Dipartimento
di Matematica
Università di Pisa

APPUNTI DEL CORSO DI

LOGICA MATEMATICA

A cura di Chiara Di Sano
c.disano1@studenti.unipi.it

Con il contributo di Arianna Misuraca

Rielaborazione delle lezioni del prof.
A. Berarducci
A.A. 2021-2022

27-09-2021 Lezione 1 Prof. Berarducci

- Tutti gli uomini sono mortali, Socrate è un uomo, quindi Socrate è mortale

predicati ↑ ↑ costante

$\{U(x), M(x), S\{$ linguaggio → serve a formalizzare una proposizione logica

$\forall x\ (U(x) \to M(x)) \wedge U(S) \to M(S)$

formula della logica del 1° ordine, valida.

quantificare su elementi

intuitivamente: vera in ogni interpretazione dei simboli del linguaggio

- C'è qualcuno qui tale che se lui vince la lotteria tutti la vincono

↳ il più sfortunato di tutti

$\exists x\ (V(x) \to \forall s\ V(s))$ Valida

Dim: per casi: o tutti vincono, $\forall s\ V(s)$, o c'è almeno un x che non vince, $\exists V(x)$. Nel 1° caso prendo un x qualunque. Altrimenti prendo un x che non vince. ↳ V → V vera → F → F ∨ V vero

Intuizionisti: "se c'è un x devi darmi un modo per trovarlo"

- h funzione binaria $L = \{h\{$

$[\forall x y z\ h(x, h(y,z)) = y] \to \forall x\ y\ (x = y)$ Valida? (x es)

- Teorema (Church ~1935?)

Non esiste un algoritmo che data una formula mi dice se è valida. (l'insieme delle φ (formule) valide non è definibile)

Però esiste un semialgoritmo (è semi decidibile).

↳ più debole di un algoritmo

è come una macchina

Esiste un algoritmo che genera tutte le φ valide in qualche ordine

E. Post Un insieme è decidibile se sia lui che il complemento sono semidecidibili. "macchina" che genera formule non valide

Formule aritmetiche $+, \cdot, 0, 1 \longrightarrow$ interpretazione usuale su $\mathbb{N}$

le variabili variano su $\mathbb{N}$ (numeri naturali)

"x è primo"

$\forall a, b \quad (x = a \cdot b \to x = a \vee x = b)$ ← oppure

Congettura dei primi gemelli ← Formule aritmetiche

$\forall x \quad \exists y > x \quad (y \text{ è primo} \wedge y+2 \text{ è primo})$ ≡ esistono primi gemelli arbitrariamente grandi

DEF:
- $y > x \leftrightarrow \exists z\,(y+z = x \wedge z \neq 0)$
- $\exists y > x \;\; \varphi \leftrightarrow \exists y\,(y > x \to \varphi)$
- $2 = 1+1$

"Se do un interpretazione diversa a + e · la formula può diventare falsa"

Non si sa se è vera.

Teo (Gödel 1931) Le formule aritmetiche **vere** (vere in ogni interpretazione ← Valide ≠ vere → ho già dato un'interpretazione) non sono neppure semidecidibili.

Teo (Gödel 1931) (se T è del 1° ordine le regole sono sempre le stesse e si conoscono)

Sia T di assiomi e regole per l'aritmetica

ad es: (successore)

$$\forall xy \begin{cases} Sx = Sy \to x = y \\ Sx \neq 0 \\ x \neq 0 \to \exists y \;\; Sy = x \\ x + 0 = x \\ x \cdot 0 = 0 \\ x \cdot Sy = x \cdot y + x \end{cases}$$

$L = \{0, S, +, \cdot\}$ — Q di Robinson

induzione (tipo di quantificatore ≠ da $\forall xy$)

- 2° ordine: $\forall P \;\; (P(0) \wedge \forall x (Px \to P(Sx)) \to \forall y \, P(y)$
- 1° ordine: Data $\phi(x, \bar{y})$ del 1° ordine metto l'ax $\text{Ind}_{\phi, x}$

Faccio ind. solo sui pred. che riesco a scrivere: $\forall \bar{y} \;\; [\phi(0, \bar{y}) \wedge \forall x [\phi(x, \bar{y})] \to \phi(Sx, y)] \to \forall z \; \phi(z, y)]$

Svantaggio: Utilizzo infiniti assiomi

Vantaggio: Sono del 1° ordine

PA = Q + schema induzione del 1° ordine (Peano; infiniti assiomi) $\qquad PA^{(2)} = Q + \text{Ind } 2°$

Teo (Gödel 1931)

Per qualunque sistema T di assiomi (e regole) per l'aritmetica (dal T = PA) (cioè che dimostra solo cose vere → quindi non tutte)

esiste una φ formula aritmetica vera ma non dimostrabile in T.

Due domande:

1) esempio? Con(T) (coerenza di T (teoria)) → si può trasformare in una formula aritmetica

2) Come facciamo a sapere che è vera se non è dimostrabile?

1) Con(T) ≡ "T è coerente" equivale a una formula aritmetica

Esempio: $\forall x_1, \dots, x_n \quad p(x_1 \dots x_n) \neq 0$ allora $p(\bar{x}) \in \mathbb{Z}[\bar{x}]$

('è un polinomio esibibile che non ha zeri ma non è dimostrabile che non li abbia

2) Se credo che T dimostri solo cose vere, devo anche fidarmi del fatto che T sia coerente.

- Connettivi logici
  - booleani: $\wedge$ (e) $\vee$ (o) $\rightarrow$ (implica) $\neg$ (non) → sono sufficienti
  - quantificatori: $\forall x$ (per ogni) $\exists x$ (esiste) → se ne possono avere altri

0 = falso 1 = vero

A	B	A ∧ B	A ∨ B	A → B
0	0	0	0	1
0	1	0	1	1
1	0	0	1	0
1	1	1	1	1

A, B sono variabili proposizionali (variabile a valore 0,1)

formule proposizionali:

$[(A \vee B) \wedge \neg A] \rightarrow B$

A B	φ
0 1	1
1 0	1
0 0	1
1 1	1

Tautologia = vera in tutti e 4 i casi

Def Una formula proposizionale è una stringa di simboli costruita a partire dalle variabili proposizionali, i simboli $\wedge, \vee, \rightarrow, \neg$, e le parentesi. Grammatica ↓

Formula ::= Atomica | (Formula ∨ Formula) | (Formula ∧ Formula) | ¬Formula

φ, ψ Formule ⇒ (φ ∨ ψ) è una formula ecc.

La definizione è induttiva.

(A ∧ B → → A(A) non è una formula

Tautologia ⊂ Formule Proposizionali

Semantica: (= studio del significato / verità)

Sia v : Variabili Proposizionali $\to \{0,1\}$

estendo v a $\hat{v}$: Formule Prop $\to \{0,1\}$ usando le tavole

$\hat{v}((\varphi \wedge \psi)) = 1$ se $\hat{v}(\varphi) = 1$ e $\hat{v}(\psi) = 1$

$\hat{v}((\varphi \vee \psi)) = 1$ se $\hat{v}(\varphi) = 1$ o $\hat{v}(\psi) = 1$

→ falsa negli altri casi

$$\hat{v}(\neg\varphi) = \begin{cases} 1 & \text{se } \hat{v}(\varphi) = 0 \\ 0 & = 1 \end{cases}$$

$$\hat{v}(\varphi \to \psi) = \begin{cases} 0 & \text{se } \hat{v}(\varphi) = 1 \text{ e } \hat{v}(\psi) = 0 \\ 1 & \text{negli altri casi} \end{cases}$$

φ tautologia $\iff \forall v \quad \hat{v}(\varphi) = 1$

28-09-2021 Lezione 2 Prof. Berarducci

Tautologia $\subset$ Formule Proposizionali

ES $(A \vee B) \wedge \neg B \to A$ è una taut.

A	B	$\neg B$	$A \vee B$	$(A \vee B) \wedge \neg B$	$(A \vee B) \wedge \neg B \to A$
0	0	1	0	0	1
0	1	0	1	0	1
1	0	1	1	1	1
1	1	0	1	0	1

due casi

→ 4 valutazioni

tutti 1, quindi è una tautologia

Se la formula ha n variabili devo fare 2^n prove.

Si può riconoscere se $\varphi(a_1, \dots, a_n)$ è una tautologia in tempo polinomiale in lunghezza di φ?

Non si sa: a priori ci metto tempo 2^n

L = linguaggio proposizionale = insieme di variabili

L-formule = formule proposizionali costruite a partire da L

valutazioni = $v : L \to \{0,1\}$ $\quad \hat{v} : L\text{-formule} \to \{0,1\}$

T insieme di L-formule

$Mod_L(T) = \{v \mid$ per ogni $\varphi \in T \quad \hat{v}(\varphi) = 1\}$ → ogni φ è sempre vera in T

↓

ogni formula in T esclusa quella falsa

ES $T = \{A \vee B\}$ $\quad L = \{A, B\}$

$Mod_L(T) = \{ v_1, v_2, v_3 \}$ $\quad v_1(A) = v_1(B) = 1$

$v_2(A) = 1 \quad v_2(B) = 0$

$v_3(A) = 0 \quad v_3(B) = 1$

	A	B	A ∨ B
v_0	0	0	0
v_1	1	1	1
v_2	1	0	1
v_3	0	1	1

$\hat{v}$

T insieme di formule, φ singola formula

Def $T \models \varphi :\Leftrightarrow_{def} Mod_L(T) \subset Mod_L(\varphi)$

(si legge φ è conseguenza logica di T) $\rightarrow Mod_L(\{\varphi\})$

Es $\{ A \vee B, \neg A \} \models B$

esercizio $\{\varphi_1, \dots, \varphi_n\} \models \psi \Leftrightarrow (\varphi_1 \wedge \dots \wedge \varphi_n \rightarrow \psi) \in TAUT$ (tautologia)

$(A \rightarrow B) \rightarrow C \qquad (A \models B) \models C$ → non ha senso

Le premesse possono essere finite, le formule no

Scrivo $\models \varphi$ se $\{\} \models \varphi$ ($\{\}$ insieme vuoto)

oss. $\models \varphi \Leftrightarrow \varphi \in TAUT$

$T \models \varphi \Leftrightarrow Mod_L(T) \subset Mod_L(\varphi)$

$\Leftrightarrow \forall v : L \rightarrow \{0,1\} \quad v \in Mod(T) \rightarrow v \in Mod(\varphi)$

$\forall \varphi \in T \quad \hat{v}(\varphi) = 1$

$\forall \varphi \ (\varphi \in T \rightarrow \hat{v}(\varphi) \models 1)$

Se T è vuoto, $v \in Mod(T)$ è vero

$\Leftrightarrow$ se T è vuoto $\forall v \ v \in Mod(\varphi)$ cioè $\varphi \in TAUT$

φ è contraddittoria se non ha modelli $(= Mod_L \varphi = \{\})$

$\Leftrightarrow \models \neg\varphi$

Es T è contraddittoria $\Leftrightarrow Mod(T) = \{\}$

$\Leftrightarrow T \models \bot$

Oltre a $\neg \vee \wedge \rightarrow$ ho anche $\bot$
↑ bottom: formula sempre falsa

OSS $A \vee \neg A \in TAUT$

$A \wedge \neg A$ contraddittoria

Esercizio inventiamoci un connettivo ternario

A	B	C	if A then B else C
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	1

$(A \rightarrow B) \wedge (\neg A \rightarrow C)$ equivale al nuovo connettivo

Qualunque nuovo connettivo si può esprimere mediante $\neg \wedge \vee \rightarrow \bot$

$\varphi \equiv (2) \vee (4) \vee (7) \vee (8)$

$\equiv (\neg A \wedge \neg B \wedge C) \vee (\neg A \wedge B \wedge C) \vee (A \wedge B \wedge \neg C) \vee (A \wedge B \wedge C)$

Forma normale disgiuntiva

DNF = disgiunzione di congiunzione di letterali

letterale = variabili, $\neg$variabili

Ogni φ proposizionale, equivale a un DNF

$\varphi \equiv \psi$

$\varphi \models \psi$ e $\psi \models \varphi$

$Mod(\varphi) = Mod(\psi)$

CNF = congiunzione di disgiunzione di letterali

ES if A then B else C
|||
$(A \rightarrow B) \wedge (\neg A \rightarrow C)$

$(A \rightarrow B) \equiv (\neg A \vee B)$

$(\neg A \vee B) \wedge (A \vee C)$ ← CNF

Per trovare la CNF si guardano i casi falsi e si dice

(non sto in questo caso) $\wedge$ (non sto in questo caso) ecc.

De Morgan

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

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

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

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

avendo $\neg$ con $\wedge$ faccio la $\vee$ e viceversa

$A \mid B$ significa né A né B

↖ con questo connettivo faccio tutti gli altri

Tavola di verità:

A	B	$A \mid B$
0	0	1
0	1	0
1	0	0
1	1	0

$\neg A \equiv A \mid A$

$A \wedge B \equiv \neg A \mid \neg B$

Basi di connettivi: $\neg \wedge \vee \rightarrow$ base

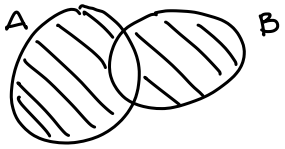
$\neg \wedge$ base

$\neg \vee$ base

$\mid$ base

||| con quelli faccio tutto

A	B	$A \oplus B$
0	0	0
0	1	1
1	0	1
1	1	0



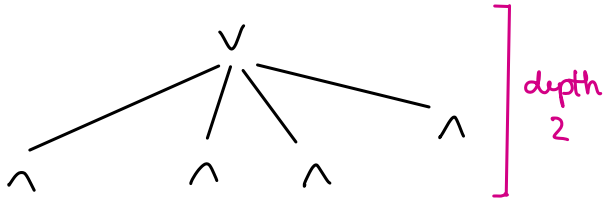
$A \oplus B \equiv (A \vee B) \wedge \neg(A \wedge B)$

DNF

$A \vee B \vee C$
|||

$(A \vee B) \vee C$
|||

$A \vee (B \vee C)$

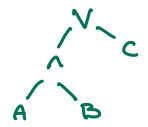


Unicità della lettura / Grammatica non ambigua

$F ::= \neg F \mid (F \vee F) \mid (F \wedge F) \mid (F \to F)$

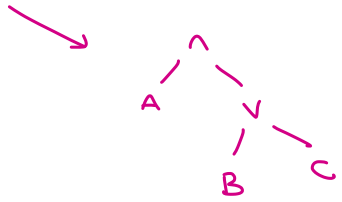
Se non metto le parentesi la grammatica è ambigua

$A \wedge B \vee C$ → $(A \wedge B) \vee C$, $A \wedge (B \vee C)$



parsing tree di $(A \wedge B) \vee C$

notazione polacca



$(\varphi \vee \psi) \sim \vee \varphi \psi$

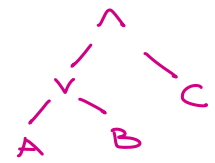
$(\varphi \wedge \psi) \sim \wedge \varphi \psi$

$\neg \varphi \sim \neg \varphi$

$\varphi \to \psi \sim \to \varphi \psi$

$(A \vee B) \wedge C \sim \wedge \vee ABC$

esercizio: non è ambigua



04-10-2021 Lezione 3 Prof. Berarducci

$T \models \varphi \iff Mod(T) \subseteq Mod(\varphi)$

$\{A \vee B, \neg A\} \models B$

A	B	A ∨ B	¬A	B
0	0	0	1	0
→0	1	1	1	①1
1	0	1	0	0
→1	1	1	0	①1

valutazione booleana

$Mod(\{A \vee B, \neg A\}) = \{v \mid v(A) = 0, v(B) = 1\}$

$\cap$

$Mod(B)$

Vogliamo estendere il concetto di conseguenza logica al caso predicativo (= logica 1° ordine)

$\{\forall x (A(x) \to B(x)), A(s)\} \models B(s)$

Anche nel caso predicativo $T \models \varphi \iff Mod(T) \subseteq Mod(\varphi)$, cambia la def. di $Mod(\ )$.

⊛ $\models$ è un simbolo della metateoria, prendiamo per buona questa teoria ma potremmo formalizzarla; come metat. potremmo prendere la teoria degli ins. ecc

L - Struttura

Un linguaggio è un insieme L di simboli di: (o segnatura)

- Relazione (o predicati) — a ogni simbolo è associata una arità = numero di argomenti
- funzione — le costanti hanno arità zero, gli altri simboli
- costante — hanno arità $\in \mathbb{N}$

Esempio $L = \{0, 1, +, \cdot, <\}$

$0, 1$ costanti

$+, \cdot$ funzioni binarie $\longrightarrow$ $+ : \mathbb{R}^2 \longrightarrow \mathbb{R}$, $\cdot : \mathbb{R}^2 \longrightarrow \mathbb{R}$

$<$ relazioni binarie

L - termini: $x,\ x \cdot y,\ 1,\ 0$

L - formule: $\forall x\,(\underbrace{x \neq 0}_{\neg(x \doteq 0)} \rightarrow \exists y\ \underbrace{x \cdot y \doteq 1}_{\cdot(x,y) \doteq 1})$ ($\doteq$ simbolo)

L - struttura: $(\mathbb{R},\ 0^{\mathbb{R}},\ 1^{\mathbb{R}},\ +^{\mathbb{R}},\ \cdot^{\mathbb{R}},\ <^{\mathbb{R}})$ ↳ definiti dalla metateoria

(Il pensiero non è lineare è una spirale)

$L' = \{0, 1, +, \cdot\}$

L' - struttura $= (Mat_{2\times 2}(\mathbb{R}),\ 0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},\ 1 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix},\ \cdot_{Mat},\ +_{Mat})$

Il ruolo dei modelli è preso dalle strutture.

Fisso un insieme V di simboli chiamati variabili

$V = \{x, y, t, x_1, x_2, x_3, \dots\}$ (in genere V è numerabile)

L - termini induttivamente:

1) $V \subset$ L - termini

2) $t_1, \dots, t_n$ L - termini e $f \in L$. Simbolo di funzione n-aria $\Rightarrow$ $f(t_1, \dots, t_n)$ L - termine

3) $c \in L$ simbolo di costante $\Rightarrow$ c · L - termine

Es $L = \{0, 1, +, \cdot, <\}$ $(0+1)\cdot x + 1$ L - termine $+(\cdot(+(0,1), x), 1)$

L - formule induttivamente: ↳ la più piccola stringa che verifica 1, 2, 3

I termini sono un insieme di stringhe = una successione di simboli

1) Ogni L - formula atomica è una L - formula

2) Se φ, ψ sono L - formule $\Rightarrow$ $\neg\varphi$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \rightarrow \psi)$, $\bot$ sono L - formule.

Una L-formula atomica è del tipo:

- $t_1 \doteq t_2$ dove t_1, t_2 sono L-termini
- $R(t_1, \dots, t_n)$ dove $t_1, \dots, t_n$ L-termini

$R \in L$ simboli di relazione n-aria

ES $L = \{0, 1, +, \cdot, <\}$

$0 + x < y \cdot x$ atomica

$<(+(0,x), \cdot(y,x))$

Cosa è il simbolo $\doteq$?
- Qualcuno lo mette in L
- altri tra i simboli logici al pari di $\wedge \vee \neg \to \forall \exists$

Non sarà mai una vera uguaglianza ma una congruenza (rel. d'equiv. che rispetta le operazioni aritmetiche)

Per il momento la metto tra i simboli logici.

