Logica predicativa, sintassi e semantica

Lezione 14 di Fondamenti di informatica

Docente: Giuseppe Scollo

Università di Catania
Facoltà di Scienze Matematiche, Fisiche e Naturali
Corso di Laurea in Informatica, I livello, AA 2009-10

Indice

definizioni ricorsive

una definizione, in un linguaggio, ha due costituenti:

definiendum: il termine da definire
definiens: l'espressione o frase che lo definisce

una definizione è **ricorsiva** quando il *definiendum* occorre nel *definiens*

per l'inerente circolarità, una definizione ricorsiva rischia di essere semanticamente viziosa: inutilizzabile al fine di stabilire il significato dei suoi costituenti; tuttavia ...

... si può impedire la formazione di circoli viziosi se il *definiendum* è un termine parametrico, con un parametro che assume valori in un insieme **"ben ordinato"**

N.B. il significato esatto di questa qualificazione è specificato più avanti

in tal caso, possiamo rendere **costruttiva**, anziché viziosa, la circolarità in una definizione ricorsiva assicurando che le occorrenze del *definiendum* nel *definiens* siano riferite a valori del parametro più piccoli di quello a cui è riferito il *definiendum* in quanto tale

una definizione ricorsiva siffatta è, a tutti gli effetti, una **definizione induttiva**

principio di induzione di Peano

il principio di induzione naturale, dovuto a **Giuseppe Peano** (1889), ha due distinte, sebbene correlate, manifestazioni:

nella **definizione** dei numeri naturali, come principio di **minimalità costruttiva**, evidente nella **terza clausola** appresso:

0 è un numero naturale
se **n** è un numero naturale, **n+1** è un nuovo numero naturale
non esistono altri numeri naturali

nelle **dimostrazioni** di proprietà sui numeri naturali:

se vale **P(0)**
e se vale l'implicazione **P(n) → P(n+1)**
allora **P(n)** vale per tutti i numeri naturali **n**

la minimalità costruttiva dei numeri naturali giustifica l'uso del principio di induzione naturale come regola di inferenza logica

definizione induttiva di termini

esempi di costruzioni induttive di largo impiego nella definizione di linguaggi formali, quali ad es. linguaggi logici, linguaggi di programmazione, etc., si hanno nelle definizioni degli **insiemi dei termini**, **formule** o **espressioni** del linguaggio

tali **universi sintattici** hanno definizione induttiva nei casi d'interesse pratico

ecco, ad esempio, la definizione induttiva dell'insieme dei termini generato da una **segnatura algebrica**, ovvero famiglia di **operatori**, cioè **simboli di operazione**, dove ogni operatore ha una **arietà**: il numero di argomenti dell'operazione che esso designa

quando l'arietà è 0, l'operatore è un **simbolo di costante**

per una data interpretazione degli operatori quali costanti e operazioni di un'algebra, un termine privo di variabili descrive il calcolo di un valore nell'algebra, a partire da costanti

l'insieme dei termini di complessità 0 è costituito dai simboli di costante
se ω è un operatore di arietà $k>0$, e $t_1, \ldots, t_k$ sono termini di complessità massima **n**, allora $\omega(t_1, \ldots, t_k)$ è un termine di complessità **n+1**

ogni termine ha una complessità, definita induttivamente dalle clausole precedenti

induzione strutturale

la costruzione induttiva dei termini ben si presta ad introdurre una tecnica di definizione e di dimostrazione molto utile nei linguaggi di programmazione: l'**induzione strutturale**

supponiamo di voler definire una nuova funzione, o dimostrare che una certa proprietà valga, per tutti i possibili valori assunti da una struttura dati:

per applicare l'induzione strutturale occorre che ogni valore sia rappresentabile da (almeno) un termine privo di variabili

in tali condizioni, l'induzione strutturale consiste nel

definire o dimostrare per le strutture più piccole, tipicamente le **costanti**
definire o dimostrare per le strutture generate dalle operazioni $C(t_1,\ldots,t_k)$, di costruzione del tipo di dati, **assumendo** di aver già definito o dimostrato per $t_1,\ldots,t_k$ **(ipotesi di induzione)**

il principio di induzione strutturale può essere facilmente dedotto dal principio di induzione naturale di Peano, giacché altro non è che induzione naturale sulla complessità dei termini che rappresentano i valori delle strutture dati in gioco; il seguente principio di induzione, al contrario, è una **generalizzazione propria** del principio di Peano

