

Overview

- Supponiamo di sapere che cos'è una formula della logica del primo ordine. (FOL)
- Consideriamo $(\mathbb{N}, +, \times)$
- Definiamo la teoria del primo ordine di $(\mathbb{N}, +, \times)$ come:

$$\text{Th}(\mathbb{N}, +, \times) := \{ \varphi \in \text{FOL} \mid \begin{array}{l} \text{cp } \varphi \text{ vera} \\ \text{in } (\mathbb{N}, +, \times) \end{array} \}$$

$$\exists m \forall m (m+m=m) \in \text{Th}(\mathbb{N}, +, \times)$$

- $\text{Th}(\mathbb{N}, +, \times)$ è decidibile?

No. Possiamo dimostrarlo:

$$\text{ETH} \leq \text{Th}(\mathbb{N}, +, \times)$$

- $\text{Th}(\mathbb{N}, +)$ è decidibile!

- Come Corollario otteniamo il teorema di incompletezza di Gödel (1930).

"Ci sono formule riguardanti l'aritmetica che sono vere ma non possono essere dimostrate."

2 FOZ: Syntax

Obiettivo: definiamo cos'è una formula

Def Un vocabolario (signature) del primo ordine
consiste di:

- simboli di funzione f, g, h, \dots
 - simboli di relazione p, q, \dots
- ognuno con la sua aritá (numero di argomenti)

Def Un termine é definito per induzione:

- una variabile é un termine
- Se t_1, \dots, t_n sono termini e f é un simbolo di funzione n -aria, allora $f(t_1, \dots, t_n)$ é un termine

Def Una formula φ è definita per induzione:

- $\underbrace{P(t_1 \dots t_m)}$ è una formula
predicato m-ario
- Se φ e ψ sono formule, allora
 $\neg\varphi$, $\varphi \wedge \psi$, $\varphi \vee \psi$, $\varphi \Rightarrow \psi$
 $\exists x. \varphi$, $\forall x. \psi$ sono formule.

Vocabolario: simboli di funzioni
 $+^2$ x^2 $-^1$ 0° $S(-)^1$

$$S(0) \quad S(S(0)) + S(0) \quad -0$$

simboli di relazione

$$\text{pari}(-)^1 = ^2$$

$$\text{pari}(0) \quad \exists m \forall n (\underline{m+n=0})$$

Data una formula φ , definiamo
 freevar(φ) come l'insieme delle
 variabili libere in φ . Se freevar(φ)
 $= \emptyset$ allora φ è un enunciato
 (= sentence, = formula chiusa).

$$\varphi = \exists m (m + m = 0)$$

$$\text{freevar}(\varphi) = \{m\}$$

$$\varphi = \exists z (\text{pari}(z) \wedge (z=0))$$

$$\text{freevar}(\varphi) = \{z\}$$

Dato un vocabolario, una Teoria è
 un insieme di formule basate su
 quel vocabolario.

3 FOL: Semantica

Obiettivo: definire quando una formula è vera in un modello.

Def Un modello U riferito ad un vocabolario $(f_1 \dots f_k, P_1, \dots P_j)$ consiste di:

- Un insieme U (detto anche universo)

- funzioni $f_1^U \dots f_k^U$ e relazioni $P_1^U \dots P_j^U$ tali che:

$$U = \mathbb{N}$$

$$(+^2, \text{pari}(-^1))$$

$$+^2 \mapsto \text{somma}$$

$$\text{pari}(-^1) \mapsto \begin{array}{l} \text{sottoinsieme} \\ \text{di numeri} \\ \text{pari} \subseteq U^1 \end{array}$$

$$=^2 \mapsto \left\{ (m, m) \mid \begin{array}{l} m \in \mathbb{N} \\ \subseteq U^2 \end{array} \right\}$$

- Se f_i ha aritma n , allora

$$f_i^U : U^n \rightarrow U.$$

$$P_i^U \subseteq U^m$$

Def Dato un insieme di variabili Var ,
una interpretazione (di variabili) è
una funzione $I: \text{Var} \rightarrow U$

Possiamo sempre estendere in modo
canonico I ad una interpretazione \hat{I}
per Termini:

I $\hat{I}(+)$ è definita per induzione:

$$\begin{array}{l} x \mapsto 3 \\ y \mapsto 5 \end{array} \quad \text{- se } t \text{ è una variabile allora}$$

$$\hat{I}(+) = I(+)$$

$$x+y \mapsto \begin{array}{l} \text{Somma} \\ \text{di } 3 \\ \text{e } 5 \end{array} \quad \text{- se } t = f(t_1, \dots, t_k) \text{ allora}$$
$$\hat{I}(+) = f^U(\hat{I}(t_1), \dots, \hat{I}(t_k))$$