SEMANTICA (significato) → L-Struttura:

Una L-Struttura $\mathcal{M}$ è data da

1) Un insieme non vuoto $M = dom(\mathcal{M})$

2) Una funzione interpretazione che associa ad ogni simbolo di L la sua interpretazione in $\mathcal{M}$

$c \in L$ simbolo di costante $\Rightarrow c^{\mathcal{M}} \in M$

$f \in L$ " funzione n-aria $\Rightarrow f^{\mathcal{M}} : M^n \to M$

$R \in L$ " relazione n-aria $\Rightarrow R^{\mathcal{M}} \subseteq M^n$

qualcuno la def. come $R^{\mathcal{M}} : M^n \to \{0, 1\}$

idea $(a_1, \dots, a_n) \in R^{\mathcal{M}} \Leftrightarrow$ in $\mathcal{M}$ è vero $R(a_i, \_, a_n)$

Ambiente Un ambiente è una funzione v: Variabili $\to M$

$L = \{0, 1, +, \cdot, <\}$ L-struttura $\mathbb{R}$ con le solite interpretazioni dei simboli

$\exists x\, (x \cdot x < y)$ è vera in $\mathbb{R}$ nell'ambiente $y \mapsto 2$

è falsa in $\mathbb{R}$ nell'ambiente $y \mapsto 0$

Semantica di Tarski (definizione di verità)

"oggi piove" è vera $\leftrightarrow$ oggi piove

↳ è un antivirgolette

M L-struttura, v: Variabili $\to M$ ambiente

t L-termine Voglio definire $t^{(M,v)} \in M$

1) $c \in L$ costante $\Rightarrow c^{(M,v)} = c^M$

2) x variabile $\Rightarrow x^{(M,v)} = v(x)$

3) $f \in L$ simb. funz. n-aria, $t_1, \dots, t_n$ L-termini

$f(t_1, \dots, t_n)^{(M,v)} = f^M(t_1^{(M,v)}, \dots, t_n^{(M,v)})$

$c \mapsto c^M$
$f \mapsto f^M$
$R \mapsto R^M$

Es $L = \{0, 1, +, \cdot, <\}$ $M = (\mathbb{R}, 0^{\mathbb{R}}, \dots)$

$(x+1)\cdot(1+1)^{(M, x \mapsto \sqrt{2})} = 2(\sqrt{2}+1) \in \mathbb{R}$

Semantica delle formule

"oggi piove" è vera $\leftrightarrow$ oggi piove

1) $R \in L$ simbolo relazione n-aria M L-struttura

$R(t_1, \dots, t_n)^{(M,v)} = \begin{cases} \text{vera} & \text{se } (t_1^{(M,v)}, \dots, t_n^{(M,v)}) \in R^M \\ \text{falsa} & \text{se } \quad " \quad " \quad \notin \quad " \end{cases}$

$R(t_1, \dots, t_n)$ atomica

2) Scrivo vero = 1, falso = 0

φ, ψ L-formule

il valore di verità di $(\varphi \wedge \psi)^{(M,v)}$, $(\varphi \vee \psi)^{(M,v)}$, $(\neg\varphi)^{(M,v)}$, $(\varphi \to \psi)^{(M,v)}$

si ricava da quello di $\varphi^{(M,v)}$, $\psi^{(M,v)}$ usando le tavole di verità.

il valore di $\bot^{(M,v)}$ è falso

3) $(\forall x\, \varphi)^{(M,v)}$ = vero se [...] ← come lo definisco?

falso altrimenti

Esempio $L = \{0, 1, +, \cdot, <\}$ L-struttura $\mathbb{R}$

$\exists x\, (x \cdot x = 1+1)^{(\mathbb{R}, v)}$ = vera (perché $\sqrt{2} \in \mathbb{R}$) o ambiente

nota: non posso dire che $\exists$ un L-termine t tc $(t \cdot t = 1 \cdot 1)^{(\mathbb{R}, v)}$

perché tale termine non c'è in L.

devo dire: esiste $a \in \mathbb{R}$ tc $\underbrace{a \cdot a = 1+1}$

ma questa non è una L-formula

dico: esiste $a \in \mathbb{R}$ tale che $(x \cdot x = 1+1)^{(\mathbb{R}, x \mapsto a)}$.

Formalmente,

$(\exists x\ \varphi)^{(M,v)}$ = vero $\Leftrightarrow \exists\, a \in M$ tale che $(\varphi)^{(M, v[a/x])}$

$v[a/x]$ è un nuovo ambiente che coincide con v eccetto per il fatto che da valore a alla variabile x. (sovrascrive ie valore di x).

Es $\exists x\ (x \cdot x = y)^{(\mathbb{R},\ y \mapsto \pi)}$ = vero se esiste $a \in \mathbb{R}$ $(x \cdot x = y)^{(x \mapsto a,\ y \mapsto \pi)}$

in effetti esiste $(a = \sqrt{\pi})$ quindi la formula è vera.

$\exists x\ (x \cdot x = 1+1)$ è vera (in $\mathbb{R}$) $\Leftrightarrow$ esiste $a \in \mathbb{R}$ tale che $a \cdot a = (1+1)^{\mathbb{R}}$

"la neve è bianca" è vera $\Leftrightarrow$ la neve è bianca.

CONSEGUENZA LOGICA

T insieme di L-formule

φ L-formule

$T \models \varphi \ :\Leftrightarrow \ Mod_L(T) \subset Mod_L(\varphi)$

$Mod_L(\varphi) = \{ (M, v) \mid \varphi^{(M,v)} = \text{vera} \}$

$Mod_L(T) = \bigcap_{\varphi \in T} Mod_L(\varphi)$

Es $L = \{0, 1, +, \cdot, <\}$ $M = \mathbb{N}$ con la solita interpretazione

$\varphi(x) \equiv \forall ab\ (ab \doteq x \to a \doteq x \vee b \doteq x)$

$\psi = \forall a\ (\exists x\ a = x + x \wedge a > 1+1 \longrightarrow \exists u, v\ \varphi(u) \wedge \varphi(v) \wedge a = u + v)$

ogni pari > 2 è somma di due primi.

$(\psi)^{(N, \text{ambiente})}$ = vera $\Leftrightarrow$ vale la congettura di Goldbach

È più facile capire $T \models \varphi$

$\to$ Teorema di Completezza di Gödel

05-10-2021 Lezione 4 Prof. Berarducci

Semantica di Tarski

per $\wedge\ \neg\ \vee\ \rightarrow$ (conn. booleani) si seguono le tavole di verità

$(\forall x\, \varphi)^{(M,v)} = \begin{cases} 1 & \text{se per ogni } a \in M \quad \varphi^{(M, v[x/a])} = 1 \\ 0 & \text{altrimenti} \end{cases}$

($\forall$: quantif.)

$(\exists x\, \varphi)^{(M,v)} = \begin{cases} 1 & \text{se esiste } a \in M \quad \varphi^{(M, v[x/a])} = 1 \\ 0 & \text{altrimenti} \end{cases}$

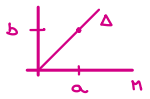
M L-struttura, v: variabili $\to M$ (Ambiente)

$(t_1 \doteq t_2)^{(M,v)} = 1$ se $t_1^{(M,v)} = t_2^{(M,v)}$

($\doteq$: simbolo; $=$: metateoria)

↑ che vuol dire?

$a = b \iff (a,b) \in \Delta = \{(x,y) \text{ tc } x = y\}$ (diagonale)



Variabili libere

$VL(t_1 \doteq t_2)$ = variabili in t_1 $\cup$ variabili in t_2

$VL(R(t_1, \dots, t_n)) = \bigcup_{i=1}^{n}$ variabili in t_i

$VL(\varphi \wedge \psi) = VL(\varphi \vee \psi) = VL(\varphi \rightarrow \psi) = VL(\varphi) \cup VL(\psi)$

$VL(\neg\varphi) = VL(\varphi)$

$VL(\forall x\, \varphi) = VL(\varphi) \setminus \{x\}$ (la x non è più libera perché l'abbiamo quantificata)

$VL(\exists x\, \varphi) = VL(\varphi) \setminus \{x\}$

Esempio $VL[(\forall x (\exists y\ y > x)) \wedge x = 1 + 1] = \{x\}$

(occorrenza legata a x; occorrenza libera di x; non ci sono VL)

Esercizio se $v|_{VL(\varphi)} = w|_{VL(\varphi)} \Rightarrow \varphi^{(M,v)} = \varphi^{(M,w)}$ (stesso valore di verità) [induzione sul n° dei connettivi di φ]

(v, w: ambienti)

Ad Es: $(x > 1+1)^{(\mathbb{R},v)}$ mi basta conoscere $v(x)$

$v(x) = 2 \quad v(y) = 3$

$w(x) = 2 \quad w(y) = 4$

$\Rightarrow (x > 1+1)^{(\mathbb{R},v)} = 1 \iff (x > 1+1)^{(\mathbb{R},w)} = 1$

$(\varphi \wedge \psi)^{(M,v)} = 1$ se $\varphi^{(M,v)} = 1$ e $\psi^{(M,v)} = 1$

conviene che v dia un valore a tutte le variabili

Esempio: $(x > y \wedge y > z)^{(M,v)}$

Se φ è chiusa, cioè $VL(\varphi) = \emptyset$, $\varphi^{(M,v)}$ non dipende da v e quindi

↳ valore di verità

posso scrivere $\varphi^K \underset{\text{def}}{=} \varphi^{(M,v)}$ per v qualsiasi

$Mod_L(\varphi) = \{ (M,v) \mid \varphi^{(M,v)} = 1 \}$

$T \models \varphi \iff Mod_L(T) \subseteq Mod_L(\varphi)$ dove $Mod_L(T) = \bigcap_{\psi \in T} Mod_L(\psi)$.

} ripasso

Se T, φ chiuse, non c'è bisogno di menzionare l'ambiente v, basta la struttura M

Esempio: T = teoria dei gruppi $\quad L = \{ 1, \cdot, (\,)^{-1} \}$

(costante, op. binaria, operazione unaria)

$T = \{$ $\forall x \quad 1 \cdot x = x$

$x \cdot 1 = x$

$x \cdot (x)^{-1} = 1$

$\forall x\, y\, z \quad (x \cdot y) \cdot z = x \cdot (y \cdot z) \}$

} assiomi (della Teoria dei gruppi)

$\varphi = \forall a \, [\forall x \, (x \cdot a = x) \to a = 1]$ $\quad Vl(\varphi) = \emptyset$

unicità dell'elem. neutro

↘ vera in tutti i gruppi perché φ è chiusa

$T \models \varphi \qquad Mod_L(T) =$ i gruppi

$T \not\models$ (∃ grp non ab) $\forall x\, y \quad (x \cdot y \doteq y \cdot x)$ esempio: M = matrici invertibili 2×2

$T \not\models$ (∃ grp abe) $\neg \forall x y \quad (x \cdot y \doteq y \cdot x)$ esempio: $M = \mathbb{Z}_n$

Una teoria è il dato di:

- un linguaggio L
- un insieme T di L-formule chiuse dette assiomi

Es: L-Teoria vuota → qui è L!

$Mod_L(\emptyset)$ = tutte le L-strutt.

La teoria è la coppia (L,T) ma se L è sottointeso scrivo solo T.

Def T è incoerente se $T \models \bot$ cioè se non ha modelli

cioè $Mod_L(T) \subseteq Mod_L(\bot) = \emptyset$

cioè $Mod_L(T) = \emptyset$

Def T è coerente se $T \not\models \bot$ cioè $Mod_L(T) \neq \emptyset$, almeno un modello

Def T è completa se è coerente e per ogni L-formula chiusa φ si ha $T \models \varphi$ o $T \models \neg\varphi$

Esempi: 1) La teoria dei gruppi non è completa, infatti non si può dedurre se un gruppo è abeliano o no dai soli assiomi.

2) ZFC = teoria degli insiemi di Zermelo-Fraenkel non è completa nonostante le speranze che lo fosse

$L = \{ \in \}$

$ZFC \nvdash CH$ (Cohen, 1963) $\quad ZFC \nvdash \neg CH$ (Gödel, 1941) $\quad CH$ = ipotesi del continuo

CH: ogni sottoinsieme infinito di $\mathbb{R}$ è in biiezione con $\mathbb{R}$ o con $\mathbb{N}$

3) T = Teoria degli anelli commutativi con soli due elementi → completa!

$L = \{ 0, 1, +, \cdot \}$

se φ è vera in $\mathbb{Z}/(2)$ $\quad T \vDash \varphi$

φ è falsa in $\mathbb{Z}/(2)$ $\quad T \vDash \neg\varphi$

T è completa

4) ACA_0 = teoria dei campi algebricamente chiusi di caratteristica 0

$L = \{ 0, 1, +, \cdot \}$

$\mathbb{C} \in Mod(ACA_0)$

$\mathbb{R} \notin Mod(ACA_0)$

Assiomi:

campi:
- $0 \cdot x = 0 = x \cdot 0$
- $1 \cdot x = x = x \cdot 1$
- $x + y = y + x$, $(x+y)+z = x+(y+z)$
- $x \cdot y = y \cdot x$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
- $x \cdot (y+z) = x \cdot y + x \cdot z$
- $\forall x (x \neq 0 \to \exists y \ \ x \cdot y = 1)$

algebricamente chiusi:
- $\forall a\, b \ \ \exists x \ \ x^2 + ax + b = 0$
- $\forall a\, b\, c \ \ \exists x \ \ x^3 + ax^2 + bx + c = 0$
- $\forall a\, b\, c\, d \ \ \exists x \ \ x^4 + ax^3 + bx^2 + cx + d = 0$
- $\vdots$

Servono infiniti assiomi!

caratt. zero:
- $0 \neq 1$
- $0 \neq 1+1$
- $0 \neq 1+1+1$
- $\vdots$

$\mathbb{Q} \notin Mod(ACA_0) \rightsquigarrow x^2 - 2$ non ha radici

$\mathbb{R} \notin Mod(ACA_0) \rightsquigarrow x^2 + 1$ non ha radici

I polinomi di 1° grado hanno radici in ogni campo

$\overline{\mathbb{Q}} \subset \mathbb{C}$, $\overline{\mathbb{Q}} \in Mod(ACA_0)$

$\overline{\mathbb{Q}} = \{ a \in \mathbb{C} \mid a$ è radice di un polinomio $p(x) \in \mathbb{C}[x]$ a coef. in $\mathbb{Q} \}$

$\pi \notin \overline{\mathbb{Q}}$ serve la dimostrazione

$|\overline{\mathbb{Q}}| = \aleph_0$ $|\mathbb{C}| = 2^{\aleph_0}$ $\overline{\mathbb{Q}} \neq \mathbb{C}$ non sono neanche isomorfi

$\overline{\mathbb{Q}} \equiv \mathbb{C}$ (elementarmente equivalente) cioè per ogni φ chiusa $\varphi^{\overline{\mathbb{Q}}} = \varphi^{\mathbb{C}}$. (stessa verità)

Teo se prendo due modelli A, B di ACA_0 ho $A \equiv B$.

Cor ACA_0 è completa.

Se φ è vera in $\mathbb{C}$ $\Rightarrow$ è vera in tutti i modelli di ACA_0
$\Rightarrow ACA_0 \vdash \varphi$

Teorie per l'aritmetica

$L = \{ 0, S, +, \cdot \}$
↳ successore

Diamo una teoria completa per $(\mathbb{N}, 0, s, +, \cdot)$ ← L-struttura con $0, S, +, \cdot$ interpretati nel solito modo

$Th(\mathbb{N}) = \{ \varphi \mid \varphi^{\mathbb{N}} = 1 \}$ teoria di $\mathbb{N}$
↑ assiomi: tutte le formule vere in $\mathbb{N}$

questa teoria è completa ma ha un difetto: non so dire se ad esempio la congettura di Goldbach è un assioma. → non conosco gli assiomi

Cerchiamo teorie $T \subset Th(\mathbb{N})$ di cui conosciamo gli assiomi

Teoria di Robinson Q

$L = \{ 0, S, +, \cdot \}$

Q1 $\forall x \forall y$	$Sx = Sy \to x = y$
Q2	$Sx \neq 0$
Q3	$x \neq 0 \to \exists y \ \ Sy = x$
Q4	$x + 0 = x$
Q5	$x + Sy = S(x + y)$
Q6	$x \cdot 1 = x$
Q7	$x \cdot Sy = x \cdot y + x$

Da questi assiomi non riesco a dimostrare neanche che il + è commutativo!

È completa? NO

$Mod_L(Q) = \{ \mathbb{N}$, e poi? $\}$

Definisco $(x$ è pari$) \equiv \exists y \ \ (y + y = x)$

$(x$ è dispari$) \equiv \exists y \ \ (S(y + y) = x)$

$Q \nvdash \forall x \ (x \text{ è pari} \vee x \text{ è dispari})$: $\mathbb{Z}[x]^+ \in Mod(Q)$

$Q \nvdash \exists \forall x \ (x \text{ è pari} \vee x \text{ è dispari})$: $\mathbb{N} \in Mod_L(Q)$

$\mathbb{Z}[x]^+$ = i polinomi $p(x) \in \mathbb{Z}[x]$ tali che $p(x) \equiv 0$

o $p(x) = a_0 + a_1 x + \dots + a_n x^n$ con $a_n > 0$

con $0, s, +, \cdot$ definiti nel modo ovvio.

$x = s(x-1)$ $\quad x-1 \in \mathbb{Z}[x]^+$

x non è né pari né dispari : $\nexists p(x)$ tc $p(x) + p(x) = x$ perché $\frac{x}{2} \notin \mathbb{Z}[x]^+$

Q è incompleta.

Es ! Peano (=PA) (definito nella 1ª lez)

$PA \vdash \forall x \ (x \text{ pari} \vee x \text{ dispari})$

— o —

Come mostro $T \vdash \varphi$?

metodo 1 : A buon senso

metodo 2 : regole fisse

↓

vantaggio : sono meccaniche, le posso insegnare a un computer

es: $\dfrac{T \vdash \alpha \quad T \vdash \alpha \to \beta}{T \vdash \beta} \qquad \alpha \vdash \alpha$

Come mostro $T \nvdash \varphi$?

metodo 1 : si trova un controesempio

metodo 2 : sconveniente

11-10-2021 lezione 5 Prof. Berarducci

Es T è completa $\Leftrightarrow$ è coerente e $\forall A, B \in Mod(T)$ $\boxed{A \equiv B}$ cioè $\forall \varphi$ chiusa φ^A è vera $\Leftrightarrow$ φ^B è vera.

A, B sono elementarmente equivalenti

La Semantica di Tarski fornisce una def di $T \vDash \varphi$ ma non un algoritmo.

Vogliamo definire una relazione $\vdash$ che poi a posteriori si dimostra equivalente a $\vDash$.

$T \vdash \varphi$ si legge "φ è dimostrabile da T"

$T \vDash \varphi$ " " "φ è conseguenza logica di T"

Regole di inferenza — Hilbert / Gentzen / Prawitz

(∧) $\dfrac{T\vdash\alpha \quad T\vdash\beta}{T\vdash\alpha\wedge\beta}$ $\qquad \dfrac{T\vdash\alpha\wedge\beta}{T\vdash\alpha}$ $\qquad \dfrac{T\vdash\alpha\wedge\beta}{T\vdash\beta}$

(∨) $\dfrac{T\vdash\alpha}{T\vdash\alpha\vee\beta}$ $\qquad \dfrac{T\vdash\beta}{T\vdash\alpha\vee\beta}$ $\qquad \dfrac{T,\alpha\vdash\gamma \quad T,\beta\vdash\gamma}{T,\alpha\vee\beta\vdash\gamma}$ (dove $T,\alpha \equiv T\cup\{\alpha\}$)

(→) $\dfrac{T\vdash\alpha \quad T\vdash\alpha\to\beta}{T\vdash\beta}$ $\qquad \dfrac{T,\alpha\vdash\beta}{T\vdash\alpha\to\beta}$

Lemmi:
per dimostrare β dimostro $\alpha\to\beta$

(idea: $\neg A \equiv A\to\bot$)

(¬, ⊥) $\dfrac{T\vdash\bot}{T\vdash\alpha}$ dal bottom dimostriamo qualsiasi cosa $\qquad \dfrac{T,\alpha\vdash\bot}{T\vdash\neg\alpha}$ $\qquad$ (RAA) reductio ad absurdum $\dfrac{T,\neg\alpha\vdash\bot}{T\vdash\alpha}$

Indebolimento: $T\vdash\alpha$, $T\cup S\vdash\alpha$ (↗ potenzialmente infinito)

Assiomi $\quad T,\alpha\vdash\alpha$ $\qquad \dfrac{T\vdash\alpha \quad T\vdash\neg\alpha}{T\vdash\bot}$

le regole qui sopra valgono sia per la logica proposizionale che predicativa.