induzione noetheriana

un ordinamento stretto < su un insieme S è detto **ben fondato**, e si dice che S è **ben ordinato** da <, se non esistono catene discendenti infinite $a_0 > a_1 > \dots a_n > \dots$, cioè se ogni catena discendente termina

tecniche di dimostrazione della terminazione di un programma si basano sulla possibilità di poter ben ordinare l'insieme delle sue possibili computazioni

una proprietà P definita per gli elementi di S, strettamente ordinato da <, è detta **ereditaria** se vale l'implicazione: $(\forall y<x\ P(y)) \rightarrow P(x)$

il seguente principio di induzione è dovuto a Emmy Noether:

in un insieme ben ordinato ogni proprietà ereditaria vale in tutto l'insieme

l'ordinamento dei naturali è ben fondato, dal che discende una forma equivalente dell'induzione di Peano (la cui base deriva dalla validità vacua dell'implicazione di ereditarietà sui naturali quando x=0)

non si può invece ricondurre l'induzione noetheriana a quella di Peano: l'ordinamento dei naturali è totale, l'induzione noetheriana si applica a una più ampia classe di ordinamenti (ben fondati)

sintassi predicativa

costruzione di **formule predicative** (del I ordine), dati un insieme **V** di **variabili** e una segnatura algebrica (in senso lato) omogenea, o **segnatura del I ordine,** $\Sigma=(\Omega,\Pi)$:

Ω è una segnatura algebrica (in senso stretto) omogenea, come sopra definita

Π è una famiglia di **simboli relazionali**, dotati di **arietà**, detti anche:

predicati, se di arietà >0 (Π_k: insieme dei predicati di arietà k)

simboli proposizionali, se di arietà 0 (insieme Π_0)

l'insieme $T_\Sigma(V)$ dei **termini** su Σ e **V** è definito induttivamente come sopra, ma su una base più estesa, poiché anche le variabili sono termini di complessità 0

l'insieme delle **formule atomiche** su Σ e **V** è costituito dai simboli proposizionali in Π_0 e dalle espressioni $P(t_1,\dots,t_k)$ e $(t_1 = t_2)$, dove $P\in\Pi_k$ e $t_1,t_2,\dots,t_k\in T_\Sigma(V)$

l'insieme $F_\Sigma(V)$ delle **formule** su Σ e **V** è definito induttivamente come segue:

le **formule atomiche** su Σ e **V** sono in $F_\Sigma(V)$

se φ e ψ sono in $F_\Sigma(V)$, e $x\in V$, allora sono in $F_\Sigma(V)$ anche le formule $(\neg\varphi)$, $(\varphi\wedge\psi)$, $(\varphi\vee\psi)$, $(\varphi\rightarrow\psi)$, $(\varphi\leftrightarrow\psi)$, $(\forall x\varphi)$, $(\exists x\varphi)$

variabili in termini e formule

sia i **termini** sia le **formule** di una segnatura del I ordine sono rappresentabili come **alberi ordinati**, ai cui nodi sono associati simboli della segnatura, variabili e, per le formule, i connettivi logici e i quantificatori introdotti nella loro definizione induttiva

Def.: un albero è **ordinato** se è radicato e con un ordine totale dei figli di ciascun nodo interno

N.B. una segnatura del I ordine come definita sopra è detta **omogenea** perché dà una sintassi per algebre (in senso lato) omogenee; una segnatura **eterogenea**, o **multisortale** ha inoltre un insieme di **sorte** (nomi per gli insiemi sostegno), e più articolate arietà dei simboli, che ne specificano le sorte degli argomenti (e dei risultati di operazioni); in tal caso anche le variabili hanno sorta; per semplicità, ci limitiamo al caso omogeneo

le variabili di un termine sono quelle che vi occorrono (associate a foglie del suo albero); per le formule, vanno distinte le occorrenze **libere** di variabili da quelle **vincolate**

un'occorrenza di variabile è **vincolata** se cade nell'ambito di una sua quantificazione, altrimenti è **libera**; una variabile **occorre libera** in una formula se vi ha qualche occorrenza libera; l'insieme $Var(t)$ delle variabili di un termine t, e l'insieme $Free(\varphi)$ delle variabili libere di una formula φ sono induttivamente definiti, v. esercizio 8

un termine t è **liberamente sostituibile a x in $\varphi(x)$** se, sostituendo t in tutte le occorrenze libere di x in $\varphi(x)$, nessuna variabile di t in tali sostituzioni viene quantificata