Def Definiamo quando una formula φ è vera in un modello (U, I) per \Vdash

induzione su φ

$(U, I) \models \varphi$

pari $x+y$
 \uparrow

somma
 $d\in S = \bigoplus_{i=1}^n$
 \in insieme
 dei pari

$U, I \models P(t_1, \dots, t_k)$

$\wedge \hat{I}(t_1), \dots, \hat{I}(t_k) \in P^U$

$U, I \models \varphi \wedge \psi$ se $U, I \models \varphi$ e $U, I \models \psi$

$U, I \not\models \neg \varphi$ se $U, I \not\models \varphi$

:

$U, I \models \forall x. \varphi$ se puntualmente gli elementi
 $a \in U$

$\forall x \text{ pari}(x)$
 $\exists x \text{ pari}(x)$

$U, I[x \mapsto a] \models \varphi$

$U, I \models \exists x. \varphi$ se per almeno un elemento
 $a \in U$

$U, I[x \mapsto a] \models \varphi$

Esempio

Vocabolario: ${}^2+, {}^2=$

Formula: $\varphi = \forall y \exists x (x+x=y)$

$((\mathbb{N}, "somma", "uguale"), I) \not\models \varphi$

$((\mathbb{R}, "somma", "uguale"), I) \models \varphi \quad \checkmark$

φ è valida se per tutti i modelli \cup
e interpretazioni I , $\cup, I \models \varphi$.

$\forall x (pari(x) \vee \neg pari(x))$

4 Decidibilità

Teorema Il problema "φ è valida?"

per φ una formula su vocabolario arbitrario, è indecidibile

$$\{ \varphi \mid \varphi \text{ è valida} \}$$

Dimostrazione :

Strategia generale

$$\text{ETH} \leq \text{VALIDITY}$$

$$M \mapsto \varphi_M$$

M ferma su Σ se φ_M è valida.

M si ferma su Σ se φ_M è valida

$$\{ x \mid x = \text{code}(\varphi_M) \in \varphi_M \text{ è valida} \}$$

Costruiamo un vocabolario:

- simboli di funzione:

- O^0 , S^1 , P^1

abbreviazione: $\underbrace{S(\dots(S(0)) =: m}$

- simboli di relazione:

- head 2

head (m, m) vera se la
testima è sulla cella # m al
parro m.

- state 2

state (m, m) vera se al parro m
lo stato è q_m

- cell_i 2

cell_i (m, m) vera se al
parro m la cella m contiene i.

- = 2

Costruiamo

φ_M

$\varphi_M := (\varphi_1 \wedge \varphi_2 \wedge \varphi_3 \wedge \varphi_4 \wedge \varphi_5) \Rightarrow \varphi_H$

$$\varphi_1 = \left\{ \begin{array}{l} \forall x \neg (S(x) = 0) \wedge \\ \forall x \forall z ((S(x) = S(z)) \Rightarrow x = z) \\ \forall x (\neg (x = 0) \Rightarrow \exists y (S(y) = x)) \\ (+ \text{ assiomi per predecessori}) \end{array} \right.$$

"Zero è successore se compiono come in \mathbb{N} "

$$\varphi_2 = \left\{ \begin{array}{l} \text{state}(0,0) \wedge \text{head}(0,1) \\ \wedge \forall y (\neg \text{cell}_0(0,y) \wedge \neg \text{cell}_1(0,y)) \\ \wedge \forall y (\neg \text{head}(0,y) \wedge \neg \text{head}(0, \text{succ}_y)) \\ \wedge \forall y (\neg \text{state}(0, S(y))) \end{array} \right.$$

"Al parro 0, lo stato è q. la testa è sulla
cella #1 e tutte le celle sono vuote"

$$\varphi_3 = \left\{ \begin{array}{l} \forall y \forall z \forall w (\neg(z=w) \Rightarrow \\ \quad \neg(\text{state}(y,z) \wedge \text{state}(y,w))) \\ \wedge \\ \forall y \forall z \forall w (\neg(z=w) \Rightarrow \\ \quad \neg(\text{head}(y,z) \wedge \text{head}(y,w))) \\ \wedge \\ \forall y \forall z (\neg(\text{cell}_0(y,z) \wedge \text{cell}_1(y,z))) \end{array} \right.$$