Regole per ∀, ∃

L-linguaggio:
T insieme di L-formule
φ L-formula
t L-termine

(∀) $\dfrac{T\vdash\forall x\varphi}{T\vdash\varphi[t/x]}$ dove t è un termine sostituibile per x in φ

$\dfrac{T\vdash\varphi}{T\vdash\forall x\varphi}$ e $x\notin VL(T)=\bigcup_{\varphi\in T} VL(\varphi)$

(∃) $\dfrac{T\vdash\varphi[t/x]}{T\vdash\exists x\varphi}$ dove t è sostituibile

(idea: $\exists x\varphi \equiv \neg\forall x\neg\varphi$ mentre le regole per ∀ e ¬ ottengo quelle dell'esiste)

$\dfrac{T,\varphi\vdash\gamma}{T,\exists x\varphi\vdash\gamma}$ $x\notin VL(T,\gamma)$ idea: $\forall x(\varphi(x)\to\gamma)\to(\exists x\ \varphi(x))\to\gamma$

Esempio (vogliamo usare le regole anziché le tavole di verità)

$\vdash A\vee\neg A$ (mi dice che è una taut.)

Soluzione: non posso sperare di avere $\vdash A$ né $\vdash\neg A$, devo usare RAA.

1) $\neg A \vdash \neg A$ (Assioma di base)

2) $\neg A \vdash A \vee \neg A$ (Introduzione di $\vee$)

3) $\neg A, \neg(A \vee \neg A) \vdash A \vee \neg A$ (Indebolimento) — ho aggiunto un'hp

4) $\neg A, \neg(A \vee \neg A) \vdash \neg(A \vee \neg A)$ (Ass.)

5) $\neg A, \neg(\underbrace{A \vee \neg A}_{A \wedge \neg A}) \vdash \bot$ (3+4+Intro $\bot$)

6) $\neg(A \vee \neg A) \vdash A$ (RAA, $\overbrace{T, \neg A \vdash}^{A \vee \neg A} \Rightarrow T \vdash A$)

Ripeto gli stessi passaggi ma per A (anziché $\neg A$)

7) $A \vdash A$

8) $A \vdash A \vee \neg A$

9) $A, \neg(A \vee \neg A) \vdash A \vee \neg A$

10) $A, \neg(A \vee \neg A) \vdash \neg(A \vee \neg A)$

11) $A, \neg(A \vee \neg A) \vdash \bot$

12) $\neg(A \vee \neg A) \vdash \neg A$ (RAA)

13) $\neg(A \vee \neg A) \vdash \bot$ (6+12+$\bot$)

14) $\vdash A \vee \neg A$ (RAA)

Teorema:
Nel caso proposizionale $\vdash \varphi \iff \varphi$ TAUT.

(*) deduco (3) da (2) e (4) dagli assiomi

Regole intuizioniste = tutte le regole $\setminus \{RAA\}$

A partire dalle regole intuizioniste si ottengono sistemi equivalenti, aggiungendo una delle seguenti:

1) aggiungo RAA
2) aggiungo $\vdash A \vee \neg A$
3) aggiungo $\vdash \neg\neg A \to A$
4) $\dfrac{T, \alpha \vdash \beta \quad T, \neg\alpha \vdash \beta}{T \vdash \beta}$

Esercizio: Dim. che sono equivalenti

Con la logica intuizionista non si dim:

$\vdash \exists x\,(V(x) \to \forall y\, V(y))$

Termini sostituibili per x in φ

$\forall x\ \exists y\ (y \neq x) \not\vdash \exists y\ (y \neq y)$ non è vero che da $\forall x \varphi x$ ottengo $\varphi(t)$ con t termine qualunque.

$\forall x\ \varphi(x) \not\vdash \varphi(y)$

Servono restrizioni:

$\dfrac{T \vdash \forall x \varphi}{T \vdash \varphi[t/x]}$ con t sostituibile cioè tale che le variabili di t non diventano legate dopo la sostituzione $\varphi[t/x]$.

I termini chiusi sono sempre sostituibili. I termini aperti potrebbero non esserlo: $\forall x\ \exists y\ (y \neq x) \vdash \exists y\ (y \neq z)$ VA BENE!

Esercizio: $\exists x\ \neg P(x) \vdash \neg \forall x\ P(x)$ $\quad L = \{P\}$ (P predicato)

Soluzione: $\neg P(x), \forall x P(x) \vdash P(z) = P(x)[z/x]$

$\forall x P(x), \neg P(z) \vdash P(z)$

$\forall x P(x), \neg P(z) \vdash \neg P(z)$

$\forall x P(x), \neg P(z) \vdash \bot$

$\neg P(z) \vdash \neg \forall x P(x)$

$\exists z \neg P(z) \vdash \neg \forall x P(x)$ potevo mettere ovunque x al posto di z

non ho adoperato RAA $\rightsquigarrow$ È intuizionista.

Esempio: $\neg \forall x P(x) \vdash \exists x \neg P(x)$ Serve RAA

Soluzione: $\neg P(x) \vdash \neg P(x)$ (Ass.)

$\neg P(x) \vdash \exists x \neg P(x)$ (Intro $\exists$)

$\neg P(x), \neg \exists x \neg P(x) \vdash \bot$ (perché ottengo sia $\exists x \neg P(x)$ sia $\neg \exists x \neg P(x)$ — Indebolim.)

$\neg \exists x \neg P(x) \vdash P(x)$ (RAA)

$\neg \forall x P(x), \neg \exists x \neg P(x) \vdash \bot$ (ottengo sia $\neg \forall x P(x)$ sia $\forall x P(x)$)

$\neg \forall x P(x) \vdash \exists x \neg P(x)$ (RAA)

Regole dell'$\doteq$

$\vdash x \doteq x$

$\vdash x \doteq y, \alpha[x/u] \vdash \alpha[y/u]$

con x, y sostituibili per u in α

$\alpha \equiv \exists x (x \neq u)$

$\alpha[y/u] \equiv \exists x (x \neq y)$

$\alpha[x/u] \equiv \exists x (x \neq x)$

} motivo per cui serve x, y sostituibili

Esercizio:
- $x \doteq y \vdash y \doteq x$
- $x \doteq y, y \doteq z \vdash x \doteq z$

Prossimo obiettivo: $T \models \varphi \Leftrightarrow T \vdash \varphi$

15-10-2021 Lezione 6 Prof. Berarducci

$x \doteq x$

$x \doteq y, \varphi[x/u] \vdash \varphi[y/u]$ x, y sostituibili per u in φ

Esercizio

$x \doteq y \vdash y \doteq x$

come φ prendo $u \doteq x$

Per la 2) ho $x \doteq y, x \doteq x \vdash y \doteq x$

$x \doteq y \vdash x \doteq x \to y \doteq x$ (intro $\to$)

1) $\vdash x \doteq x$

$x \doteq y \vdash x \doteq x$

$x \doteq y \vdash y \doteq x$ □

Transitività

$x \doteq y, y \doteq z \vdash x \doteq z$. Come φ prendo $(u \doteq z)$

Dim. $y \doteq x, \varphi[y/x] \vdash \varphi[x/u]$

$y \doteq x, y \doteq z \vdash x \doteq z$

$y \doteq z \vdash y \doteq x \to x \doteq z$

$x \doteq y \vdash y \doteq x$ (es. precedente)

$x \doteq y, y \doteq z \vdash x \doteq z$

$x \doteq y \to x \doteq z$. □

Domanda: $\begin{cases} x \doteq y, \varphi[x/u] \vdash \varphi[y/u] \\ x \doteq x \end{cases}$

$\Downarrow$

$\begin{cases} x \doteq y \vdash y \doteq x \\ x \doteq y, y \doteq z \vdash x = z \\ x \doteq x \end{cases}$

Esistono operazioni binarie che rispettano le regole dell'= ma non sono l'uguaglianza?

Dal 2° gruppo di regole non si dimostra $L = I + I$

$x \doteq y \vdash x + z \doteq y + z$. Si ottiene dal primo gruppo con φ: $xc + z \doteq u + z$

$x \doteq y, \varphi[x/z] \vdash \varphi[y/z]$

$x + z = x + z \vdash x + z = y + z$

mi manca da ottenere $\vdash x+z \doteq x+z$

lo ottengo così: $\vdash x \doteq x$

$\vdash \forall x\,(x \doteq x)$

$\vdash x+z \doteq x+z$

$x+z$ è sostituibile al posto di x in $x \doteq x$

Leibnitz

$x=y \Leftrightarrow \forall P\,(P(x) \leftrightarrow P(y))$ → uno dei modi per pensare l'uguaglianza

↕ 2° ordine

Def $T \vdash_{DN} \varphi$

DN = deduzione naturale (Prawitz)

$\Leftrightarrow$ def

esiste una successione di coppie $(T_1,\varphi_1),\dots,(T_n,\varphi_n)$ tali che $\varphi_n=\varphi$ $T_n=T$ per ogni $i \leq n$

$\dfrac{T,\alpha \vdash \beta}{T \vdash \alpha \to \beta}$

(T_i,φ_i) (lo penso come $T_i \vdash \varphi_i$) si ottiene da uno o due coppie prec. tramite una regola, oppure $\varphi_i \in T_i$.

O meglio: dimostrazione formale

$T \vdash_{DN} \varphi \Leftrightarrow \exists$ successione $(T_1,\varphi_1),\dots,(T_n,\varphi_n)$ tale che ogni (T_i,φ_i) o è un assioma (cioè $\varphi_i \in T_i$) oppure segue da coppie precedenti tramite una regola e $T_1,\dots,T_n$ sono insiemi finiti di formule, $T \supset T_n$, $\varphi_n=\varphi$

Teo (compattezza sintattica)

$T \vdash_{DN} \varphi \Leftrightarrow \exists\, T' \subset T$ (T' finito) $\; T' \vdash_{DN} \varphi$

Dim: ovvio

Teo (compattezza semantica)

$T \models \varphi \Leftrightarrow \exists\, T' \subset T$ (T' finito) $\; T' \models \varphi$

non è affatto ovvio!

(falso per la logica del 2° ordine)

Si deduce dal fatto che $\vdash_{DN}$ equivale a $\models$

Esempio $L=\{0,1,+,\cdot\}$ linguaggio dei campi

φ L-formula chiusa

φ vera in tutti i campi di caratteristica zero

$\Rightarrow \exists\, p$ primo tc φ è vera in tutti i campi di caratteristica $\geq p$

Dim. T = teoria dei campi

L'ipotesi dice che $T \cup \{0\neq 1,\ 0\neq 1+1,\ \dots\} \vDash \varphi$ "φ è vera in ogni $\mathbb{K}$ $\mathrm{char}(\mathbb{K})=0$"

per il teo di compattezza esiste un sottoinsieme finito $S \subset T \cup \{0\neq 1,\ 0\neq 1+1,\dots\}$

$S \vDash \varphi \Rightarrow T \cup \{0\neq 1,\dots,0\neq \underbrace{1+\dots+1}_{p}\} \vDash \varphi$

Quindi φ è vera nei campi di char. $> p$

PA = Q + Schema di induzione $L=\{0,S,+,\cdot\}$

PA ha un modello non isomorfo a $\mathbb{N}$.

Dim: Sia $L' = L \cup \{c\}$ c nuova costante

$T = PA \cup \{c\neq 0,\ c\neq S0,\ c\neq SS0,\ \dots\}$

claim $T \not\vdash \bot$ (cioè T ha un modello)

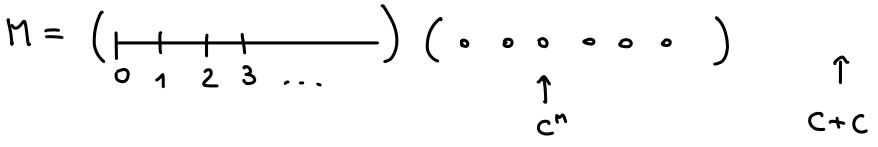
se no esiste $S \subset_{\text{finito}} T$ $S \vDash \bot$ (compattezza)

$\Rightarrow \exists\, n$ $PA \cup \{c\neq 0,\dots,c\neq \underbrace{SS\dots S}_{n \text{ volte}}0\} \vDash \bot$

Però prendo una $L \cup \{c\}$-struttura M fatta come $\mathbb{N}$ ma con c interpretato come $n+1$. Assurdo. QED claim.

Quindi esiste $M \in \mathrm{Mod}(T)$ M $L \cup \{c\}$-struttura

$M|_L$ è un modello di PA non isomorfo a $\mathbb{N}$ perché contiene un elemento ($c^M \in M$) diverso da $0,1,2,\dots$ □



So solo dimostrare che esiste ma non lo so esibire!

È un modello strano.

Espansioni $L \subset L'$

A L-struttura

B L'-struttura

B si dice espansione di A (A restrizione di B) se $\text{dom}B = \text{dom}A$ e i simboli di L sono interpretati nello stesso modo in A e in B

ES $(\mathbb{R}, +, 0)$ sono una restrizione di $(\mathbb{R}, +, \cdot, 0, 1)$
gruppo (non c'è il simbolo di $\cdot$, ma esiste!) campo

Peano 2 invece ha un unico modello!

Notazione: M L-struttura, φ formula, v: Variabili $\to$ M ambiente

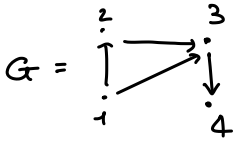
$\varphi^{(M,v)}$ = vero $\Leftrightarrow M \vDash \varphi(v)$; se φ è chiusa scrivo $M \vDash \varphi$ se $\forall v \ \varphi^{(M,v)}$ = vera (equivale a $\exists v \ \varphi^{(M,v)}$ = vera)

NB: non confondere $M \vDash \varphi$ (φ vera in M) con $T \vDash \varphi$ ($\text{Mod}(T) \subset \text{Mod}(\varphi)$)

Esempio: $L = \{E\}$ E relazione binaria

$\text{Mod}_L(\emptyset)$ = Grafi = insiemi con relazione binaria (non devono verificare alcun assioma)
(insieme vuoto)

Grafo $G = (V, E_G)$ $E_G \subset V \times V$



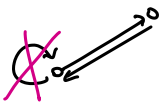
vertici
$V = \{1, 2, 3, 4\}$

$E_G = \{(1,2), (2,3), (1,3), (3,4)\}$
spigoli

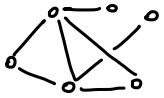
Esempio di grafo orientato

Grafi non orientati

$T = \{\forall x\, y \quad E(x,y) \to E(y,x), \ \forall x \ \neg E(x,x)\}$



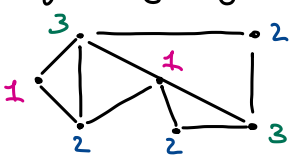
esempio

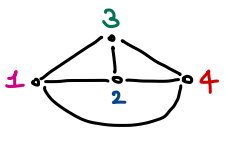


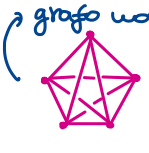
$\text{Mod}(T)$ = Grafi non orientati senza loop. Una colorazione di un grafo $G = (V, E_G)$ è una mappa $c: V \to \{\text{colori}\}$ (insieme finito) tc $E_G(x,y) \to c(x) \neq c(y) \quad \forall x, y \in V$

Teorema dei 4 colori

Ogni grafo planare è colorabile con al più 4 colori.



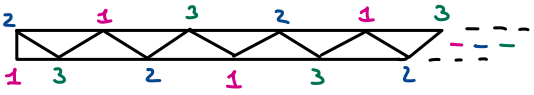




grafo non planare → servono 5 colori

Per i grafi non planari il teorema non vale!

Teorema: Se $G=(V, E_G)$ grafo infinito tale che ogni sottografo $(V', \underbrace{E_G|_{V'}}_{E_G \cap (V' \times V')})$ $V' \subset V$ finito è K-colorabile $\Rightarrow$ G è K-colorabile

$G =$ 

(per concretezza prendo $K=3$)

Dim: Fisso $G=(V, E_G)$ grafo infinito. Suppongo che tutti i suoi sottografi finiti siano 3-colorabili. Voglio mostrare che G è 3-col.

Costruisco una teoria T_G fatta così:

$L(T_G) = \{ E, \underbrace{v_0, v_1, v_2, \dots}_{\text{tante cost. quanti vertici di } V}, \underbrace{c_1, c_2, c_3}_{\text{3 predicati numerici}} \}$ $\qquad V = \{0, 1, 2, \dots\} = \mathbb{N}$

E: Rel. binaria

Voglio assiomi tali che ogni modello di T_G induce una 3-colorazz. di $G=(V, E_G)$ e viceversa

Assiomi di T_G:

$\forall x \, [C_1(x) \vee C_2(x) \vee C_3(x)]$

$\forall x \, [C_1(x) \to \neg C_2(x) \wedge \neg C_3(x)]$ etc. (ogni vertice ha un solo valore)

$\forall x, y \; [E(x,y) \wedge C_1(x) \to \neg C_1(y)]$ idem per C_2, C_3

$\{ E(v_i, v_j) \mid (i,j) \in E_G \}$ $\quad \{ \neg E(v_i, v_j) \mid (i,j) \notin E_G \}$

Dato $M \models T_G$ colloco $G=(V, E_G)$ assegnando ad $i \in V$ il colore $j \in \{1,2,3\}$

$\Leftrightarrow M \models C_j(v_i)$

Viceversa data una 3-colorazione $c: V \to \{1,2,3\}$ di $G=(V, E_G)$

trovo un modello $M = (V, E_G, C_1^M, C_2^M, C_3^M)$.

$C_1^M \subset V$ $\qquad C_1^M = \{ i \in V \mid c(i) = 1 \}$

$C_2^M \subset V$ $\qquad$ idem

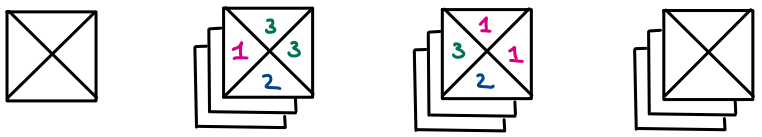
$C_3^M \subset V$ $\qquad$ "

Ora applico la compattezza. Se ogni sottografo finito di $G=(V, E_G)$ è 3-colorabile $\Rightarrow$ ogni sottoteoria finita S di T_G ha un modello.

$\Rightarrow$ T_G ha un modello $\Rightarrow$ G è 3-colorabile.

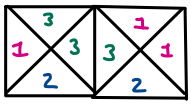
Compattezza $\square$

Hao Wang

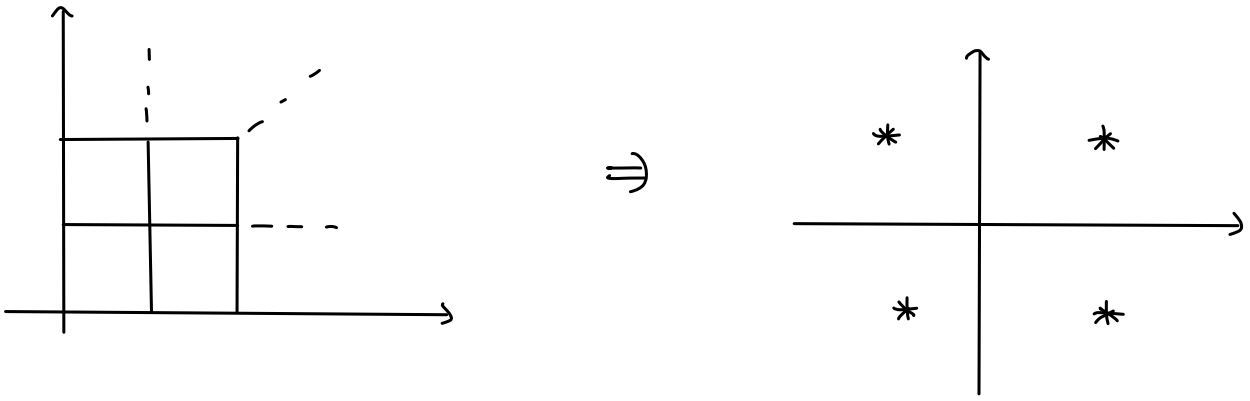


Affiancare le piastrelle affinché i colori combacino.

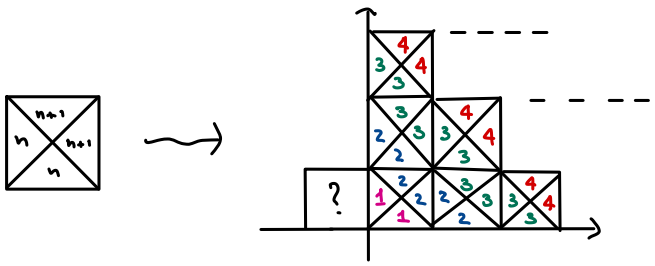
Ad esempio:



Supponiamo di avere un numero finito di tipi di piastrelle fatti in modo tale che in qualche modo riesco a tassellare un quadrante infinito del piano. Allora posso tassellare tutto il piano.