N.B. la libera sostituibilità di un termine a una variabile in una formula è necessaria alla correttezza della sostituzione, v. ad es. la sostituzione del termine x alla variabile y in $\exists x \neg(x=y)$

semantica predicativa

definiamo innanzitutto la semantica degli **enunciati**, cioè formule prive di variabili libere

un enunciato di segnatura Σ trova significato in un **modello** che interpreta i simboli di Σ

una Σ-struttura algebrica M dota le sue operazioni e relazioni di una sintassi, alla quale dà significato con la sua **funzione di interpretazione:** $\_^M : \Sigma \to \Sigma^M$

l'interpretazione t^M dei **termini chiusi** $t \in \mathcal{T}_\Sigma$ è definita per induzione strutturale

qui conviene considerare una **segnatura estesa** $\Sigma(D)$, in cui gli elementi del sostegno D di M sono aggiunti come simboli di costante (e interpretati come se stessi nella $\Sigma(D)$-struttura M)

la semantica è data dalla **relazione di validità** $\models$ di Σ-enunciati in Σ-modelli: $M \models \varphi$

l'interpretazione di Π e $\mathcal{T}_{\Sigma(D)}$ in M dà la validità degli **enunciati atomici:**

$M \models Q$ sse $Q^M = 1 \quad (Q \in \Pi_0)$

$M \models P(t_1,\dots,t_k)$ sse $(t_1^M,\dots,t_k^M) \in P^M \quad (P \in \Pi_k,\ k > 0,\ t_1,\dots,t_k \in \mathcal{T}_{\Sigma(D)})$

$M \models t_1 = t_2$ sse $t_1^M = t_2^M \quad (t_1, t_2 \in \mathcal{T}_{\Sigma(D)})$

quella degli altri enunciati si definisce quindi per induzione strutturale (v. esercizio 9)

teorie predicative

Mod$_\Sigma$: la classe dei Σ-modelli ("classe di similarità")

Mod$_\Sigma(\varphi)$: la sottoclasse di **Mod**$_\Sigma$ caratterizzata dalla validità dell'enunciato φ

Mod$_\Sigma(\Psi)$: la sottoclasse di **Mod**$_\Sigma$ caratterizzata dalla validità di **tutti** gli enunciati dell'insieme Ψ in **ciascun modello** della classe

relazione di **conseguenza** semantica: $\Psi \models \varphi$ sse **Mod**$_\Sigma(\Psi) \subseteq$ **Mod**$_\Sigma(\varphi)$

> **N.B.** si adopera lo stesso simbolo che designa la relazione di validità, ma si tratta di una relazione **diversa** (fra insiemi di enunciati ed enunciati), sebbene semanticamente basata su quella di validità

Σ-**teoria predicativa:** un insieme di Σ-enunciati **chiuso per conseguenza**:

$$\Psi \models \varphi \;\Rightarrow\; \varphi \in \Psi$$

chiusura deduttiva di un insieme di Σ-enunciati Ψ: $Th(\Psi) = \{\varphi \mid \Psi \models \varphi\}$

Ψ è **soddisfacibile** se **Mod**$_\Sigma(\Psi)$ non è vuota, altrimenti è **insoddisfacibile:** $\Psi \models \bot$

principio di dimostrazione per assurdo: $\Psi \models \varphi \;\Leftrightarrow\; \Psi \cup \{\neg\varphi\} \models \bot$

