proposizionale. $P \equiv Q$ (usando la definizione di equivalenza logica in logica classica) sse posso dimostrare $P \equiv Q$ usando solamente le equivalenze notevoli classiche appena elencate. Dimostrazione: interessante, ma lunga e complessa.

Equivalenze logiche notevoli

Quantificatori dello stesso tipo commutano:

$$\forall x.\forall y.P \equiv \forall y.\forall x.P$$

$$\exists x.\exists y.P \equiv \exists y.\exists x.P$$

Quantificatori di tipo diverso **NON** commutano:

$$\exists x.\forall y.P \not\equiv \forall y.\exists x.P$$

$$\forall x.\exists y.P \not\equiv \exists y.\forall x.P$$

Esempio: $\forall x.\exists y.x < y$ vs $\exists y.\forall x.x < y$ in \mathbb{N} .

Equivalenze logiche notevoli

Le seguenti equivalenze possono essere utilizzate per spostare i quantificatori in posizione di testa nelle formule:

$$\forall x.(P \wedge Q) \equiv (\forall x.P) \wedge (\forall x.Q) \quad (\text{usata da dx a sx})$$

$$\exists x.(P \vee Q) \equiv (\exists x.P) \vee (\exists x.Q) \quad (\text{usata da dx a sx})$$

$$\forall x.P \equiv P \text{ se } x \notin FV(P) \quad (\text{usata da dx a sx})$$

$$\exists x.P \equiv P \text{ se } x \notin FV(P) \quad (\text{usata da dx a sx})$$

$$\forall x.(P \vee Q) \equiv (\forall x.P) \vee Q \text{ se } x \notin FV(Q) \quad (\text{usata da dx a sx})$$

$$\exists x.(P \wedge Q) \equiv (\exists x.P) \wedge Q \text{ se } x \notin FV(Q) \quad (\text{usata da dx a sx})$$

Equivalenze logiche notevoli

Le leggi di De Morgan si estendono ai quantificatori universali ed esistenziali (pensati come congiunzioni/disgiunzioni infinite):

$\neg\forall x.P \equiv \exists x.\neg P$	solo in logica classica
$\exists x.\neg P \Vdash \neg\forall x.P$	in logica intuizionista
$\neg\exists x.P \equiv \forall x.\neg P$	in logica classica e intuizionista

Attenzione: per dimostrare che $\neg\forall x.P$ basta dimostrare che $\exists x.\neg P$ ovvero è sufficiente un controesempio. Ma per dimostrare $\neg\exists x.P$ dobbiamo dimostrare $\forall x.\neg P$ ovvero serve una dimostrazione.

Equivalenze logiche notevoli

Sia $x \notin FV(Q)$ (sempre vero per un qualche Q' che sia α -convertibile con Q). Si ha

$$(\forall x.P) \Rightarrow Q \equiv \exists x.(P \Rightarrow Q)$$

$$\exists x.(P \Rightarrow Q) \Vdash (\forall x.P) \Rightarrow Q$$

$$(\exists x.P) \Rightarrow Q \equiv \forall x.(P \Rightarrow Q)$$

$$Q \Rightarrow (\exists x.P) \equiv \exists x.(Q \Rightarrow P)$$

$$Q \Rightarrow (\forall x.P) \equiv \forall x.(Q \Rightarrow P)$$

solo in logica classica

in logica intuizionista

Quantificazioni limitate

Informalmente si usano sovente forme di quantificazioni limitate a un particolare dominio o proprietà:

$$\forall x \in A. P(x) \qquad \exists x \in A. P(x)$$

per ogni x t.c. $Q(x)$ si ha $P(x)$ esiste x t.c. $Q(x)$ per cui $P(x)$

che corrispondono alla versioni formali

$$\forall x. (x \in A \Rightarrow P(x)) \qquad \exists x. (x \in A \wedge P(x))$$

$$\forall x. (Q(x) \Rightarrow P(x)) \qquad \exists x. (Q(x) \wedge P(x))$$

Riflettete sul caso $\forall x \in \emptyset. P(x)$!