NB: È importante che il numero sia finito! Altrimenti potrei avere:



Hint: usare la compattezza più il fatto che le mattonelle sono un numero finito.

18-10-2021 Lezione 7 Prof. Berarducci

$T \vdash_{DN} \varphi$ φ è dimostrabile da T usando le regole di inferenza.

(Scrivo $T \vdash \varphi$ invece di $T \vdash_{DN} \varphi$ per semplicità)

Def: T è coerente se $T \nvdash \bot$

T è soddisfacibile se $T \nvdash \bot$, ovvero T ha un modello.

Oss: Sono equivalenti:

1) $T \vdash \bot$ (incoerente)

2) $\exists \theta \quad T \vdash \theta$ e $T \vdash \neg\theta$

3) $\forall \theta \quad T \vdash \theta$

dim: (1→3) $\dfrac{T \vdash \bot}{T \vdash \theta}$, (3→2) ovvio, (2→1) $\dfrac{T \vdash \theta \qquad T \vdash \neg\theta}{T \vdash \bot}$. □

Teo di correttezza: $T \vdash \varphi \Rightarrow T \models \varphi$

Dim (nel caso proposizionale)

Basta mostrare che le regole di inferenza sono corrette.

esempio: $\dfrac{T, \alpha \vdash \gamma \qquad T, \beta \vdash \gamma}{T, \alpha \vee \beta \vdash \gamma}$ Regola (∨-sinistra)

è corretta nel senso che:

$$T, \alpha \models \gamma \qquad T, \beta \models \gamma \quad \Rightarrow \quad T, \alpha \vee \beta \models \gamma$$

dimostra che è corretta. Assumo $T, \alpha \models \gamma$ $T, \beta \models \gamma$.

Mostro $T, \alpha \vee \beta \models \gamma$. Prendo un modello $v: Var \to \{0,1\}$ di $T, \alpha \vee \beta$.

Mostro $\tilde{v}(\gamma) = 1$. So che $\tilde{v}(\alpha \vee \beta) = 1$, quindi $\tilde{v}(\alpha) = 1$ o $\tilde{v}(\beta) = 1$.

Nel caso $\tilde{v}(\alpha) = 1$, allora visto che $T, \alpha \models \gamma$, $\tilde{v}(\gamma) = 1$.

Nel caso $\tilde{v}(\beta) = 1$, visto che $T, \beta \models \gamma \Rightarrow \tilde{v}(\gamma) = 1$. In ogni caso è vero γ in $\tilde{v}$. Quindi $T, \alpha \vee \beta \models \gamma$.

Analogamente tutte le altre regole proposizionali sono corrette.

Devo mostrare $T \vdash_{DN} \varphi \Rightarrow T \models \varphi$.

$T \vdash_{DN} \varphi$ significa che c'è una successione di coppie $(T_1, \varphi_1), \ldots, (T_n, \varphi_n)$ dove ciascuna è un assioma o segue da precedenti coppie tramite una regola e $\varphi_n = \varphi$, $T_n \underset{\text{finito}}{\subseteq} T$.

Per induzione su $K \leq n$ mostro che $T_K \models \varphi_K$. Il passo induttivo segue dalla correttezza delle regole. C'è anche il caso in cui (T_K, φ_K) non segue dai passi precedenti ma è un assioma, cioè $\varphi_K \in T_K$. In quel caso è ovvio che $T_K \models \varphi_K$. Quindi $T_n \models \varphi_n$.

Quindi $T \vdash \varphi$ perché $\varphi = \varphi_n$, $T \supset T_n$.

Teo di Completezza (proposizionale):

$T \models \varphi \Rightarrow T \vdash_{DN} \varphi$

Dim:

① $T \nvdash \neg\varphi \Rightarrow T, \varphi$ coerente.

dim. $T, \varphi \vdash \bot \Rightarrow T \vdash \neg\varphi$ per una delle regole

② $T \nvdash \varphi \Rightarrow T, \neg\varphi$ coerente

dim. $T, \neg\varphi \vdash \bot \Rightarrow T \vdash \varphi$ per RAA

③ Se T è coerente massimale (cioè non è strettamente contenuta in una teoria coerente $T' \supset T$ nello stesso linguaggio) $\Rightarrow T$ è completa.

dim: se T è incompleta $\Rightarrow \exists\, \theta$ L-formula $T \nvdash \theta$ e $T \nvdash \neg\theta$

però se $T \nvdash \theta \Rightarrow T, \neg\theta$ coerente $\overset{\uparrow}{\Rightarrow}$ $\neg\theta \in T \Rightarrow T \vdash \neg\theta$. Assurdo.
per massimalità

Es $L = \{A, B\}$ proposizionale, $T = \{A, B\}$ è completa.

es: $\theta = A \to B$ $\quad T \vdash \neg\theta$

Chiaro che semanticamente vale la negazione: $T \models \neg(A \to B)$,

verificare sintatticamente = con le regole: $T \vdash \neg(A \to B)$)

T non è massimale, ad es. non contiene né θ né $\neg\theta$ = teorema ma non assioma di T

Esercizio T completa $\Leftrightarrow \{\varphi \mid T \vdash \varphi\}$ è coerente massimale

④ T coerente $\Leftrightarrow \forall\, T' \underset{\text{finito}}{\subset} T$ T' è coerente.

dim. $\Rightarrow$ ovvia ($\nexists\, T' \vdash \bot \Rightarrow T \vdash \bot$)

$\Leftarrow$ Se $T \vdash \bot$ per compattezza sintattica $\exists T' \underset{\text{finito}}{\subset} T$ $T' \vdash \bot$. $\square$

⑤ Sia $(T_i \mid i \in I)$ una catena di L-teorie coerente $\Rightarrow \bigcup_i T_i$ è coerente
↳ $\forall i, j \in I$ $T_i \subset T_j$ o $T_j \subset T_i$

dim: $\bigcup_{i \in I} T_i \vdash \bot$ per compattezza esiste $T' \underset{\text{finita}}{\subset} \bigcup_i T_i$ $T' \vdash \bot$

$T' = \{\varphi_1, \dots, \varphi_k\}$ $\varphi_1 \in T_{i_1}$ $\varphi_2 \in T_{i_2}$ … $\varphi_k \in T_{i_k}$ siccome è una catena

$T_{i_1} \cup \dots \cup T_{i_K}$ è uno dei T_i (formalmente si fa per induzione su K)

LEMMA DI LINDENBAUM

⑥ Ogni teoria coerente è contenuta in una teoria coerente massimale (in $\mathcal{L}$) dim: Zorn applicato all'insieme ordinato dall'inclusione delle teorie coerenti $\supseteq T$

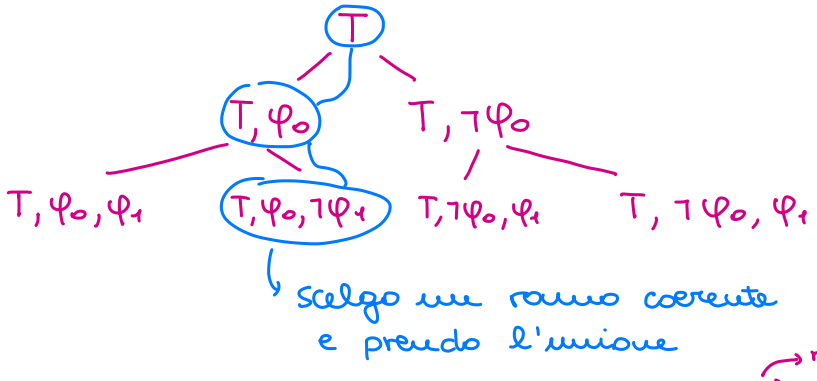
Se $\mathcal{L}$ è numerabile posso evitare Zorn. Fisso un'enumerazione $(\varphi_n \mid n \in \mathbb{N})$ delle $\mathcal{L}$-formule. Costruisco una successione $T_0 = T \subset T_1 \subset T_2 \subset T_3 \subset \dots$

$$T_{n+1} = \begin{cases} T_n \cup \{\varphi_n\} & \text{se coerente} \\ T_n \cup \{\neg\varphi_n\} & \text{altrimenti} \end{cases}$$

Se T_n è coerente, $T_n \cup \{\varphi_n\}$ non coerente

$\to T_n, \varphi_n \vdash \bot \Rightarrow T_n \vdash \neg\varphi_n \Rightarrow T_n, \neg\varphi_n$ coerente $\Rightarrow \bigcup_n T_n$ coerente massimale

$\Rightarrow$ König



⑦ Ogni teoria coerente massimale T ha un (UNICO) modello $v: V_v \to \{0,1\}$ (→ nel caso proposizionale)

dim: sia $A \in \mathcal{L}$ variabile proposizionale

definisco $v(A) = 1$ se $A \in T$

$v(A) = 0$ se $\neg A \in T$

Siccome T è coerente, non può essere che sia A sia $\neg A$ sono in T.

Siccome T è massimale, una delle due è in T quindi v è ben definita. Devo mostrare che $\boxed{\varphi \in T \Rightarrow \hat{v}(\varphi) = 1}$. ← induzione su φ usando le proprietà seguenti

Questo dipende dalla seguente lista di proprietà delle teorie coerenti.

PROPRIETÀ DELLE TEORIE COERENTI

Sia T coerente:

- se $\neg\neg\varphi \in T \Rightarrow T, \varphi$ è coerente

- se $\varphi \wedge \psi \in T \Rightarrow T, \varphi, \psi$ è coerente
- se $\neg(\varphi \wedge \psi) \in T \Rightarrow T, \neg\varphi$ è coerente o $T, \neg\psi$ è coerente
- se $\varphi \vee \psi \in T \Rightarrow T, \varphi$ coerente o T, ψ coerente
- se $\neg(\varphi \vee \psi) \in T \Rightarrow T, \neg\varphi, \neg\psi$ coerente
- se $\varphi \to \psi \in T \Rightarrow T, \neg\varphi$ coerente o T, ψ coerente
- se $\neg(\varphi \to \psi) \in T \Rightarrow T, \varphi, \neg\psi$ coerente

Si nota che se T è coerente massimale dire che T, α è coerente equivale a dire $\alpha \in T$.

verifico una delle tante:

$\varphi \vee \psi \in T \Rightarrow T, \varphi$ coerente o T, ψ coerente se $T, \varphi \vdash \bot$ e $T, \psi \vdash \bot$

$\Rightarrow T, \varphi \vee \psi \vdash \bot$

$\Rightarrow T$ incoerente

Usando le proprietà suddette ottengo $\varphi \in T \Rightarrow \hat{v}(\varphi) = 1$ per riduzione sul numero dei connettivi di φ.

ad es: se $\varphi = \alpha \vee \beta \in T \Rightarrow T, \alpha$ coerente o T, β coerente

$\Rightarrow \alpha \in T$ o $\beta \in T$ (per massimalità)

$\Rightarrow \hat{v}(\alpha) = 1$ o $\hat{v}(\beta) = 1$

induzione

$\Rightarrow \hat{v}(\alpha \vee \beta) = 1$

□

⑧ Ogni teoria coerente T ha un modello

dim: la estendo ad una $T' \supset T$ coerente massimale con Zorn.

Prendo modello v di T'. È anche modello di T.

⑨ $T \models \varphi \Rightarrow T \vdash_{DN} \varphi$

dim. Se $T \nvdash \varphi \Rightarrow T, \neg\varphi$ coerente $\overset{⑧}{\Rightarrow} T, \neg\varphi$ ha un modello v. $T \not\models \varphi$.

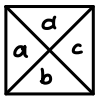
⑩ $T \vdash \varphi \Rightarrow T \models \varphi$ (correttezza)

⑪ T vuota:

$\vdash \varphi \iff \models \varphi$

$\iff \varphi$ è una tautologia

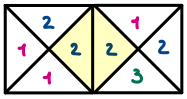
Tessere di Hao Wang (vedi Lemma di König e Tableaux)

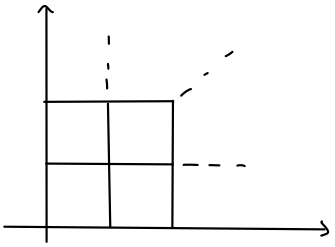
Piastrelle del tipo 

$a, b, c, d \in \{1, \dots, n\}$ (colori)

Abbiamo un numero finito di tipi di piastrelle

es:  etc. Infinite copie di ogni tipo.

Possiamo affiancarle se i colori combaciano: 



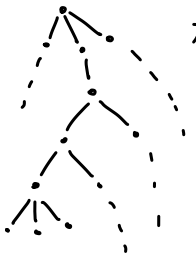
Scopo: Cercare di ricoprire tutto il piano

Ipotesi: I tipi di piastrelle sono tali che posso coprire un quadrante del piano.

Tesi: Si riesce a coprire il piano

2 dimostrazioni: ① lemma di König
② Teo di completezza proposizionale
} sostanzialmente si equivalgono

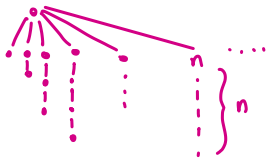
Lemma di König Se ho un albero infinito tale che ogni nodo ha un numero finito di figli/e



→ esiste un ramo infinito $(a_0, a_1, a_2, \dots)$

a_{n+1} figlio di a_n. $\forall n$

È necessario che l'albero abbia ramificazione finita se no:



Dim: È NECESSARIO l'assurdo

Costruisco induttivamente $a_0, \dots, a_n, \dots$ in modo che a_n abbia infiniti discendenti. a_0 = radice (che per ipotesi ha infiniti discendenti).

Se a_n ha infiniti discendenti e un numero finito di figli, uno dei figli ha infiniti discendenti e lo scelgo come a_{n+1}.

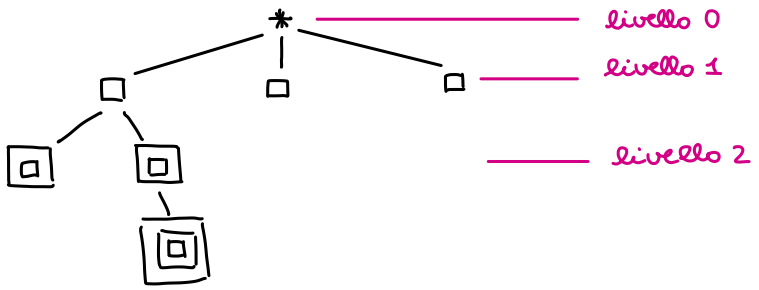
□

Torniamo alle tessere. L'ipotesi che posso coprire un quadrante

⇒ $\forall n$ posso coprire un quadrato $n \times n$

Definisco un albero: a livello n ci sono i ricoprimenti dei quadrati $2n-1 \times 2n-1$

I figli di un nodo X sono i ricoprimenti che estendono il ricoprimento associato ad X con una cornice concentrica.



Le ipotesi mi dicono che:

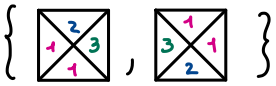
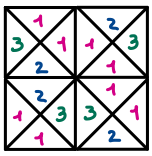
1) ad ogni livello c'è almeno un nodo (⇒ ci sono infiniti livelli non vuoti)

2) Ogni nodo ha un numero finito di figli
(perché ci sono un numero finito di tipi di tessere)

⇒ ∃ ramo infinito $(a_0, a_1, \dots)$ la cui "unione" è un ricoprimento del piano

(Non si possono ruotare o ribaltare le piastrelle)

2ª dimo. del problema di Hao Wang usando il teo di completezza proposiz.

es:  

22-10-2021 Lezione 8 Prof. Berarducci

Soluzione tessere di Hao Wang:

$\mathcal{B} = \{ \underset{t_1}{\boxtimes} \dots \underset{t_n}{\boxtimes} \}$ tipi di tessere

ipotesi: posso coprire un quadrante (quindi quadrati $n \times n$ $n \in \mathbb{N}$ arbitrario)

tesi Posso coprire il piano.

idea: introduco variabili proposizionali A_{ijt} tali che A_{ijt} "dice" che in posizione $i, j \in \mathbb{Z}$ (↪ Nota bene) c'è una tessera di tipo $t \in \mathcal{B}$.

Assiomi: $T_{\mathcal{B}} = \{ A_{ijt} \longrightarrow A_{i+1,j,t_1} \vee \dots \vee A_{i+1,j,t_K}$, etc $\}$ dove $t_1, \dots, t_K$ sono i tipi leciti a destra di t etc. = tutte le altre regole per la tassellazione corretta.

ad es. $A_{ijt} \rightarrow A_{i,j+1,t'_1} \vee \dots \vee A_{i,j+1,t'_n}$ dove $t'_1, \dots, t'_n$ sono i tipi leciti sopra t.
idem per sotto, sinistra

Devo anche dire: $A_{i,j,t} \rightarrow \neg A_{i,j,t'}$ se $t' \neq t$

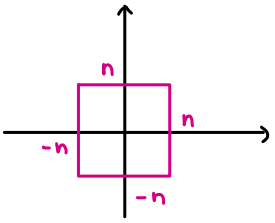
; $A_{ijt_1} \vee \dots \vee A_{ijt_s}$ dove $\{t_1, \dots, t_n\}$ = tutti i tipi possibili = $\mathcal{B}$

$Mod(T_{\mathbb{B}})$ sono in corrispondenza biunivoca con i ricoprimenti del piano leciti.

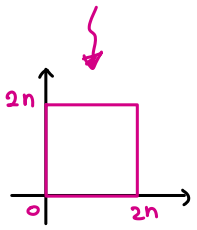
Se nel modello $v: Var \to \{0,1\}$ $v(A_{ijt}) = 1 \iff$ nel ricoprimento c'è il tipo t in posizione i,j.

Ora supponiamo che io possa coprire un quadrante. Voglio trovare un modello di $T_{\mathbb{B}}$ e da quello coprire il piano. Per il teo di compattezza esiste un modello di $T_{\mathbb{B}} \iff \forall S \underset{\text{finite}}{\subset} T_{\mathbb{B}}$ S ha un modello. Quindi devo mostrare che se prendo un sottoinsieme finito S di $T_{\mathbb{B}}$ ha un modello.

$\exists n$: S menziona solo le variabili A_{ijt} con $|i| \leq n$ $|j| \leq n$.



Se so coprire il quadrato $[-n, n] \times [-n, n]$ trovo un modello di S. Lo so fare perché nel quadrante trovo un ricoprimento del quadrato $[0, 2n] \times [0, 2n]$ e lo traslo.



Basta il teorema di compattezza proposizionale. (Non uso $\forall i, \forall j \ldots$)

Teorema di correttezza predicativo

$$\frac{P(x) \vdash P(x)}{P(x) \vdash \forall x\, P(x)}$$

Mostro che le regole sono corrette.

Inizio con la regola $\dfrac{T \vdash \varphi}{T \vdash \forall x \varphi}$ se x non compare libera in T. (ipotesi)

Dire che questa regola è corretta significa $T \vdash \varphi \Rightarrow T \vdash \forall x \varphi$ (tesi) dove

$T \vdash \varphi \iff Mod(T) \subset Mod(\varphi)$, $Mod(\varphi) = \{(M, v) \mid M, v \vdash \varphi\}$ v: variabili $\to M$

($M, v \vdash \varphi \leftrightarrow \varphi^{M,v} = 1$ (vero))

$Mod(T) = \bigcap_{\theta \in T} Mod(\theta)$

Suppongo $T \vdash \varphi$. Mostro $T \vdash \forall x \varphi$. Prendo $(M, v) \vdash T$ devo far vedere che $M, v \vdash \forall x \varphi$ $(M \vdash \varphi(v))$.

$M, v \vdash \forall x \varphi \underset{\text{Tarski}}{\longleftrightarrow} \forall a \in M \quad M, v[a/x] \vdash \varphi$

(v è un nuovo ambiente)

Sapevo che $T \vdash \varphi$ quindi $(M, w) \vdash T \Rightarrow (M, w) \vdash \varphi$ ($(M,w) \vdash T$: vera)

siccome $x \notin VL(T)$ e $M, v \vdash T \Rightarrow M, w \vdash T$ (↕ esercizio)

Concludo $(M, w) \vdash \varphi$ □

correttezza regola: $\dfrac{T \vdash \forall x \varphi}{T \vdash \varphi[t/x]}$ con t sostituibile per x in φ

devo mostrare $T \vDash \forall x \varphi \Rightarrow T \vDash \varphi[t/x]$.