"A ogni parso y , la TM può essere solo in uno stato, la testa è su un'unica cella e ogni cella contiene al più un simbolo"

$$\varphi_4 = \forall y \forall z (\neg \text{head}(y,z) \Rightarrow \left(\begin{array}{l} \text{cell}_0(y,z) \Rightarrow \text{cell}_0(Sy,z) \\ \wedge \\ \text{cell}_1(y,z) \Rightarrow \text{cell}_1(Sy,z) \end{array} \right))$$

"Se la testina non è sulla cella z , allora il contenuto di z non cambia"

$$\varphi_S = \{ \bigwedge_{\text{tupla} \in S} \varphi_{\text{tupla}} \}$$

$$\text{tupla} = \langle q_i, \sigma, q_j, \sigma', \neg \exists \rangle$$

$$\begin{aligned} \varphi_{\text{tupla}} &= \forall y \forall z \left(\text{state}(y, i) \wedge \right. \\ &\quad \text{head}(y, z) \wedge \\ &\quad \text{cell}_{\sigma}(y, z) \\ &\Rightarrow \left. \begin{array}{l} \text{state}(s(y), j) \wedge \\ \text{head}(s(y), s(z)) \wedge \\ \text{cell}_{\sigma'}(s(y), z) \end{array} \right) \end{aligned}$$

"M ferma im uno stato finale q:"

$$\varphi_H = \exists y \bigvee_{q_i \text{ stato finale}} \text{state}(y, i)$$

5 Dimostrabilità

Def Dato un vocabolario, un sistema deduttivo (proof system) P consta di:

- assiomi (formule)
- regole di inferenza

$U, I \models \varphi$ - $P \vdash \varphi$ se φ è un assioma

- Se $P \vdash \varphi$ e $P \vdash \psi$ allora
 $P \vdash \varphi \wedge \psi$

Una dimostrazione di φ è una sequenza

$\varphi_1 \dots \varphi_m$ dove $\varphi = \varphi_m$ e
 φ_i è derivata da $\varphi_1 \dots \varphi_{i-1}$ usando
regole di inferenza.

Assumiamo due proprietà di P :

(A1)

$\{ \langle \varphi, \pi \rangle \mid \pi \text{ è una dimostrazione di } \varphi \}$
è decidibile.

(A2)

$P \vdash \varphi$ implica φ è valida.
(correttezza, "soundness")

Lemma Data una teoria T e

un sistema deduttivo P ,

$\{ \varphi \mid \varphi \in T \text{ e } P \vdash \varphi \}$
è riconoscibile.

Idea della dimostrazione:

Ispettiamo tutte le possibili dimostrazioni π
di φ in P di lunghezza crescente.

6 Incompletezza

$$\text{Th}(\mathbb{N}, +, \times) = \{\varphi \mid (\mathbb{N}, +, \times) \models \varphi\}$$

OBIETTIVO: dimostrare che esiste

$\varphi \in \text{Th}(\mathbb{N}, +, \times)$ non dimostrabili
in nessun P (che soddisfi A1 e A2).

Teorema 1

$\text{Th}(\mathbb{N}, +, \times)$ è indecidibile.

Idea della dimostrazione

$$\text{ETH} \leq \text{Th}(\mathbb{N}, +, \times)$$

Si fa in modo simile a quanto dimostrato
in precedenza

(codifica assomiglia alla Gödlistazione)

Teorema 2

Esiste $\varphi \in \text{Th}(\mathbb{N}, +, \times)$ tale che

φ non è dimostrabile in nessun P .

Dimostrazione

Supponiamo per assurdo che ogni $\varphi \in \text{Th}(\mathbb{N}, +, \times)$ sia dimostrabile in un qualche P .

Allora possiamo decidere $\text{Th}(\mathbb{N}, +, \times)$.

L'algoritmo è il seguente:

INPUT φ : 1. cerca in parallelo una dimostrazione

Osservazione: $\varphi \in \text{Th}(\mathbb{N}, +, \times)$ \top di φ e una di $\neg\varphi$ in P .

$\varphi \in \text{Th}(\mathbb{N}, +, \times)$ oppure 2. Se φ è dimostrabile in P

$\neg\varphi \in \text{Th}(\mathbb{N}, +, \times)$ allora la risposta è SÍ.

Poiché P è assunto completo, allora $\neg\varphi$ è dimostrabile e la risposta è NO.

$P \vdash \varphi$ oppure $P \vdash \neg\varphi$.

In A2, se $P \vdash \varphi$

allora $\varphi \in \text{Th}(\mathbb{N}, +, \times)$

Se $P \vdash \neg\varphi$ allora $\neg\varphi \in \text{Th}(\mathbb{N}, +, \times)$

Quindi la ricerca terminerà sempre.