φ è una **verità logica** o **tautologia** se **Mod**$_\Sigma(\varphi)$ = **Mod**$_\Sigma$ (in tal caso si scrive $\models \varphi$)

semantica predicativa Tarskiana

fissato un dominio $\mathcal{D}$, la semantica dei $\Sigma(\mathcal{D})$-enunciati $\varphi \in F_{\Sigma(\mathcal{D})}$ può essere specificata definendo $Mod_{\Sigma(\mathcal{D})}(\varphi)$ per induzione sulla struttura di φ, come segue:

$$Mod_{\Sigma(\mathcal{D})}(Q) = \{M \in Mod_{\Sigma(\mathcal{D})} \mid Q^M = 1\}$$
$$Mod_{\Sigma(\mathcal{D})}(P(t_1,\ldots,t_k)) = \{M \in Mod_{\Sigma(\mathcal{D})} \mid (t_1^M,\ldots,t_k^M) \in P^M\}$$
$$Mod_{\Sigma(\mathcal{D})}(t_1 = t_2) = \{M \in Mod_{\Sigma(\mathcal{D})} \mid t_1^M = t_2^M\}$$
$$Mod_{\Sigma(\mathcal{D})}(\varphi \wedge \psi) = Mod_{\Sigma(\mathcal{D})}(\varphi) \cap Mod_{\Sigma(\mathcal{D})}(\psi)$$
$$Mod_{\Sigma(\mathcal{D})}(\varphi \vee \psi) = Mod_{\Sigma(\mathcal{D})}(\varphi) \cup Mod_{\Sigma(\mathcal{D})}(\psi)$$
$$Mod_{\Sigma(\mathcal{D})}(\neg\varphi) = Mod_{\Sigma(\mathcal{D})} - Mod_{\Sigma(\mathcal{D})}(\varphi)$$
$$Mod_{\Sigma(\mathcal{D})}(\varphi \rightarrow \psi) = Mod_{\Sigma(\mathcal{D})}(\neg\varphi \vee \psi)$$
$$Mod_{\Sigma(\mathcal{D})}(\varphi \leftrightarrow \psi) = Mod_{\Sigma(\mathcal{D})}((\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi))$$
$$Mod_{\Sigma(\mathcal{D})}(\forall x \varphi(x)) = \bigcap_{a \in \mathcal{D}} Mod_{\Sigma(\mathcal{D})}(\varphi(a))$$
$$Mod_{\Sigma(\mathcal{D})}(\exists x \varphi(x)) = \bigcup_{a \in \mathcal{D}} Mod_{\Sigma(\mathcal{D})}(\varphi(a))$$

validità di formule predicative

per definire la validità di formule con variabili si ricorre al concetto di **assegnamento:**

ρ: $V \to D$, una funzione che associa elementi del sostegno D alle variabili in V

notazione: l'assegnamento $\rho_{x=a}$ coincide con ρ eccetto che associa a alla variabile x

un assegnamento ρ: $V \to D$ nel sostegno D di un Σ-modello M viene induttivamente esteso ad una corrispondente **funzione di valutazione**, che estende ai termini con variabili l'interpretazione fornita dal modello: $\_{}_{\rho}^{M} : T_{\Sigma(V)} \to D$

si estende alle variabili la base della definizione induttiva dell'interpretazione di termini, ponendo $x_{\rho}^{M} = \rho(x)$; l'interpretazione fornita dal modello fa il resto

la definizione induttiva di validità di enunciati è così riproponibile per quella di **validità di formule**, relativa a un dato assegnamento ; **N.B.** per la semantica dei quantificatori si pone:

$M \models_{\rho} \forall x\varphi(x)$ sse $\{a \in D \mid M \models_{\rho_{x=a}} \varphi(x)\} = D$

$M \models_{\rho} \exists x\varphi(x)$ sse $\{a \in D \mid M \models_{\rho_{x=a}} \varphi(x)\} \neq \emptyset$

si ottiene anche una definizione di validità di formule **indipendente dall'assegnamento** stipulando che una formula (con variabili) è valida in un modello quando lo è, nel senso della definizione precedente, per tutti gli assegnamenti

temi per ulteriori approfondimenti

1. **Linguaggi di specifica algebrica**
   La logica predicativa costituisce il nucleo essenziale della gran parte dei linguaggi di specifica algebrica, progettati per la definizione formale di proprietà di sistemi software e per lo sviluppo e la verifica di correttezza di tali sistemi con metodologie matematicamente ben fondate. In tempi recenti è stata compiuto un tentativo di armonizzare diversi linguaggi di questo tipo: il progetto CoFI ha prodotto la definizione della famiglia di linguaggi ***CASL (Common Algebraic Specification Language)***, basati sulla logica predicativa multisortale con operazioni parziali. Documentazione su CASL e sui relativi strumenti di supporto è reperibile al sito del progetto: www.cofi.info