Lemma (V1): $\varphi[t/x]$ dice di t ciò che φ dice di x (serve t sostituibile)

↳ cos'è che φ dice di x?

Notazione: $VL(\varphi) = \{x_1, \dots, x_n\}$ $\quad a_1, \dots, a_n \in M$

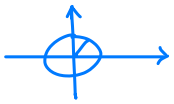
$M \vDash \varphi(a_1/x_1, \dots, a_n/x_n) \Leftrightarrow M \vDash \varphi(v)$ dove $v(x_i) = a_i$

Lemma (V2): $\forall$ M L-struttura, v ambiente (V2 più precisa di V1)

$P = \{a \in M \mid \varphi(v[a/x])\}$ $\quad VL(\varphi) = \{x, y_1 \dots y_n\}$

$\varphi(a/x, b_1/y_1 \dots b_n/y_n)$ $\quad v(x) = a$, $v(y_i) = b_i$

P è un sottoinsieme di M definibile con parametri $b_1, \dots, b_n$

ES $\{(x,y) \mid x^2 + y^2 = \pi^2\} \subset \mathbb{R}^2$  cerchio di raggio π $\subset \mathbb{R}^2$

è definibile in $M = (\mathbb{R}, +, \cdot, 0, 1)$ con parametro π. ↳ me lo fornisce l'ambiente

Sia $a = t^{M,v} \in M$ $\quad M \vDash \varphi[t/x](v) \Leftrightarrow M \vDash \varphi(v[a/x])$ (*) $\quad \Leftrightarrow a \in P$ $\Leftrightarrow t^{M,v} \in P$

↳ se t è sostituibile

Dim Bisogna definire per bene induttivamente $\varphi[t/x]$

- $(\alpha \wedge \beta)[t/x] = \alpha[t/x] \wedge \beta[t/x]$
- $(\forall x \alpha)[t/x] = (\forall x \alpha)$
- $(\forall y \alpha)[t/x] = \forall y (\alpha[t/x])$ se y è una variabile diversa da x
- etc

Nel caso atomico $[t/x]$ significa letteralmente che sostituisco x con t ovunque trovo x.

Dimostro il caso speciale della (*).

$\varphi = \forall y \alpha$

$M \vDash (\forall y \alpha)[t/x](v)$ Vale questo

$\leftrightarrow M \vDash \forall y\, (\alpha[t/x])(v)$ def di $[t/x]$

$\leftrightarrow \forall b \in M \quad M \vDash \alpha[t/x](v[b/y])$

$\leftrightarrow \forall b \in M \quad M \vDash \alpha(v[b/y, a/x])$

↓ induttiva della (*)

$a = t^{v[b/y]} \overset{(*)}{=} t^{M,v}$ (*) $y \notin VL(t)$ → { perché t è sostituibile per x in $\varphi = \forall y \alpha$

$\leftrightarrow \forall b \in M \quad M \models \alpha(v[^a/_x, {}^b/_y])$

$\leftrightarrow M \models (\forall y \alpha) v[a/x]$ sse vale questo

che è quello che volevo.

Ora è immediato che $(M,v) \models \forall x \varphi \Rightarrow (M,v) \models \varphi[t/x]$ se t è sostituibile.

Dim. $M, v \models \forall x \varphi \Rightarrow \forall b \quad M, v[^b/_x] \models \varphi$

se prendo come b proprio $t^{M,v}$ ottengo per ie lemma di prima:

$$M, v \models \varphi[t/x]$$

Corollario: $\models \forall x \varphi \rightarrow \varphi[t/x]$ per t sostituibile.

Il teorema di correttezza $T \vdash \varphi \Rightarrow T \models \varphi$ segue facilmente.

Verifico la correttezza di $\dfrac{T \vdash \forall x \varphi}{T \vdash \varphi[t/x]}$ t sostituibile.

Suppongo $T \models \forall x \varphi$. Mostro $T \models \varphi[t/x]$. Prendo $(M,v) \models T$ devo mostrare $(M,v) \models \varphi[t/x]$. So che $M, v \models \forall x \varphi$. Quindi $\forall b \in M$, $M, v[b/x] \models \varphi$.

Prendo $b = t^{M,v}$, ho $(M,v) \models \varphi[t/x]$. □

Analogamente verifico la correttezza delle altre regole.

Teo $T \vdash_{DN} \varphi \Rightarrow T \models \varphi$

Dim: Induzione sul numero dei passaggi usati per ottenere $T \vdash_{DN} \varphi$ usando la correttezza delle regole.

Completezza: $T \models \varphi \rightarrow T \vdash \varphi$

Mi riduco a:

Lemma: T coerente $(T \not\vdash \bot) \rightarrow T$ ha un modello

La completezza segue dal lemma: se $T \not\vdash \varphi \Rightarrow T, \neg\varphi$ coerente

$\Rightarrow T, \neg\varphi$ ha un modello $M \Rightarrow T \not\models \varphi$

Manca il lemma

idea: Sia T coerente. Ingrandisco T per farla diventare di "Hintikka", poi trovo il modello.

"Teorie di Hintikka"

L-teoria T è di Hintikka se contiene solo termini chiusi e:

- $\varphi \in T \Rightarrow \neg\varphi \notin T$
- $\neg\neg\varphi \in T \Rightarrow \varphi \in T$
- $\varphi \wedge \psi \in T \Rightarrow \varphi \in T$ e $\psi \in T$
- $\varphi \vee \psi \in T \Rightarrow \varphi \in T$ o $\psi \in T$
- $\neg(\varphi \wedge \psi) \in T \Rightarrow \neg\varphi \in T$ o $\neg\psi \in T$
- $\neg(\varphi \vee \psi) \in T \Rightarrow \neg\varphi \in T$ e $\neg\psi \in T$
- $\varphi \to \psi \in T \Rightarrow \neg\varphi \in T$ o $\psi \in T$
- $\neg(\varphi \to \psi) \in T \Rightarrow \varphi \in T$ e $\neg\psi \in T$
- $\forall x\,\varphi \in T \Rightarrow$ per ogni t chiuso $\varphi[t/x] \in T$
- $\exists x\,\varphi \in T \Rightarrow$ esiste un termine chiuso $\varphi[t/x] \in T$
- $\neg\forall x\,\varphi \in T \Rightarrow$ esiste t chiuso $\neg\varphi[t/x] \in T$
- $t \doteq t \in T$ se t chiuso
- $t \doteq q \in T$, $\varphi[t/x] \in T \Rightarrow \varphi[q/x] \in T$

Teo: Ogni teoria di Hintikka ha un modello

esempi: 1) $L = \{P, Q\}$ $\quad T = \{\exists x\,[P(x) \vee Q(x)]\}$

ha un modello? Sì ma non è di Hintikka: non mi dice chi è il modello.

Rendiamola di Hintikka: espandiamo il linguaggio

$L = \{P, Q, a\}$ $\quad T = \{\exists x\,[P(x) \vee Q(x)], P(a) \vee Q(a)\}$

Non è ancora di Hintikka

Mi dice che vale $P(a) \vee Q(a)$ ma non mi dice nessuno dei due.

Per renderla di Hintikka decidiamo noi quale far valere:

$T = \{\exists x\,[P(x) \vee Q(x)], P(a) \vee Q(a), P(a)\}$ Ora è di Hintikka (senza $\doteq$)

2) Estendere a una teoria di Hintikka la teoria:

$T = \{ \exists x\, P(x),\ \forall x (P(x) \to \exists y\, \neg Q(x,y)),\ \forall x (P(x) \to Q(x,x)) \}$

estendo T a T' di Hintikka

1) $\exists x\, P(x) \Rightarrow$ devo avere un termine chiuso $\Rightarrow$ aggiungo $P(a)$

2) $\forall x\, P(x) \Rightarrow$ deve valere $\forall$ t. chiuso $\Rightarrow$ aggiungo $\underbrace{P(a)}_{A} \to \underbrace{\exists y\, \neg Q(a,y)}_{B}$

3) Ora ho due scelte: poiché ho $A \to B$ devo aggiungere o $\neg A$ o B, dunque $\neg P(a)$ oppure $\exists y\, \neg Q(a,y)$, ma chiaramente (per il punto ①) non posso aggiungere $\neg P(a) \Rightarrow$ aggiungo $\exists y\, \neg Q(a,y)$

4) Poiché ho aggiunto y $\Rightarrow$ devo avere almeno un termine <u>diverso</u> da a perché entrerebbe in contraddizione con gli assiomi $\Rightarrow$

$\Rightarrow$ aggiungo $\neg Q(a,b)$.

5) $\forall x (P(x) \to Q(x,x)) \Rightarrow$ devo aggiungere o $\neg P(a)$ o $Q(a,a)$

ma di nuovo non posso mettere $\neg P(a) \Rightarrow$ aggiungo $Q(a,a)$

6) $T' = T \cup \{ P(a),\ P(a) \to \exists y\, \neg Q(a,y),\ \exists y\, \neg Q(a,y),\ \neg Q(a,b),$

$P(a) \to Q(a,a),\ Q(a,a),\ P(b) \to \exists y\, \neg Q(b,y),$

$P(b) \to Q(b,b),\ \neg P(b) \}$

Questa teoria è di Hintikka.

<u>Domanda</u>: Come trovo un modello M di T'?

$dom(M) = \{a,b\}$ come interpreto P, Q in M?

$P^M = \{a\} \subset M$ predicato unario (sottoinsieme del dominio)

$Q^M = \{\langle a,a \rangle\} \subset M^2$ predicato binario (insieme di coppie)

Questo M è un modello.

Ricapitoliamo: Siamo partiti da un insieme T e estendendolo ad una teoria di Hintikka siamo riusciti a trovare un modello

Strategia: Guardo le formule atomiche, tutte le altre formule "vengono gratis". Unica eccezione: $\forall$.

25-10-2021 Lezione 9 Prof. Berarducci

① Ogni teoria di Hintikka ha un modello

② Ogni teoria coerente si estende a una di Hintikka

↓

③ Ogni teoria coerente ha un modello

④ $T \models \varphi \Leftrightarrow T \vdash \varphi$ completezza

Hintikka: se c'è una formula ci sono altre formule più semplici che la semplificano (tranne il caso $\forall, \neg\exists$)

Esempio: se $\alpha \vee \beta \in T \Rightarrow \alpha \in T$ o $\beta \in T$ e ovviamente $\alpha \vdash \alpha \vee \beta$, $\beta \vdash \alpha \vee \beta$

nel caso del $\forall$ $\forall x\, \varphi \in T \Rightarrow$ per ogni t termine chiuso $\varphi[t/x] \in T$

però ovviamente $\varphi[t/x], \varphi[t'/x], \dots, \varphi[t''/x] \not\vdash \forall x\, \varphi$ perché non posso escludere di avere strutture con elementi del dominio senza "nome".

Def. (Struttura ricca)

M L-Struttura è ricca se $\forall a \in M$ esiste un L-termine chiuso t tale che $a = t^M$.

Esempio: $(\mathbb{N}, 0, S, +, \cdot)$ è ricca

$(\mathbb{R}, 0, S, +, \cdot)$ non è ricca: $\sqrt{2} \in \mathbb{R}$ ma non c'è un termine del linguaggio per indicarlo

Teorema: T L-teoria di Hintikka

$\Rightarrow T$ ha un modello M (ricco)

Dim. $\mathrm{dom}(M) = \{[t] \mid t$ L-termine chiuso$\}$

$[t]$ = classe di equivalenza di t modulo la relazione di equivalenza E definita da $t_1 E t_2 \Leftrightarrow t_1 \doteq t_2 \in T$.

Devo verificare che E è di equivalenza/congruenza

- $t \doteq t \in T$
- $t_1 \doteq t_2 \in T \Rightarrow t_2 \doteq t_1 \in T$
- $t_1 \doteq t_2 \in T$, $t_2 \doteq t_3 \in T \Rightarrow t_1 \doteq t_3 \in T$

- $t_1 \doteq t_1' \in T, \dots, t_n \doteq t_n' \in T$, $f \in L$ funzione $\Rightarrow f(t_1, \dots, t_n) \doteq f(t_1', \dots, t_n') \in T$

Verificare per esercizio.

Fatte queste verifiche devo scegliere come interpretare in $M = \{[t] \mid t \text{ chiuso}\}$ i simboli di L. Si fa la cosa ovvia:

Se $c \in L$ costante:

- $c^M = [c]$
- $f \in L$ funzione n-aria $f^M : M^n \to M$, $f^M([t_1], \dots, [t_n]) = [f(t_1 \dots t_n)]$ (↑ è congruenza)
- $R \in L$ relazione n-aria

  $R^M \subset M^n$ $\quad R^M = \{\langle [t_1], \dots, [t_n] \rangle \mid R(t_1, \dots, t_n) \in T\}$

Oss. Per induzione M è una L-struttura ricca.

Oss. $[t] \in M \Rightarrow [t] = t^M$ (ovvio se t è un simbolo di costante)

Se $t = f(t_1, \dots, t_n)$

$$t^M \underset{\text{Tarski}}{=} f^M(t_1^M, \dots, t_n^M) \underset{\text{induzione}}{=} f^M([t_1], \dots, [t_n]) \underset{\text{def } f^M}{=} [f(t_1, \dots, t_n)] = [t].$$

M è chiamato modello dei termini.

Devo mostrare che $M \vDash T$. Cioè per ogni φ chiusa $\in T$ $M \vDash \varphi$ (φ vera in M)

Induzione sul numero di connettivi di φ.

Caso $\varphi = \alpha \vee \beta$

$\varphi \in T \Rightarrow \alpha \in T \circ \beta \in T$

$$\underset{\text{ind}}{\Rightarrow} M \vDash \alpha \circ M \vDash \beta \underset{\text{Tarski}}{\Rightarrow} M \vDash \alpha \vee \beta$$

Caso $\varphi = \forall x \theta \in T$ per ogni t chiuso $\theta[t/x] \in T$

$\underset{\text{induz.}}{\Rightarrow}$ $M \vDash \theta[t/x]$ $\forall t$ chiuso

$\Rightarrow$ $\forall a \in M$ $M \vDash \theta(a/x)$ (ambiente) perché essendo M ricco, $a = t^M$ per qualche t.

(non più chiusa)

Serve anche il lemma $M \vDash \theta[t/x] \Leftrightarrow M \vDash \theta(a/x)$ dove $a = t^M$

Alcune verifiche

$t_1 \doteq t_2 \in T \Rightarrow t_2 \doteq t_1 \in T$

per def. di Hintikka: $\left.\begin{array}{l} t_1 \doteq t_2 \in T \\ \theta[t_1/t_2] \in T \end{array}\right\} \Rightarrow \theta[t_2/x] \in T$

$\theta = (x \doteq t_1)$

$\theta[t_1/x] = (t_1 \doteq t_1) \in T$ le altre verifiche per esercizio

$\theta[t_2/x] = (t_2 \doteq t_1) \in T$

Digressione:

Teoria degli ordini stretti $L = \{<\}$

$T = \{\forall x \ \neg(x<x), \forall xyz \ x<y \wedge y<z \rightarrow x<z\}$

$T, a<b \vdash b \nless a$ lo voglio fare con "passaggi stile Hintikka"

Basta mostrare che negando la tesi ho una teoria contraddittoria

$T, a<b, b<a$

$\neg(a<a)$

$a<b \wedge b<a \rightarrow a<a$

oppure

$\neg(a<b \wedge b<a)$ $\quad$ ~~$a<a$~~ escluso

o

~~$\neg(a<b)$~~ escluso $\quad$ ~~$\neg(b<a)$~~ escluso

$\Rightarrow$ tutte le strade per costruire un modello di $T, a<b, b<a$ si chiudono. Quindi non ci sono modelli. Quindi $T, a<b \vdash \neg(b<a)$

② **Teorema** (LEMMA DI LINDEMBAUMM) Ogni L-teoria coerente T si estende a una teoria coerente massimale T' nello stesso linguaggio L dim: come nel caso proposizionale (Zorn)

Nota: T' non è detto sia di Hintikka o che abbia un modello ricco.

esempio $T' = \{\varphi \mid \varphi \text{ vera in } (\mathbb{R}, +, \cdot, 0, 1)\}$

T' non è di Hintikka: $\exists x (x \cdot x = 1+1) \in T'$ però non c'è un termine chiuso t in $L = \{0, 1, +, \cdot\}$ con $(t \cdot t \doteq 1+1) \in T'$

COSTANTI DI HENKIN

Lemma (di Henkin) T L-teoria, C nuova costante $\notin L$ sia φ una L-formula

$VL(\varphi) \subseteq \{x\}$. Supponiamo che T sia coerente $\Rightarrow T \cup \{\exists x \varphi \to \varphi[c/x]\}$ è coerente

Oss a livello semantico è ovvio che se T ha un modello anche

$T \cup \{\underbrace{\exists x \varphi \to \varphi[c/x]}_{\exists x \varphi(x) \to \varphi(c)}\}$ lo ha

$\varphi[x/x]$

Dim. Sia $M \models T$. M è una L-struttura. La voglio espandere a una $L \cup \{c\}$ struttura modello di $T \cup \{\exists x \varphi \to \varphi[c/x]\}$

Caso 1 $M \not\models \exists x \varphi$. Interpreto c come voglio

Caso 2 $\exists a \in M$ $M \models \varphi(a/x)$. Interpreto c come a.

LEMMA DELLE COSTANTI

$T \vdash \varphi[c/x]$ c simbolo di costante non in T $\Rightarrow T \vdash \forall x \varphi$ (T consiste di formule chiuse)

Dim: esiste $T' \subset T$ finito $T' \vdash \varphi[c/x]$
(compattezza sintattica)

Sia y variabile che non compare in T'. Rimpiazzando nella dimostrazione di $T' \vdash \varphi[c/x]$ c con y ottengo una dimostrazione di $T' \vdash \varphi[y/x]$.

Per la regola $\forall$-introduzione $T' \vdash \forall y \varphi[y/x] \Rightarrow T' \vdash \varphi[x/x]$ cioè

$T \vdash \varphi \Rightarrow T \vdash \forall x \varphi$. □

Nota serve che c non stia in T se no $\dfrac{T(c) \vdash \theta(c,y)}{T(c) \vdash \forall y \theta(c,y)}$ legale,

ma $\dfrac{T(y) \vdash \theta(y,y)}{T(y) \vdash \forall y \theta(y,y)}$ illegale.

Def Una L-formula si chiama tautologia predicativa se si ottiene da una tautologia proposizionale per sostituzione di variabili prop. con formule.

Esempio $A \vee \neg A$ tautologia proposizionale

$\forall x (x < x) \vee \neg \forall x (x < x)$ tautologia predicativa

Ho già dimostrato $T \models \varphi \Leftrightarrow T \vdash \varphi$ nel caso proposizionale. In particolare

$\models \varphi \Leftrightarrow \vdash \varphi \Leftrightarrow \varphi$ taut. proposizionale.

Rimane vero anche per φ tautologia predicativa.

φ taut. predicativa $\Rightarrow \vdash_{DN} \varphi$

es: $\vdash \forall x\,(x < x) \vee \neg \forall x\,(x < x)$

Torniamo al lemma di Henkin:

T coerente $\Rightarrow T \cup \{\exists x\,\varphi \to \varphi[c/x]\}$ coerente

c non compare in T, φ.

Dim. Se per assurdo, $T \vdash \neg(\exists x\,\varphi \to \varphi[c/x])$

$\vdash \neg(\exists x\,\varphi \to \varphi[c/x]) \to \exists x\,\varphi \wedge \neg\varphi[c/x]$ perché è una tautologia

$\Rightarrow T \vdash \exists x\,\varphi$, $T \vdash \neg\varphi[c/x]$

$\Rightarrow$ lemma delle costanti $T \vdash \forall x\,\neg\varphi$ per $T \vdash \forall x\,\neg\varphi \to \neg\exists x\,\varphi$ (per un esercizio svolto)

quindi $T \vdash \exists x\,\varphi$ $T \vdash \neg\exists x\,\varphi \Rightarrow T \vdash \bot$ Assurdo.

Def T è una L-teoria di Henkin se per ogni L-formula chiusa $\exists x\,\varphi$ esiste una costante $c \in L$ tale che $T \vdash \exists x\,\varphi \to \varphi[c/x]$ (e T è coerente)

Teo ogni L-teoria T coerente si estende a una $T' \supset T$ coerente di Henkin in un linguaggio $L' \supset L$

Dim: Per ogni L-formula $\exists x\,\varphi$ inventiamoci una nuova costante c_φ.