Quantificazioni limitate ed equivalenze logiche notevoli

Fare attenzione all'applicazione corretta delle leggi di De Morgan sulle quantificazioni limitate:

$$\begin{array}{ll} \neg \forall x \in A. P(x) & \neg \exists x \in A. P(x) \\ = \neg \forall x. (x \in A \Rightarrow P(x)) & = \neg \exists x. (x \in A \wedge P(x)) \\ \equiv \neg \forall x. (\neg x \in A \vee P(x)) & \equiv \forall x. \neg (x \in A \wedge P(x)) \\ \equiv \exists x. \neg (\neg x \in A \vee P(x)) & \equiv \forall x. (\neg x \in A \vee \neg P(x)) \\ \equiv \exists x. (x \in A \wedge \neg P(x)) & \equiv \forall x. (x \in A \Rightarrow \neg P(x)) \\ = \exists x \in A. \neg P(x) & = \forall x \in A. \neg P(x) \end{array}$$

Nota: mentre la seconda vale anche intuizionisticamente, la prima vale intuizionisticamente solo nella direzione

$\exists x \in A. \neg P(x) \Vdash \neg \forall x \in A. P(x)$, compresa la sua variante

$\exists x \in A. P(x) \Vdash \neg \forall x \in A. \neg P(x)$

Correttezza e completezza della deduzione naturale

Anche per la deduzione naturale (sia classica che intuizionista) valgono i teoremi di correttezza e completezza:

- **Correttezza:** per ogni Γ, F della logica del prim'ordine, se $\Gamma \vdash F$ allora $\Gamma \Vdash F$
- **Completezza (forte):** per ogni Γ, F della logica del prim'ordine, se $\Gamma \Vdash F$ allora $\Gamma \vdash F$

Per la logica classica vale anche un teorema di **completezza debole** dotato di contenuto computazionale che si basa su ipotesi più strette (**finitezza di Γ ed enumerabilità del linguaggio dei termini**).

Primo teorema di incompletezza di Goedel (1931)

Attenzione: il teorema di completezza ci dice solo che tutte le conseguenze logiche degli assiomi in Γ sono dimostrabili. Ovvero data una formula P , $\Gamma \vdash P$ sse P è vera in tutti i mondi (A, I) , ξ che soddisfano Γ e $\Gamma \vdash \neg P$ sse P è falsa in tutti i mondi (A, I) , ξ che soddisfano Γ .

Quando Γ impone un numero sufficiente di vincoli da essere soddisfatti da un solo mondo, allora in quel mondo ogni P è vera o falsa e quindi $\Gamma \vdash P$ oppure $\Gamma \vdash \neg P$.

Domanda: dato un mondo, è sempre possibile imporre degli assiomi Γ che siano soddisfatti solo da lui? **NO** (dimostrazione omessa)

Primo teorema di incompletezza di Goedel (1931)

Primo teorema di incompletezza di Goedel (1931)

In ogni teoria matematica Γ sufficientemente espressiva da contenere l'aritmetica, esiste una formula P tale che, se $\Gamma \not\vdash \perp$ allora $\Gamma \not\vdash P$ e $\Gamma \not\vdash \neg P$.

- il caso $\Gamma \vdash \perp$ non è interessante (la teoria è inconsistente, tutto è dimostrabile)
- con l'aritmetica Goedel programma, **codificando nei numeri naturali** la sintassi delle formule e la sintassi degli alberi di derivazione
- la dimostrazione (lunga e complessa) ricalca il **paradosso del mentitore**: P dice "io non sono dimostrabile" usando la codifica nei numeri per creare la confusione fra livello e metalivello
- la proposizione P non è interessante: ci sono proposizioni interessanti con la stessa proprietà?

Secondo teorema di incompletezza di Goedel

Secondo teorema di incompletezza di Goedel

Nessuna teoria Γ sufficientemente espressiva da contenere l'aritmetica e consistente (ovvero tale che $\Gamma \not\vdash \perp$) è in grado di dimostrare la sua consistenza.

- per dimostrare la prova si codifica l'intera prova del primo teorema di incompletezza di Goedel nei numeri naturali
- conseguenza: **per dimostrare la consistenza di una logica+teoria non possiamo che fidarci di una meta-logica+teoria** o, in alternativa, costruire una catena ascendente infinita di meta-meta-...-logica+teoria di cui ognuna dimostra la precedente