Overview

- Supponiamo di sapere che cos'é una formula della logica del primo ordine. (FOL)

- Consideriamo $(\mathbb{N}, +, \times)$

- Definiamo la teoria del primo ordine di $(\mathbb{N}, +, \times)$ come:

$$Th(\mathbb{N}, +, \times) := \left\{ \varphi \in FOL \,\middle|\, \begin{array}{c} \varphi \text{ é vera} \\ \text{in } (\mathbb{N}, +, \times) \end{array} \right\}$$

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

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

No. Possiamo dimostrarlo:

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

- $Th(\mathbb{N}, +)$ é decidibile!

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

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

---

2 FOL: Syntax

Obiettivo: definiamo cos'é una formula

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

- simboli di funzione $f, g, h, \ldots$
- simboli di relazione $p, q, \ldots$

ognuno con la sua aritá (numero di argomenti)

Def Un termine é definito per induzione:

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

Def Una formula φ è definita per induzione:

- $\underbrace{P}_{\text{predicato } n\text{-ario}}(t_1 \dots t_n)$ è una formula

- 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.

simboli di funzione

Vocabolario: $\boxed{+^2 \quad \times^2 \quad -^1 \quad 0^0 \quad S(\cdot)^1}$

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

simboli di relazione

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

$\text{pari}(0) \qquad \exists n \, \forall m \, (n + m = 0)$

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

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

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

$$\psi = \exists z\,(\mathrm{pari}(z) \wedge (z=0))$$

$$\mathrm{freevar}(\psi) = \{z\}$$

Dato un vocabolario, una <u>teoria</u> 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 $\mathcal{U}$ 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:
  - Se f_i ha arità n, allora $f_i^U : U^n \to U$.
  - Se P_i ha arità n, allora $P_i^U \subseteq U^n$

$U = \mathbb{N}$

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

$+^2 \mapsto$ somma

$\text{pari}(-)^1 \mapsto$ sottoinsieme dei numeri pari $\subseteq U^1$

$=^2 \mapsto \{(n,n) \mid n \in \mathbb{N}\} \subseteq U^2$

Def Dato un insieme di variabili Var, una <u>interpretazione</u> (di variabili) é una funzione $I : Var \to U$

Possiamo sempre estendere in modo canonico I ad una interpretazione $\hat{I}$ per <u>termini</u>:

I

$x \mapsto 3$
$y \mapsto 5$

$\hat{I}$

$x+y \mapsto$ somma di 3 e 5

$\hat{I}(t)$ é definita per induzione:

- se t é una variabile allora

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

- se $t = f(t_1 \dots t_k)$ allora

$$\hat{I}(t) = f^U(\hat{I}(t_1), \dots, \hat{I}(t_k))$$

Def Definiamo quando una formula φ è vera in un modello $\mathcal{U}$ per induzione su φ $\Rightarrow$ $(\mathcal{U}, I) \models \varphi$

`\vdash`

pari, $x+y$, somma di 4 e 5 = 9, $\in$ insieme di pari

$$\mathcal{U}, I \models P(t_1 \dots t_k) \quad \text{sse} \quad \langle \hat{I}(t_1) \dots \hat{I}(t_k) \rangle \in P^{\mathcal{U}}$$

$$\mathcal{U}, I \models \varphi \wedge \psi \quad \text{sse} \quad \mathcal{U}, I \models \varphi \text{ e } \mathcal{U}, I \models \psi$$

$$\mathcal{U}, I \models \neg \varphi \quad \text{sse} \quad \mathcal{U}, I \not\models \varphi$$

$\vdots$

$\mathcal{U}, I \models \forall x . \varphi$ sse per tutti gli elementi $a \in \mathcal{U}$

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

$\forall x$ pari(x)

$\exists x$ pari(x)

$\mathcal{U}, I \models \exists x . \varphi$ sse per almeno un elemento $a \in \mathcal{U}$

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

Esempio

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

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

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

$((\mathbb{R}, \text{"somma"}, \text{"uguale"}), I) \models \varphi$ ✓

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

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

↳ 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

$$ETH \leq VALIDITY$$

$$M \longmapsto \varphi_M$$

M ferma su ε sse φ_M è valida.