$T^* = T \cup \{\exists x\,\varphi \to \varphi[c_\varphi/x] \mid \varphi$ L-formula$\}$.

T^* è coerente: compattezza + lemma di Henkin

Ora sia $T_0 = T$, $T_1 = T^*$, , $T_{n+1} = T_n^*$

$T' = \bigcup_{n \in \mathbb{N}} T_n$. T' è coerente di Henkin. Infatti qualsiasi formula $\exists x\,\Theta$ in $L(T')$ sta già in $L(T_n)$ per qualche n e la sua costante c_Θ sarà in $L(T_{n+1}) \subset L(T')$.

Lemma Ogni L-teoria coerente T è contenuta in una teoria coerente massimale e di Henkin in un linguaggio $L' \supset L$.

dim. Prima ottengo $T' \supset T$ di Henkin coerente in $L' \supset L$, poi estendo T' a una coerente massimale $T'' \supset T$ nello stesso linguaggio e osservo che

rimane di Henkin. □

Vedremo che T coerente massimale di Henkin

→ T di Hintikka

→ ha un modello

Quindi ogni teoria coerente ha un modello.

→ $T \models \varphi \leftrightarrow T \vdash \varphi$

29-10-2021 Lezione 10 Prof. Berarducci

Teorema: Ogni L-teoria coerente massimale di Henkin è di Hintikka.

Ripasso:
- coerente massimale ⇒ completa
- completa ⇒ i suoi teoremi sono una teoria coer. mass.
- teoria di Henkin: se ho $\exists x \varphi \Rightarrow T \vdash \exists x \varphi \to \varphi[^c/_x]$
- teoria di Hintikka: lunga serie di clausole
- coerente massimale ⇒ Hintikka
- Hintikka ⇏ completa

Hintikka → dice tutto ma solo sulle sottoformule della teoria

Dim: T L-teoria coerente massimale.

Verifico alcune clausole della definizione di teoria

(∨) $\alpha \vee \beta \in T$, voglio $\alpha \in T \vee \beta \in T$. Se così non fosse poiché è coerente massimale $\neg\alpha \in T$, $\neg\beta \in T$, ma T coerente quindi T non può contenere $\alpha \vee \beta, \neg\alpha, \neg\beta$ dim: con le tavole di verità si vede subito ma vogliamo adoperare le regole di inferenza

$$\frac{T, \alpha \vdash \bot \qquad T, \beta \vdash \bot}{T, \alpha \vee \beta \vdash \bot} \quad (\text{perché } \neg\alpha \in T, \neg\beta \in T) \Rightarrow T \vdash \bot$$

Assurdo perché T è coerente.

(∧) $\alpha \wedge \beta \in T \Rightarrow \alpha \in T$ e $\beta \in T$

dim: se così non fosse $\alpha \notin T$ o $\beta \notin T$ ma allora poiché

T coer. massimale avrei: $\neg\alpha \in T$ o $\neg\beta \in T$

CASO 1 / CASO 2

$\alpha \wedge \beta, \neg\alpha \vdash \bot$ infatti

$\alpha \wedge \beta \vdash \alpha$ e $\alpha \wedge \beta, \neg\alpha \vdash \alpha, \neg\alpha \vdash \bot$

$T \vdash \bot \Rightarrow T$ incoerente

Similmente se $\neg\beta \in T$ ottengo $T \vdash \bot$

In ogni caso ottengo un assurdo perché T incoerente.

(∃) $\exists x \varphi \in T$ Voglio trovare $c \in L$ costante $\varphi[c/x] \in T$

So che T è di Henkin, quindi $\exists x \varphi \to \varphi[c_\varphi/x] \in T$, inoltre $\exists x \varphi \in T$. Dico che $\varphi[c/x] \in T$.

Se per assurdo $\varphi[c/x] \notin T$ avrei $\neg\varphi[c/x]$ (T coer. mas.).

Avrei $\exists x \varphi \to \varphi[c/x]$, $\exists x \varphi$, $\neg\varphi[c/x] \in T$. Attraverso le regole proposizionali ottengo un assurdo (T contraddittoria)

$$\dfrac{\dfrac{\exists x \varphi \to \varphi[c/x] \qquad \exists x \varphi}{\varphi[c/x]} \qquad \neg\varphi[c/x]}{\bot}$$

$T \vdash \bot$ ↯

Sto dimostrando che le teorie coerenti massimali sono chiuse per deduzione.

(∀) $\forall x \varphi \in T$ sia t termine chiuso.

Voglio mostrare $\varphi[t/x]$.

$$\dfrac{T \vdash \forall x \varphi}{T \vdash \varphi[t/x]}$$

T coerente $T \vdash \varphi[t/x] \Rightarrow T, \varphi[t/x]$ coerente $\overset{\text{per massimalità}}{\Longrightarrow} \varphi[t/x] \in T$

Analogamente si svolgono le altre verifiche.

Teorema T coerente $\Rightarrow$ T ha un modello

Dim: estendo T a una teoria di Henkin $T' \supset T$, $L(T') \supset L(T)$ (↓ aggiungo le costanti di Henkin)

estendo T' a un $T'' \supset T'$ $\quad \underbrace{L(T'')}_{L''} = L(T')$

T" ricade di Henkin $\Rightarrow$ T" è di Hintikka

$\Rightarrow$ T" ha il modello dei termini M (quozientati)

M è una L" struttura.
$M_{|L}$ è una L-struttura. (↳ restrizione)

$\left.\begin{array}{l} M \text{ è una } L'' \text{ struttura.} \\ M_{|L} \text{ è una } L\text{-struttura.} \end{array}\right\} M \models T'' \Rightarrow M \models T \Rightarrow M_{|L} \models T$

□

Teo: $T \models \varphi \Rightarrow T \vdash \varphi$

Dim: $T \not\vdash \varphi \Rightarrow T, \neg\varphi$ coerente

$\Rightarrow T, \neg\varphi$ ha modello M

$\Rightarrow T \not\models \varphi$

Già conoscevamo la correttezza: quindi $T \models \varphi \Leftrightarrow T \vdash \varphi$

Calcolo la cardinalità del modello dei termini:

T coerente L-teoria

Per farla diventare di Henkin T' quante costanti devo aggiungere?

$T' = \bigcup_{n\in\mathbb{N}} T_n \qquad T_0 = T$

$T_{n+1} = T_n \cup \{ \exists x\, \varphi \to \varphi[c_\varphi / x] \mid \varphi \in L(T_n) \}$ (aggiungo tante costanti quante sono le formule di T_n)

$|L(T_{n+1})| = |L(T_n)| + |\{ c_\varphi \mid \varphi \in L(T_n) \}| = (*)$

Digressione (ETI): Σ alfabeto, $\Sigma^* = \bigcup_{n\in\mathbb{N}} \Sigma^n$

Che rapporto c'è tra $|\Sigma|$ e $|\Sigma^*|$?

Se $|\Sigma| \le \alpha$ con α cardinale infinito $\Rightarrow \alpha \cdot \alpha = \alpha$

$\Rightarrow |\Sigma^n| = |\Sigma|$ se Σ infinito

Chiamo $\alpha = \max(|\Sigma|, \aleph_0)$. $\alpha \ge \aleph_0$

Per induzione $|\Sigma^n| \le \alpha \Rightarrow |\bigcup_{n\in\mathbb{N}} \Sigma^n| \le \aleph_0 \cdot \sup_n |\Sigma^n| \le \aleph_0 \cdot \alpha = \alpha$ (↑)

Oss: Se $|L| = \beta \Rightarrow |L\text{-formule}| = \max(\aleph_0, \beta)$

Dopo questa digressione possiamo fare le stime:

$(*) = |L(T_n)| + \max(\aleph_0, |L(T_n)|)$

Se $|L(T_0)| = \alpha \Rightarrow |L(T')| = \max(\alpha, \aleph_0) = \alpha \cdot \aleph_0$

(per ind. si dimostra $|L(T_n)| \leq \max(\alpha, \aleph_0)$)

Nel passaggio tra T coerente e la sua estensione T' di Henkin la cardinalità dell'insieme delle formule non cambia.

$|L| = \alpha \Rightarrow |L\text{-formule}| = \max(\alpha, \aleph_0)$ nel passaggio da T' alla sua estensione coerente massimale T'' il linguaggio rimane lo stesso.

$|\text{Modello dei termini di } T| = |\text{termini di } T''| \leq \max(\alpha, \aleph_0) = \max(|L(T)|, \aleph_0)$

Cor Ogni teoria coerente al più numerabile (cioè con un linguaggio di card $\leq \aleph_0$) ha un modello numerabile.

Questo è il Teorema di Löwenheim-Skolem, forma debole.

Es ZF (Teoria degli insiemi), $Th(\mathbb{R}, 0, 1, +, \cdot, \leq) = \{\varphi \text{ chiusa} \mid \mathbb{R} \models \varphi\}$ (Teoria completa dei numeri reali)

Questa è assiomatizzata dagli:

- assiomi dei campi ordinati;
- ogni polinomio che cambia segno ha uno zero: servono più assiomi

$$\forall a,b \ \exists x \ a + bx + x^2 > 0 \qquad \exists x' \ a + bx + x^2 < 0 \Rightarrow \exists x \ a + bx + x^2 = 0 \quad \dots$$

C'è un assioma per ogni grado!

$Th(\mathbb{R}, 0, 1, +, \cdot, <)$ ha un modello ovvio (cioè $\mathbb{R}$) ma per il teo appena dimostrato deve anche avere un modello numerabile. Com'è fatto?

Cerchiamo di costruirlo come per Henkin (oss: non è unico)

Preludo ad es: $\exists x \ (x^2 = 1 + 1) \in T \Rightarrow$ aggiungo $\sqrt{2}$ al modello, non serve ad esempio aggiungere π (difficile da descrivere in formule)

Un possibile modello numerabile è dato dai reali algebrici:

$$A = \{\alpha \in \mathbb{R} \mid \exists\, p(x) \in \mathbb{Q}[x] \setminus \{0\} \text{ tc } p(\alpha) = 0\}$$

Tarski Ogni formula di $Th(\mathbb{R}, +, \cdot, 0, 1)$ equivale a una formula senza quantificatori.

ad es: $\exists x\,(x^2+bx+c=0) \leftarrow \varphi(x,b,c)$

$\updownarrow$ $\qquad$ $\updownarrow T_{\mathbb{R}}$

$\Delta \geq 0 \qquad b^2-4c \geq 0$

↳ serve il $\leq$ per eliminare $\forall, \exists$

$\Rightarrow x \geq 0 \leftrightarrow \exists y\,(x=y^2)$

es: $\exists xy \left(x \neq 0 \vee y \neq 0 \;\wedge\; \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right)$

$\updownarrow$ $\qquad$ $ax+by=0 \wedge$

$ad-bc=0$ $\qquad$ $cx+dy=0$

se il det $=0$

ZF (se coerente) ha un modello numerabile (discussione postposta)

Teorema (Löwenheim - Skolem verso l'alto (debole))

Se T ha un modello infinito, allora per ogni cardinale K ha un modello di cardinalità $\geq K$

ES PA ha un modello di cardinalità $2^{\aleph_0} = |\mathbb{R}|$

Si possono indebolire le ipotesi:

Teo (L.S.↑) Se $\forall n \in \mathbb{N}$ T ha un modello di card $\geq n$ (non per forza infinito)

$\Rightarrow \forall K$ cardinale T ha modello di card $\geq K$

Dim: Assumo $\forall n$ T ha un modello M_n di card $\geq n$. $L^* = L \cup \{c_i \mid i \in K\}$ (K nuove cost. $\neq$)

Sia $T^* = T \cup \{c_1 \neq c_j \mid \text{per } i \neq j \text{ in } K\}$.

Dico che T^* è coerente per compattezza.

Infatti $S \subseteq_{\text{finita}} T^*$, S menziona un numero finito di nuove costanti, diciamo $c_1, \dots, c_n \in K$. $S \subseteq T \cup \{c_1 \neq c_2, c_1 \neq c_3, c_1 \neq c_3, \dots, c_1 \neq c_n\}$

Un modello di S è facile da trovare: prendo un modello M_n di T con $\geq n$ elementi $a_1, \dots, a_n \in \text{dom}(M_n)$ NB: $L \subseteq M_n) = L$

Sia $\hat{M}_n$ = l'espansione di M_n nel linguaggio $\hat{L} = L \cup \{c_1, \dots, c_n\}$ che interpreta c_i con a_i.

$\hat{M}_n \models T \cup \{c_i \neq c_j \mid \text{per } i,j \leq n\} \Rightarrow \hat{M}_n \models S$. Quindi T^* è coerente.

Quindi ha un modello M e $|M| \geq K$ perché deve verif. gli assiomi $c_i \neq c_j$ $i \neq j$ in K

$M|_{L(T)} \models T$ dove $M|_{L(T)} = \text{dom } M$ quindi ho un modello di T di card $\geq K$

Controesempio: $Th(\mathbb{Z}/(2)) = \{\varphi \mid \mathbb{Z}/(2) \models \varphi\}$ $\quad L = \{0, 1, +, \cdot\}$

$M \models Th(\mathbb{Z}/(2)) \Rightarrow |M| = 2$ o meglio $M \cong \mathbb{Z}/(2)$ (c'è un'unico modello a meno di iso)

$Th(\mathbb{Z}/(2)) \vdash \exists x\, y\, (x \neq y \wedge \forall z\, z \doteq x \vee z \doteq y)$

$\Rightarrow$ Qualunque modello deve avere due e due soli elementi.

Esempio: T = Teoria dei campi finiti $= \{\varphi \mid \forall F$ campo finito $F \models \varphi\}$ non è completa ma è interessante

esiste un campo infinito K che è un modello di questa teoria.

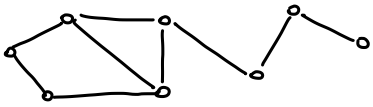
$\mathbb{Z}/(2) \models T$, $\mathbb{Z}/(3) \models T$, ...

$\prod_{p \in U} \mathbb{Z}/(p)/U \models T$ Richiede conoscenze algebriche, vediamo un altro esempio

$\prod_{p \in U}$ → ultraprodotto, U → ultrafiltro

ESEMPIO:

GRAFI CONNESSI



connesso

non connesso

$L = \{E\}$ $\quad E(x,y)$ x è adiacente a y

Grafi non diretti: $E(x,y) \leftrightarrow E(y,x)$, senza loop: $\neg E(x,x)$

connesso (non lo possiamo dire con la logica del 1° ordine): $\forall x, y\ \exists n \in \mathbb{N}\ \exists \langle a_0, \dots, a_n \rangle, x = a_0 \bigwedge_{i<n} E(a_i, a_{i+1})\ y = a_n$ → sto quantificando su successioni finite

Non esiste alcuna L-teoria T : $Mod(T) =$ Grafi connessi

Riesco a fare $\subseteq$ non $=$ ↑ assioma $\forall x y\, E(x,y)$

Per assurdo sia T tale che $Mod(T) =$ Grafi connessi (non diretti)

$L' = \{E, a, b\}$ $\quad a, b$ costanti

$T' = T \cup \{ a \neq b, \neg E(a,b), \neg\exists x\ E(a,x) \wedge E(x,b)$
$\neg\exists xy\ E(a,x) \wedge E(x,y) \wedge E(y,b), \text{etc} \}$

↗ l'n-esimo assioma dice che $dist(a,b) \geq n$

T' è coerente per compattezza

Se prendo un numero finito di assiomi di $T' \Rightarrow \exists n$ $T \cup \{ dist(a,b) \geq n \}$

Come modello prendo un grafo connesso con più di n passi:

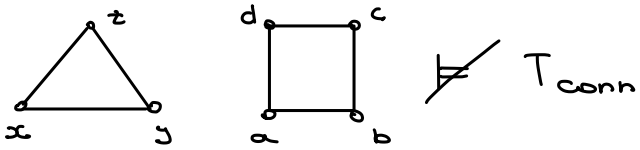
$\Rightarrow$ T' ha un modello M necessariamente sconnesso (perché a^M, b^M sono in componenti diverse) $L = \{ E, a, b \}$ - struttura

$\Rightarrow$ $M|_E \models T$ sconnesso. Assurdo

Però esiste la teoria $T_{conn} = \{ \varphi \mid \varphi$ vera in tutti i grafi connessi $\}$

però avrà pure modelli sconnessi.

Il problema è trovare un modello!



Esercizio: Perché questo non va bene come modello?

Esercizio: Quale potrebbe essere un modello sconnesso di questa teoria?

05-11-2021 Lezione 11 Prof. Berarducci

- Completezza (e correttezza) $T \vdash \varphi \Leftrightarrow T \models \varphi$
  ↑ Teoria; ↑ Teorema della teoria T; ↑ Teorema della metateoria

- Compattezza lo abbiamo espresso in due forme

  $T \models \varphi \Rightarrow \exists S \subset_{\text{finito}} T \quad S \models \varphi$ (esistono dimo puramente semantiche)

  $\Rightarrow$ $T \models \bot \Rightarrow \exists S \subset_{\text{finito}} T \quad S \models \bot$ → banale se si usa $\vdash$ al posto di $\models$

  Se T non ha modelli; esiste un sottoins. finito S di T che non ha un modello

→ [Quindi se ogni sottoinsieme finito di T ha un modello allora anche T lo ha]

- Löwenheim-Skolem verso l'alto e il basso in forma debole

L.S.↑ L.S.↓

(debole) LS↑ Se T ha $\forall n \in \mathbb{N}$ un modello M con più di n elementi

$\Rightarrow$ $\forall \alpha$ cardinale T ha un modello M_α di card $\geq \alpha$

(debole) LS↓ Se T ha un modello $\Rightarrow$ ha anche un modello M di card $\leq \max(\aleph_0, |L|)$

Esempi: • PA ha modelli di cardinalità $2^{\aleph_0}$ (LS↑)

• $Th(\mathbb{R}, 0, 1, +, \cdot)$ ha modelli numerabili (LS↓)

Vogliamo vedere LS↑↓ in forma forte

MORFISMI

Def Un morfismo $\mu : A \to B$ (con A, B L-struttura) è una funzione $\mu : dom(A) \to dom(B)$ tale che:

- Se $c \in L$ simbolo di costante $\mu(c^A) = c^B$
- Se $f \in L$ simbolo di funzione n-aria

$a_1, \dots, a_n \in A \quad \mu(f^A(a_1, \dots, a_n)) = f^B(\mu(a_1), \dots, \mu(a_n))$

- Se $R \in L$ simbolo di relazione n-aria

$a_1, \dots, a_n \in A \quad (a_1, \dots, a_n) \in R^A \Rightarrow (\mu a_1, \dots, \mu a_n) \in R^B$, $A \models R(a_1/x_1, \dots, a_n/x_n)$

Es A, B sono ordini totali $A = (A_i \leq_A)$ $B = (B_i \leq_B)$

$\mu : A \to B$ è un morfismo $\Leftrightarrow \forall a_1, a_2 \in A \quad a_1 \leq_A a_2 \Rightarrow \mu a_1 \leq_B \mu a_2$

Def $\mu : A \to B$ è un isomorfismo se è un morfismo biunivoco e $\mu^{-1} : B \to A$ è un morfismo

Esempio: $L = \{ \leq \}$

$A = \{ \mathbb{N}^{>0}, \leq_A \}$ $a_1 \leq_A a_2$ se $a_1 | a_2$

$B = \{ \mathbb{N}^{>}, \leq_B \}$ $b_1 \leq_B b_2$ se b_1 è minore di b_2 nel senso usuale

cioè se si lega: $\exists x \in \mathbb{N} \quad b_2 = b_1 + x$

$id: A \to B$
$x \mapsto x$

è un morfismo biunivoco ma non un isomorfismo

Esercizio: se L non contiene simboli di relazione un morfismo biunivoco è un isomorfismo.

Esempi: 1) $\mu: \mathbb{Z} \to \mathbb{Z}_{(5)}$ $L = \{0, 1, +, \cdot\}$ con la ovvia interpr. in $\mathbb{Z}$ e $\mathbb{Z}_{(5)}$
visti come anelli

$\mu(a)$ = classe d'equiv di a mod 5

μ è un morfismo

$$\mathbb{Z} \xmapsto{\mu} \mathbb{Z}_{(5)} = \{0, \_, 4\}$$

$$7 \longmapsto \mu(7) = 2$$

$$\mu(a \oplus b) = \mu(a) \oplus \mu(b)$$
$\oplus$ in $\mathbb{Z}$; $\oplus$ in $\mathbb{Z}_{(5)}$

Esercizio $\mu: A \to B$ è un morfismo se per ogni formula atomica $\varphi = \varphi(x_1, \dots, x_n)$ (cioè se $VL(\varphi) \subseteq \{x_1, \dots, x_n\}$)

$\forall a_1, \dots, a_n \in A \quad A \models \varphi(a_1/x_1, \dots, a_n/x_n) \Rightarrow B \models \varphi(b_1/x_1, \dots, b_n/x_n)$

dove $b_i = \mu(a_i)$

esempio: Se $L = \{0, 1, +, \cdot\}$

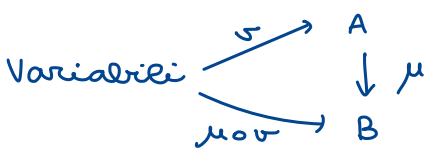
$\varphi(x_1, x_2, x_3)$ potrebbe essere $x_1 + x_2 = x_3 \Rightarrow \mu(a_1) + \mu(a_2) = \mu(a_3)$

oppure $\underbrace{x_1 + (x_1 + x_2)}_{t_1 \doteq t_2} = x_3$ $\Rightarrow$ per ind. sulla complessità delle sottof. e usare ?

In generale: Se t è un L-termine $VL(t) \subseteq \{x_1, \dots, x_n\}$

$\mu: A \to B$ morfismo di L-strutture, σ ambiente $\sigma(x_i) = a_i \in A$

$\mu(t^{A, \sigma}) = t^{B, \mu \circ \sigma}$



se $\sigma = (a_1/x_1, \dots, a_n/x_n)$
$\mu(a_i) = b_i$
$\mu \circ \sigma = (b_1/x_1, \dots, b_n/x_n)$

Teorema A, B L-strutture, φ L-formula chiusa,

$\mu : A \to B$ isomorfismo $\Rightarrow$ $A \vDash \varphi \iff B \vDash \varphi$

Idea: Induzione sul numero di connettivi di φ.

Esempio: φ è $\alpha \vee \beta$: $A \vDash \alpha \vee \beta \iff A \vDash \alpha$ o $A \vDash \beta$

$\iff B \vDash \alpha$ o $B \vDash \beta$

ind.

$\iff B \vDash \alpha \vee \beta$

Le problema sono i $\forall$ e $\exists$ $\rightsquigarrow$ non sono più formule chiuse

Esempio: $A = (\mathbb{R}, +)$ $\quad B = (\mathbb{R}^{>0}, \cdot)$

$L = \{ \circ \}$ $\quad \circ^A = +_{\mathbb{R}}$ $\quad \circ^B = \cdot_{\mathbb{R}}$

A, B sono isomorfi? Sì

$\exp : A \to B$ è un isomorfismo

$\exp(a_1 \hat{\circ} a_2) = \exp(a_1 + a_2) = e^{a_1} \cdot e^{a_2} = e^{a_1} \circ^B e^{a_2}$

ne segue che A, B verificano le stesse L-formule : $A, B \vDash \forall xy \; x \cdot y = y \cdot x$

Teorema (più forte): $\mu : A \to B$ isomorfismo

φ L formula con $VL(\varphi) \subseteq \{x_1, \dots, x_n\} \Rightarrow \forall a_1, \dots, a_n$

$A \vDash \varphi(a_1/x_1, \dots, a_n/x_n) \iff B \vDash \varphi(b_1/x_1, \dots, b_n/x_n)$ dove $b_i = \mu(a_i)$

$\varphi(a_1/x_1, \dots, a_n/x_n)$: formula con parametri $a_1, \dots, a_n \in dom(A)$

Dim (cenno): Induzione su φ. **Caso**: $\varphi = \forall y \, \vartheta$

$VL(\vartheta) \subseteq \{x_1, \dots, x_n, y\}$

$A \vDash \forall y \, \vartheta(a_1/x_1, \dots, a_n/x_n)$ $\overset{\text{Tarski}}{\iff}$ $\forall c \in A \; A \vDash \vartheta(a_1/x_1, \dots, a_n/x_n, c/y)$

($\forall$ linguaggio; $\forall$ metateoria)

$\overset{\text{ind.}}{\iff} \forall c \in A \; B \vDash \vartheta(\mu a_1/x_1, \dots, \mu a_n/x_n, \mu c/y)$

$\forall d \in B \; B \vDash \vartheta(\mu a_1/x_1, \dots, \mu a_n/x_n, d/y)$ perché μ biunivoca

$\iff B \vDash (\forall y \, \vartheta)(\mu a_1/x_1, \dots, \mu a_n/x_n)$ finire per esercizio

Esercizio Chiamo φ positiva se usa solo i connettivi $\wedge, \vee, \exists$ (e non usa $\neg, \forall, \to$)

Se $\mu : A \to B$ morfismo, φ positiva $VL(\varphi) \subset \{x_1, \dots, x_n\}$

$A \models \varphi(a_1/x_1, \dots, a_n/x_n) \Rightarrow B \models \varphi(b_1/x_1, \dots, b_n/x_n)$ dove $b_i = \mu(a_i)$

Esempio $\mathbb{Z} \models \exists x (x^2 = 4)$ $\qquad \mu : \mathbb{Z} \to \mathbb{Z}/_{(3)}$ $\qquad L = \{+\}$

$\Downarrow$

$\mathbb{Z}/_{(3)} \models \exists x (x^2 = \mu(4))$ $\qquad x \mapsto x \bmod 3$ $\qquad$ morfismo

$\mu(4) = 1$

$\exists x (x^2 = 4) = \underbrace{\exists x (x^2 = y)}_{\varphi} (4/y)$ $\quad \tau$ ambiente

per formule non positive non vale

Es $\mathbb{Z} \models \neg(4 \doteq 7)$

$\mathbb{Z}/_{(3)} \models \mu(4) \doteq \mu(7)$ $\qquad$ sono entrambi $\equiv 1 \bmod 3$

Def A, B L-strutture, A è una sottostruttura di B se

$dom(A) \subset dom(B)$ e i simboli di L vengono interpretati in A come in B ma ristretti ad A e se per le φ atomiche vale $A \models \varphi \Rightarrow B \models \varphi$.

- R relazione n-aria $\in L$, $R^A = R^B \cap A^n$
- f funzione n-aria $\in L$, $f^A = f^B|_{A^n}$
- $c^A = c^B$, con c costante

esempio $(\mathbb{Z}, 0, 1, +, \cdot)$ è una sottostruttura di $(\mathbb{R}, 0, 1, +, \cdot)$

con la solita interpretazione dei simboli $0, 1, +, \cdot$

Scrivo $A \subset B$ per indicare che A è una sottostruttura di B

SOTTOSTRUTTURA GENERATA

A L-struttura $\quad X \subseteq dom(A)$

$\langle X \rangle_A$ = il più piccolo sottoinsieme di A che richiede X ed è chiuso per l'interpretazione dei simboli di funzione e costante

$= \bigcap_{C \subset dom(A)} (C \supseteq X \wedge C$ è chiuso per le operazioni di $L)$

esercizio

$\textcircled{=} \{ t^{A,v} \mid t$ L-termini, v ambienti con valori in $x \}$

v: variabili $\to X$

$\langle X \rangle_A$ potrebbe essere vuoto (se $X = \emptyset$ e in L non ho simboli di costante)

se $\langle X \rangle_A$ non è vuoto è il dominio di un'unica struttura di A

che diamo ancora $\langle X \rangle_A$

Esempio $A = (\mathbb{R}, +_{\mathbb{R}})$ $L = \{+\}$

$X \subseteq \mathbb{R}$ $X = \{2\}$

$\langle X \rangle_A$ = numeri pari positivi $\Rightarrow (x_1 + x_1 + x_1 + \dots + x_1)(2/x_1) = 8$

È una sottostruttura, se nel linguaggio avessi anche il meno però dovrei aggiungere anche i n° pari negativi.

Def A è una sottostruttura elementare di B (scrivo $A \prec B$) se A è una sottostrutt. di B e per ogni L-formula φ e ambiente v si ha:

$A \models \varphi(v) \iff B \models \varphi(v)$ → non vale solo per le atomiche ma per tutte!

Esempio: $(\mathbb{Z}, 0, 1, +, \cdot) \subset (\mathbb{R}, 0, 1, +, \cdot)$ è una sottostruttura ma non elementare! $\mathbb{Z} \models \neg\exists x\,(x^2 = 1+1)$, $\mathbb{R} \models \exists x\,(x^2 = 1+1)$

Def A, B L-strutture, A è elementarmente equivalente a B se per ogni L-formula chiusa, $A \models \varphi \iff B \models \varphi$ e scrivo $A \equiv B$

Ho definito:

$A \subset B$ sottostruttura semplice

$A \equiv B$ elementare equivalente

$A \prec B$ sottostruttura elementare

$A \cong B$ isomorfi

Esercizio trovare A, B L-strutture con: $A \subset B$, $A \equiv B$, $A \not\prec B$ (esistono A, B con $A \subset B$, $A \cong B$, $A \not\prec B$)

Soluzione: $L = \{<\}$

$A = (\mathbb{Z}, <)$, $B = (2\mathbb{Z}, <)$

con $<$ interpretato nel solito modo in A e in B.

$A \cong B$

$x \mapsto 2x$

$\Rightarrow A \equiv B$ per l'es. di prima

però $A \not\cong B$ perché $A \models \exists x\ (2 < x \wedge x < 4)$

$B \not\models \exists x\ (2 < x \wedge x < 4)$

qui 2 e 4 sono parametri menzionati nell'ambiente

MORFISMI ELEMENTARI

$\mu: A \to B$ è un morfismo elementare se è un morfismo e per ogni L-formula φ con $VL(\varphi) \subseteq \{x_1, \dots, x_n\}$ $\forall a_1, \dots, a_n \in A$

$\circledast$ $A \models \varphi(a_1/x_1, \dots, a_n/x_n) \iff B \models \varphi(b_1/x_1, \dots, b_n/x_n)$ con $b_i = \mu(a_i)$

Oss: $A \prec B \iff id: A \to B$ $x \mapsto x$ è un morfismo elementare

Oss: Per le sottostrutture $\circledast$ vale per le atomiche o negazioni di atomiche

L.S. ↓ forma forte:

T L-teoria $A \models T \Rightarrow \exists B \prec A$ $|B| \leq \max(\aleph_0, |L|)$

Segue che $B \models T$ perché $B \equiv A$ cioè $Th(B) = Th(A) \supseteq T$

$\{\varphi$ chiuse $| A \models \varphi\}$

esempio $A \models ZF \Rightarrow$ Trovo un modello $B \models ZF$ numerabile $B \prec A$

$(\mathbb{N}, <) \models$ Estensionalità, ¬Coppia con $<$ pensato come $\in$

Coppia: $\forall x y\ \exists z\ \forall u\ u \in z \leftrightarrow u = x \vee u = y$

idea $z = \{x, y\}$

Estensionalità: $\forall x y\ \ x \doteq y \leftrightarrow \forall u\ (u \in x \vee u \in y)$

$B = (\mathbb{N}, <)$ $B \models$ Est

$B \not\models$ Coppia

L.S. ↑ forma forte:

$\forall B \models T$ infinito, $\forall \alpha$ cardinale $\exists A \succ B$ (aut. $A \models T$) con $|A| \geq \alpha$

Dati dei modelli, posso produrre dei modelli grandi e piccoli quanto mi pare in fortissima relazione con quelli che avevo già.

08-11-2021 Lezione 12 Prof. Berarducci

$A \subset B$ sottostruttura es. $(\mathbb{Z}, +, \cdot) \subset (\mathbb{R}, +, \cdot)$

$A \prec B$ sottostruttura elementare es: (Reali algebrici) $\prec (\mathbb{R}, +, \cdot)$

$(\mathbb{Q}, <) \prec (\mathbb{R}, <)$

$(\mathbb{Q}, <, +, \cdot) \not\prec (\mathbb{R}, <, +, \cdot)$

elementarmente equivalente

$A \equiv B$ se $Th(A) = Th(B)$ cioè se φ chiusa $A \vDash \varphi \iff B \vDash \varphi$

Oss: Una teoria coerente T è completa $\iff \forall A, B \vDash T \quad A \equiv B$

$A \cong B \Rightarrow A \equiv B$ ma non il viceversa (L.S. $\uparrow\downarrow$)

↳ posso trovare $A \equiv B$ ma molto più grande/piccolo

- Se $\mu : A \to B$ è morfismo, per ogni $\varphi(x_1, \dots, x_n)$ atomica

  $\forall a_1, \dots, a_n \in A$ se $A \vDash \varphi(a_1, \dots, a_n) \Rightarrow B \vDash \varphi(\mu a_1, \dots, \mu a_n)$ (*)
- $\mu : A \to B$ è un'immersione se in (*) vale il $\iff$,

  cioè se $A \overset{\cong}{\underset{\mu}{}} Im(\mu) \subset B$
- $A \subset B \iff$ inclusione $A \hookrightarrow B$ è una immersione
- $\mu : A \overset{\prec}{\longrightarrow} B$ immersione elementare se μ è un morfismo e

  (*) vale per tutte le formule (con il $\iff$)
- $A \prec B$ se l'inclusione è un'immersione elementare

Def: Una L-teoria è α-categorica (con α un cardinale) se è coerente e tutti i modelli di cardinalità α sono isomorfi

Def T è categorica se è coerente e tutti i suoi modelli sono isomorfi

PA^2 è categorica però è del 2° ordine.

Se una teoria T del primo ordine è categorica → l'unico modello a meno di iso è finito (L.S. $\uparrow$)

⇒ "Categorica" è troppo forte, mi accontento di α-categorica

Esempio: $L = \{ \leq \}$, DLO = Ordini lineari densi senza estremi

$\forall x\, y\, z$

- $x \leq x$
- $x \leq y \wedge y \leq z \rightarrow x \leq z$
- $x \leq y \wedge y \leq x \rightarrow x = y$

} ordini parziali

- $x \leq y \vee y \leq x$

} totali

- $x \leq y \rightarrow \exists z \; x < z \wedge z < y$

} densi

dove $x < z$ vuol dire $x \leq z \wedge x \neq z$.

- $\forall x \exists y \; x < y$
- $\forall x \exists y \; y < x$

} senza estremi

Teorema: DLO è $\aleph_0$-categorica, non è $2^{\aleph_0}$-categorica

non $2^{\aleph_0}$-categorica:

- $(\mathbb{R}, <) \models DLO$
- $(\text{irrazionali}, <) \models DLO$
- $(\mathbb{R} \setminus \{0\}, <) \models DLO$

$(\mathbb{R} \setminus \{0\}, <) \not\cong (\mathbb{R}, <)$

↑ Qui esiste un insieme limitato superiormente senza sup : $\mathbb{R}^{<0}$

Teo DLO è $\aleph_0$-categorica.

- $(\mathbb{Q}, <)$ è un modello
- $(\mathbb{Q} \cup \{\sqrt{2}\}, <)$ è un modello
- $(\mathbb{Q} \setminus \{0\}, <)$ è un modello

Ma sono isomorfi!

Dim (Cantor):

Usiamo la tecnica del "va e vieni" (back and forth)

Siano $A, B \models DLO$, A, B numerabili

Devo mostrare $A \cong B$. Costruisco un'isomorfismo $f : A \to B$ come unione $f = \bigcup_{n \in \mathbb{N}} f_n$ di isomorfismi f_n parziali.

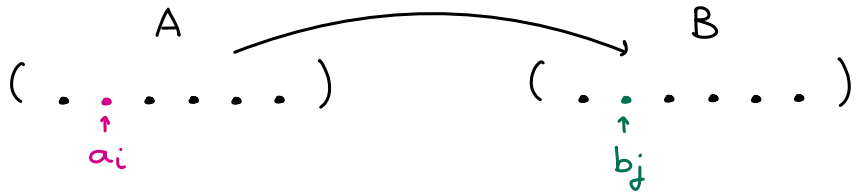
$\text{dom}(f_n) \subset A$ finito $\quad \text{Im}(f_n) \subset B$ finito $\quad f_{n+1} \supset f_n$

$A = \{a_n \mid n \in \mathbb{N}\} \quad B = \{b_n \mid n \in \mathbb{N}\}$

Al passo n: ho definito $f_n : A_n \to B_n$ $\quad |A_n| = n \quad |B_n| = n$

Al passo $n+1$: • Se $n+1$ è pari prendo il minimo indice i tale che $a_i \notin \mathrm{dom}(f_n)$ e trovo j tale che $f_n : A_n \to B_n$ si estende ad un isomorfismo $f_{n+1} : A_n \cup \{a_i\} \to B_n \cup \{b_j\}$ con $f_{n+1}(a_i) = b_j$

(Lo posso fare per densità e mancanza di estremi)



• Se $n+1$ è dispari scambio i ruoli di A, B e prendo il minimo i tale che $b_i \notin \mathrm{Im}(f_n)$ e trovo a_j in modo da estendere f_n a un isomorfismo f_{n+1} che manda a_j in b_i.

Dico che $\mathrm{dom}(f) = A$. Sia $a_n \notin \mathrm{dom}(A)$. Allora ho scelto sempre a_i con $i < n$.

Assurdo, perché ci sono solo un numero finito di indici $< n$.

Similmente $\mathrm{Im}(f) = B$. Ovviamente $f = \bigcup_{n \in \mathbb{N}} f_n$ è un $\cong$. □

Teo: Sia T L-teoria coerente α-categorica $(\alpha \geq |L| + \aleph_0)$ senza modelli finiti $\Rightarrow$ T è completa

(T non completa: $T \not\vdash \varphi$, $T \not\vdash \neg\varphi$)

Dim: Sia per assurdo φ L-formula chiusa $T \not\vdash \varphi$, $T \not\vdash \neg\varphi$.

Allora esistono $A \models T \cup \{\neg\varphi\}$ e $B \models T \cup \{\varphi\}$.

Se $|A| = |B| = \alpha \Rightarrow A \cong B$ per hp., quindi $A \equiv B$. Assurdo.

Sia $\mathrm{Th}(A) = \{\vartheta \text{ chiusa} \mid A \models \vartheta\}$, $\mathrm{Th}(B) = \{\vartheta \mid B \models \vartheta\}$.

Per L.S. $\uparrow$ esistono modelli $A' \models \mathrm{Th}(A)$, $B' \models \mathrm{Th}(B)$ con $|A| \geq \alpha$ e $|B| \geq \alpha$ con α cardinale.

Per L.S. $\downarrow$ in forma forte (da dimostrare) esistono $A'' \prec A'$ e $B'' \prec B'$ con $|A''| = |B''| = \alpha$. Assurdo perché avrei $A'' \cong B''$ per α-categoricità ma $A'' \models \neg\varphi$, $B'' \models \varphi$.

(Le abbiamo estese da A e B) □

Schema:

- Passo 1 : parto da $A \models \neg\varphi$ e $B \models \varphi$
- Passo 2 : ingrandisco (L.S. ↑)
- Passo 3 : rimpicciolisco (L.S. ↓ forte) ⇒ ottengo $A'' \cong B''$ ↘

Mi serve di dimostrare L.S. ↓ forte.

Digressione: Potrei, anziché lavorare con la teoria di A e la teoria di B, lavorare con una teoria di A con l'aggiunta di ulteriori assiomi e di nuove costanti (diverse l'una dall'altra). Queste teorie rimangono coerenti per compattezza. Quando vado giù con L.S. posso scendere fino a di una non scenderò mai sotto altrimenti non verifico gli assiomi che ci sono di nuove costanti.

Il fatto che il linguaggio abbia molte costanti non ci garantisce nulla sulla cardinalità del modello.

DECIDIBILITÀ (digressione):

- DLO è decidibile: cioè c'è un algoritmo che data φ mi dice se $DLO \vdash \varphi$, con $L = \{<\}$. Qual'è l'algoritmo?