M si ferma su ε sse φ_M è valida

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

Costruiamo un vocabolario:

- simboli di funzione:
  - 0^0, S^1, P^1

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

- simboli di relazione:
  - $head^2$ — $head(n, m)$ vera se la testina è sulla cella # m al passo n.
  - $\Sigma = \{0,1\}$ — $state^2$ — $state(n, m)$ vera se al passo n lo stato è q_m
  - $\forall i \in \Sigma$ — $cell_i^2$ — $cell_i(n, m)$ vera se al passo n la cella m contiene i.
  - $=^2$

Costruiamo φ_M

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

$$\varphi_1 = \begin{cases} \forall x \ \neg(S(x)=0) \quad \wedge \\ \forall x \forall z \left(\left([S(x) = S(y)] \right) \Rightarrow x = z \right) \wedge \\ \forall x \left(\neg(x=0) \Rightarrow \exists y \ (S(y) = x) \right) \\ (+ \text{ assiomi per predecessore}) \end{cases}$$

"Zero e successore si comportano come in $\mathbb{N}$"

$$\varphi_2 = \begin{cases} \text{state}(0,0) \wedge \text{head}(0,1) \\ \wedge \ \forall y \ (\neg \text{cell}_0(0,y) \wedge \neg \text{cell}_1(0,y)) \\ \wedge \ \forall y \ (\neg \text{head}(0,0) \wedge \neg \text{head}(0, SS(y))) \\ \wedge \ \forall y \ (\neg \text{state}(0, S(y))) \end{cases}$$

"Al passo 0, lo stato è q_0 la testa è sulla cella #1 e tutte le celle sono vuote"

$$\varphi_3 = \begin{cases} \forall y\, \forall z\, \forall w\, \big(\neg(z=w) \Rightarrow \neg(\mathrm{state}(y,z) \wedge \mathrm{state}(y,w))\big) \\ \wedge \\ \forall y\, \forall z\, \forall w\, \big(\neg(z=w) \Rightarrow \neg(\mathrm{head}(y,z) \wedge \mathrm{head}(y,w))\big) \\ \wedge \\ \forall y\, \forall z\, \big(\neg(\mathrm{cell}_0(y,z) \wedge \mathrm{cell}_1(y,z))\big) \end{cases}$$

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

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

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

$$\varphi_S = \left\{ \bigwedge_{tupla \in S} \varphi_{tupla} \right.$$

$$tupla = \langle q_i, \sigma, q_j, \sigma', \overset{\leftarrow}{\cancel{\rightarrow}} \rangle$$

$$\varphi_{tupla} = \forall y \forall z \begin{pmatrix} state(y, i) \wedge \\ head(y, z) \wedge \\ cell_\sigma(y, z) \end{pmatrix} \Rightarrow \begin{pmatrix} state(S(y), j) \wedge \\ head(S(y), \overset{P(z)}{\cancel{S(z)}}) \wedge \\ cell_{\sigma'}(S(y), z) \end{pmatrix}$$

"M ferma in uno stato finale q_i"

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

5 Dimostrabilitá

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

$\forall x \; x = x$

- assiomi (formule)
- regole di inferenza

$U, I \vDash \varphi$

- $P \vdash \varphi$ se φ é un assioma
- Se $P \vdash \varphi$ e $P \vdash \psi$ allora $P \vdash \varphi \wedge \psi$

Una dimostrazione di φ é una sequenza $\varphi_1 \dots \varphi_n$ dove $\varphi = \varphi_n$ e φ_i é derivata da $\varphi_1 \dots \varphi_{i-1}$ usando regole di inferenza.

Assumiamo due proprietà di P:

(A1) $\{ < \varphi, \pi > \mid \pi$ é una dimostrazione di $\varphi \}$
é decidibile.

(A2) $P \vdash \varphi$ implica φ é valida.
(correttezza, "soundness")

<u>Lemma</u> Data una teoria T e
un sistema deduttivo P,
$\{ \varphi \mid \varphi \in T$ e $P \vdash \varphi \}$
é riconoscibile.

<u>Idea della dimostrazione:</u>
Ispezioniamo tutte le possibili dimostrazioni π
di φ in P di lunghezza crescente.

6 Incompletezza

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

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

Teorema 1 $Th(\mathbb{N}, +, \times)$ è indecidibile.

Idea della dimostrazione

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

Si fa in modo simile a quanto dimostrato in precedenza

(codifica assomiglia alla Gödelizzazione)

Teorema 2

Esiste $\varphi \in Th(\mathbb{N},+,\times)$ tale che φ non è dimostrabile in nessun P.

Dimostrazione

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

Allora possiamo <u>decidere</u> $Th(\mathbb{N},+,\times)$.

L'algoritmo è il seguente:

Input φ : 1. cerca in parallelo una dimostrazione π di φ e una di $\neg\varphi$ in P.

2. Se φ é dimostrabile in P allora la risposta é <u>SÍ</u>.
Altrimenti, $\neg\varphi$ è dimostrabile e la risposta é <u>NO</u>.

Osservazione!
$\varphi \in Th(\mathbb{N},+,\times)$
oppure
$\neg\varphi \in Th(\mathbb{N},+,\times)$
Poiché P é assunto completo, allora $P \vdash \varphi$ oppure $P \vdash \neg\varphi$.
Quindi la ricerca terminerá sempre.

Per A2, se $P \vdash \varphi$ allora $\varphi \in Th(\mathbb{N},+,\times)$
Se $P \vdash \neg\varphi$ allora $\neg\varphi \in Th(\mathbb{N},+,\times)$