Provo in tutti i modi possibili (enumerando tutte le possibili dimostrazioni formali da DLO usando le regole) a dimostrare φ o a dimostrare $\neg\varphi$. Siccome DLO è completa prima o poi ci riesco. Se dimostrassi che ZF è completa potrei dimostrare tutto! □

- ACA_0 = campi alg. chiusi di char 0 è decidibile:

È $\aleph_1$-categorica, quindi completa, quindi decidibile, quindi

c'è un algoritmo per capire se una φ nel linguaggio $0, 1, +, \cdot$ è vera in $\mathbb{C}$ (equivale a dimostrabile in ACA_0 perché $\mathbb{C}$ è un modello e poiché la teoria è completa se è vero in un modello allora è vera in tutti).

L'unico modello di card. $\aleph_1$ (a meno di isomorfismi) è $\overline{\mathbb{Q}(x_i \mid i < \aleph_1)}$

$\mathbb{C} \cong \overline{\mathbb{Q}(x_i \mid i < 2^{\aleph_0})}$

$\overline{\mathbb{Q}} \cong \overline{\mathbb{Q}(x)} \subsetneq \overline{\mathbb{Q}(x,y)}$ sono numerabili

RCF = campi reali chiusi è completa, non è $\aleph$-categorica $\forall \alpha$

$\mathbb{R} \models RCF$, quindi c'è un algoritmo, per sapere data φ se φ è vera in $\mathbb{R}$.

Teo (L.S. ↓ in forma forte):

$\forall$ L-struttura A, per ogni $X \subseteq dom(A)$ esiste $B \prec A$, $X \subset dom(B)$.

$|X| \leq |B| \leq \max(|L| + \aleph_0, |X|)$. (se $|X| \geq \max(|L| + \aleph_0, |X|) \Rightarrow |B| = |X|$)

Criterio di Tarski-Vaught

Siano $A \subset B$ L-strutture,

ipotesi: Supponiamo che per ogni L-formula della forma

$\exists x\, \varphi(x_1, \dots, x_n, y)$ e $\forall a_1, \dots, a_n \in A$ se $B \models \exists y\, \varphi(a_1, \dots, a_n, y)$

se $B \models \exists y\, \varphi(a_1, \dots, a_n, y) \Rightarrow \exists b \in A \quad B \models \varphi(a_1, \dots, a_n, b)$

tesi: $A \prec B$

Dim: prossima volta

Esempi: Sia $\Theta(x,y)$ senza quantificatori $A \subset B$, $a \in A$.

$A \models \exists x\, \Theta(x,a) \Rightarrow B \models \exists x\, \Theta(x,a)$

$B \models \forall x\, \Theta(x,a) \Rightarrow A \models \forall x\, \Theta(x,a)$

- Si basa sul fatto che $a_1, a_2 \in A$, $A \models \Theta(a_1,a_2) \Leftrightarrow B \models \Theta(a_1,a_2)$

Per le formule di tipo $\forall x\, \exists y\, \Theta(x,y,z)$ non funziona:

$(0,1) \models \forall x \exists y\,(y<x)$, $[0,1) \not\models \forall x \exists y\,(y<x)$, $(-1,1) \models \forall x \exists y\,(y<x)$

12-11-2022 Lezione 13 Prof. Berarducci

Criterio di Tarski-Vaught

Siano $A \subset B$ L-strutture, supponiamo che $\forall a_1,\dots,a_n \in A$ per ogni $\varphi(x_1,\dots,x_n,y)$ L-formula, se $B \models \exists y\,\varphi(a_1,\dots,a_n,y) \Rightarrow \exists b \in A\ B \models \varphi(a_1,\dots,a_n,b)$

Allora $A \prec B$.

Dim: Sia $\theta(x_1,\dots,x_k)$ L-formula. Siano $a_1,\dots,a_k \in A$ devo mostrare $A \models \theta(a_1,\dots,a_k) \iff B \models \theta(a_1,\dots,a_k)$.

Il caso θ atomica è vero perché $A \subset B$.

Il caso $\theta = \neg\alpha, \alpha\wedge\beta, \alpha\vee\beta$ segue per induzione sul numero di connettivi di θ.

Il caso $\theta = \exists y\,\varphi(x_1,\dots,x_n,y)$ segue dall'ipotesi.

$B \models \theta(\bar{a}) \iff B \models \exists y\,\varphi(a_1,\dots,a_n,y) \overset{\text{ipotesi}}{\iff} \exists a \in A\ \underline{B \models \varphi(a_1,\dots,a_n,a)}$

$\overset{\text{induz.}}{\iff} \exists a \in A\ \underline{A \models \varphi(a_1,\dots,a_n,a)} \overset{\text{Tarski}}{\iff} A \models \exists y\,\varphi(x_1,\dots,x_n,y)$ □

$\forall y\,\theta \equiv \neg\exists y \neg\theta$

L.S. ↓ forma forte

Sia A L-struttura. Sia $X \subset \mathrm{dom}(A)$.

Esiste $B \prec A$, $X \subset \mathrm{dom}(B)$ $\quad |B| \leq |X| + |L| + \aleph_0 = \lambda$

(quindi se $|X| \geq |L| + \aleph_0 \Rightarrow |B| = |X|$) → somma di cardinali ∞ è = al max

Dim: Data $\exists y\,\varphi(x_1,\dots,x_n,y)$ e $a_1,\dots,a_n \in A$ se $A \models \exists y\,\varphi(a_1,\dots,a_n,y)$, scelgo un tale y e lo chiamo $f_\varphi(a_1,\dots,a_n)$ (funzione di Skölem)

Esempio: $\mathbb{R} \models \underbrace{\exists y\,(\sqrt{2} < y < \pi)}$

$\exists y\,\theta(x_1,x_2,y)\left(\frac{\sqrt{2}}{x_1}, \frac{\pi}{x_2}\right)$

$f_\varphi(\sqrt{2},\pi) = \frac{\sqrt{2}+\pi}{2}$ funzione di Skölem (ne scelgo una che verifica)

Senza perdita di generalità suppongo $X_0 = X \neq \emptyset$.

Definisco $X_{n+1} = X_n \cup \{ f_\varphi(a_1, \dots, a_k) \mid A \models \exists y \varphi(a_1, \dots, a_k, y), \varphi \text{ formula}, a_i \in X_n \}$

Dunque ho la successione $X_0 \subset X_1 \subset X_2 \subset \dots$

Definisco $X_\omega = \bigcup_n X_n$. Vorrei a questo punto $B = X_\omega$.

Claim: X_ω è il dominio di un'unica sottostruttura di A

Esempio: $L = \{0, 1, +, \cdot\}$ X_ω dimo per $0, 1, +, \cdot$

È dimo per 0 perché: $A \models \exists y (y = 0) \Rightarrow 0^A \in X_1 \subset X_\omega$

$a, b \in X_\omega \Rightarrow a +_A b \in X_\omega$

$$\left.\begin{array}{l} \exists n \; a, b \in X_n \cdot A \models \exists y (y = a + b) \\ \exists y \, \varphi(y = x_0 + x_1)(a/x_0, b/x_1) \end{array}\right\} \Rightarrow f_\varphi(a, b) = a +_A b$$

$\Rightarrow a +_A b \in X_{n+1} \subset X_\omega$. Ho dimostrato quindi il claim.

Ha senso parlare di X_ω come se fosse una struttura.

Sia B la sottostruttura di A con dominio X_ω. Dico che $B \prec A$ perché per costruzione verifica il criterio di T. V.

Infatti se $A \models \exists y \varphi(b_1, \dots, b_n, y) \Rightarrow \exists m \; b_1, \dots, b_n \in X_n$

$\Rightarrow$ trovo un testimone y in X_{m+1} $y = f_\varphi(b_1, \dots, b_n)$

Rimane solo da verificare $|B| \leq \lambda = |X| + |L| + \aleph_0$

$|B| = |X_\omega| = \bigcup_{n \in \mathbb{N}} |X_n|$ λ (card. ∞)

$|X_0| = |X| \leq \lambda \rightsquigarrow |X_{n+1}| \leq |X_n| + |L\text{-formule}| \oplus \bigcup_{k \in \mathbb{N}} |X_n|^k \leq \lambda + \lambda + \underbrace{\bigcup_{k \in \mathbb{N}} \lambda^k}_{\lambda} = \lambda$

Oss: $(a_1, \dots, a_k) \in X_n^k$ k-upla di el. di X_n, $|X_n^k| = |X_n|^k$

Per induzione $\forall n \; |X_n| \leq \lambda \Rightarrow |X_\omega| = |\bigcup_n X_n| \leq \sum_n |X_n| \leq \sum_{n \in \mathbb{N}} \lambda \leq \aleph_0 \cdot \lambda = \lambda$

Quindi $|B| \leq \lambda$. □

Cor: Se $\lambda \geq |L| + \aleph_0$, per ogni L-struttura A, $|A| > \lambda$ esiste $B \prec A$, $|B| = \lambda$.

Dim: parto da A. Scelgo $X \subset \text{dom}(A)$, $|X| = \lambda \Rightarrow$ applico L.S. ↓ forte □

Vediamo ora L.S. ↑ forte con la tecnica dei diagrammi:

DIAGRAMMI

A L-struttura, $L_A \supset L$ $\quad L_A = L \cup \{c_a \mid a \in A\}$.

$D(A) = \{\varphi(c_{a_1}, \dots, c_{a_n}) \mid \varphi(x_1, \dots, x_n)$ L-formula atomica o negata atomica tc $A \models \varphi(a_1, \dots, a_n)\}$

Esempio: $A = \mathbb{Z}/(3)$ $\quad L = \{+\}$

$\text{dom}(A) = \{0, 1, 2\}$ $\quad 1+2=0$ ecc.

$L_A = \{c_0, c_1, c_2, +\}$ $\quad D(A) = \{c_0 + c_1 = c_1,\ c_1 + c_2 = c_0,\ c_1 \neq c_2, \dots\}$ → assiomi

negata atomica

Teorema: $B \models D(A) \iff \exists$ immersione $\mu : A \to B|_L$, $\mu(a) = c_a^B$.

Dim: $A \models \varphi(a_1, a_2, \dots) \Rightarrow \varphi(c_{a_1}, c_{a_2}, \dots) \in D(A)$

$\Rightarrow B \models \varphi(c_{a_1}, c_{a_2}, \dots) \Rightarrow B|_L \models \varphi(a_1, \dots)$

(formula nel linguaggio esteso; ambiente)

diagramma elementare

$ED(A) = \{\varphi(c_{a_1}, \dots, c_{a_n}) \mid \varphi(x_1, \dots, x_n)$ L-formule (↳ non solo per le atomiche) tc $A \models \varphi(a_1, \dots, a_n)\}$.

Teorema: $B \models ED(A) \iff \exists \mu$ immersione elementare $\mu : A \xrightarrow{\prec} B$

↳ preserva tutte le φ

Dim: analoga

Esempio: $\mathbb{R} = (\mathbb{R}, 0, 1, +, \cdot)$

Sia $T = ED(\mathbb{R}) \cup \{c \mid 0 < c,\ c < \frac{1}{n}\ n \in \mathbb{N}\}$ (infinitesimo)

$L(T) = L_A \cup \{c\}$ $\quad c + c + c + \dots + c < 1$ (n volte)

T ha un modello A per compattezza, ma $B \models ED(\mathbb{R}) \Rightarrow$ esiste un'immersione elementare $\mu : \mathbb{R} \xrightarrow{\prec} B|_L$ a meno di isomorfismo $\mathbb{R} \prec B|_L$

B somiglia a $\mathbb{R}$ ma contiene degli infinitesimi.

In B ha senso lavorare con $\frac{dy}{dx}$!

Dunque in analisi non standard ha senso lavorare con gli infinitesimi: dimostriamo qualcosa in B ma poiché $\mathbb{R} \prec B|_L$ tutto ciò che è vero in B è vero anche in $\mathbb{R}$ (basta non contenga par. infinitesimi)

Esercizio: Sia $\mu : A \to B$ immersione $\Rightarrow$ esiste $B' \cong B$ (tramite $\mu : B \xrightarrow{\sim} B'$)

$\Rightarrow B'$ è una vera sottostruttura (se elementare $\Rightarrow$ sottostr. elementare)

In questo modo: $A \xrightarrow{\mu} B$, $A \cong B' \subseteq B$ (sottostruttura)

Esempio: $\mathbb{R} \longrightarrow \mathbb{R}[x]/(x^2+1)$ } def di $\mathbb{C}$

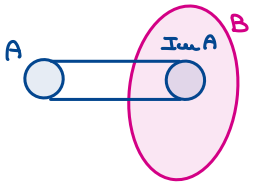
$r \longmapsto r \bmod x^2+1$

$\mathbb{R} \to \mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$ (s. strett.)

Esercizio (puramente insiemistico):

Data $f: A \to B$ iniettiva esiste $g: B' \supseteq A$ e $g: B \to B'$ biunivoca

$A \xrightarrow{f} B$, $A \cong B' \xrightarrow{g} B$



Qualunque immersione (elementare) la posso far diventare una sottostruttura (elementare)

$B' = A \cup [B \setminus Im(A)]$

IDEA: $g: B \to B'$ biunivoca e se B è una L-struttura posso rendere B' una L-struttura in modo che g diventi un isomorfismo.

L.S. ↑ forma forte:

Se A è una L-struttura infinita, $\lambda \geq |A|$, esiste $B \supset A$ con $|B| \geq \lambda$

Dim: (idea: dimostriamo che esistono delle teorie coerenti con tali caratteristiche, perché poi esistono dei modelli: prendiamo una teoria di cui B sia un modello, dunque che contenga $ED(A)$ e degli assiomi)

$T = ED(A) \cup \{c_i \neq c_j \mid i < j < \lambda\}$

T è coerente per compattezza (perché A è infinito)

$\Rightarrow$ ha un modello B tc $\exists$ immersione elementare $\mu: A \to B_{|L}$

$\Rightarrow$ Rimpiazzando B con copia isomorfa $\exists B' \cong B$ $A \subset B'$ $|B'| \geq \lambda$. □

Ricapitolando: per dimostrare ↑ si usa la compattezza

per dimostrare ↓ si usano le funzioni di Skölem

Teorema: Ogni teoria λ-categorica senza modelli finiti è completa

Dim: Basta mostrare che $\forall A, B \models T$, $A \equiv B$

$A \vdash T \xRightarrow{\text{LST}\uparrow} \exists A' \succ A \quad |A'| \geq \alpha$

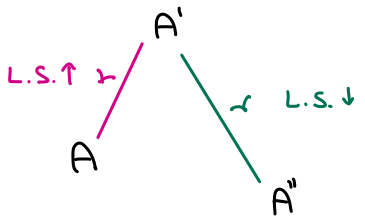
Sia $X \subset \text{dom}(A)$ $|X| = \alpha$

$\xRightarrow[\text{LS}\downarrow]{}$ esiste A'' con $X \subset \text{dom}(A'')$ $A'' \prec A$, $|A''| \leq \underset{\alpha}{|X|} + |L| + \aleph_0$

$\Rightarrow |A''| = \alpha \Rightarrow \forall A \vdash T \quad \exists A'' \equiv A \quad |A''| = \alpha$

$\Rightarrow \forall A, B \vdash T \quad \exists A'' \equiv A, B'' \equiv B, \quad |A''| = |B''| = \alpha$

e per α-categoricità $B'' \cong A'' \Rightarrow B'' \equiv A'' \Rightarrow B \equiv A$



□

Esercizio: Sia T la teoria degli ordini densi.

Allora T ha esattamente 4 estensioni complete (massimali)

Suggerimento: 1) le 4 possibilità corrispondono ad avere o no max, min

$\mathbb{Q} \cong [0,1)$, $(0,1)$, $(0,1]$, $[0,1]$ (tecnica del "back and forth")

2) $T \vdash \alpha \vee \beta$

$T' \supset T$ completa $\Rightarrow T' \vdash \alpha$ o $T' \vdash \beta$

Insiemi definibili:

A L-struttura, $X \subset \text{dom}(A)^n$

X è *definibile* (con parametri) se esiste una L-formula definita così

$\varphi(x_1, \dots, x_n, y_1, \dots, y_k)$ e parametri $a_1, \dots, a_k$ tali che:

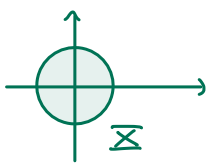
$X = \{(b_1, \dots, b_n) \in A^n \mid A \vDash \varphi(\underbrace{b_1, \dots, b_n, a_1, \dots, a_k}_{*})\}$

Se $k = 0$ X è definibile senza parametri.

(*) Ci sono due modi per farlo: o è nell'ambiente, quindi scrivo $(b_1/x_1, \dots, b_n/x_n, a_1/y_1, \dots, a_n/y_n)$, oppure arricchisco il linguaggio con le costanti $c_1, \dots, c_n$ e dico che interpreto c_1 come b_1, c_2 come b_2 ecc.

Esempio: $\mathbb{R} = (\mathbb{R}, 0, 1, +, \cdot)$,

- $X \in \mathbb{R}^2$ $X = \{(x,y) \mid \mathbb{R} \vDash x^2 + y^2 = \underset{\in L \Rightarrow \text{non è un parametro}}{1}\}$, X def. senza parametri
- $Y = \{(x,y) \mid \mathbb{R} \vDash x^2 + y^2 = \pi^2\}$, Y def. con parametro π
- $Z = \{(x,y) \in \mathbb{R}^2 \mid \mathbb{R} \vDash x^2 + y^2 = \sqrt{5}\}$ Z è def. con parametro $\sqrt{5}$?



No perché se scrivo $Z = \{(x,y) \in \mathbb{R}^2 \mid \mathbb{R} \models (x^2+y^2)^2 = 1+1+1+1+1\}$

allora è definibile senza parametri.

Ottengo che se il raggio del cerchio è un numero algebrico allora è def. senza parametri, se è un numero trascendente serve il parametro

Teo (Tarski):

$X \subset \mathbb{R}^n$ è definibile in $\mathbb{R} = (\mathbb{R}, 0, 1, +, \cdot) \Rightarrow X$ ha un n° finito di componenti connesse. In particolare se $X \subset \mathbb{R}$, X è unione finita di intervalli e punti. In particolare $\mathbb{Z} \subset \mathbb{R}$ non è definibile in $\mathbb{R}$.

Teo (Julia Robinson):

$\mathbb{Z}$ è definibile in $(\mathbb{Q}, 0, 1, +, \cdot)$.

Teo: In $(\mathbb{N}, 0, 1, +, \cdot)$ è definibile una marea di cose.

↳ se tolgo il $\cdot$ riesco a def. molto poco

15-11-2021 lezione 14 Prof. Berarducci

Iniziamo le dispense di calcolabilità e teoremi di Gödel (solo in parte)

Osservazione: $A \subset B$ sottostruttura, $\varphi(x_1, \dots, x_n, a_1, \dots, a_k)$ $a_i \in A$

$X_A \subset A^n$ $\quad X_A = \{(c_1, \dots, c_n) \in A^n \mid A \models \varphi(c_1, \dots, c_n, a_1, \dots, a_k)\}$

$X_B \subset B^n$ $\quad X_B = \{(c_1, \dots, c_n) \in B^n \mid B \models \varphi(c_1, \dots, c_n, a_1, \dots, a_k)\}$

Se $A \prec B \Rightarrow X_A = X_B \cap A^n$ per def. di sottostr elementare

(Non) Esempio: Se $A \subset B$ non elementare la stessa φ (con parametri da A) può def. insiemi completamente diversi in A e in B.

$$\left.\begin{aligned} \{x \in \mathbb{R} \mid \mathbb{R} \models \exists y \; x = y^2\} &= \mathbb{R}^{\geq 0} \\ \{x \in \mathbb{Q} \mid \mathbb{Q} \models \exists y \; x = y^2\} &\neq \mathbb{Q}^{\geq 0} \end{aligned}\right\} \text{perché } \mathbb{Q} \not\prec \mathbb{R}$$

Invece $A = \{\text{reali algebrici}\} \prec \mathbb{R} \Rightarrow \{x \in A \mid A \models \exists y \; x = y^2\} = A^{\geq 0}$

Def: T L-teoria è decidibile se esiste un algoritmo che con input φ (L-formula chiusa) stabilisce se $T \vdash \varphi$ o $T \nvdash \varphi$

Cioè se φ è un teorema o no.

Ho bisogno di precisazioni: cosa è un algoritmo?

Teo: Se T è una $\mathcal{L}$-teoria completa e l'insieme degli assiomi è decidibile $\Rightarrow$ T è decidibile.

Esempi: ACF = teoria dei campi algebricamente chiusi è decidibile ma non completa

$ACF_0 = ACF + \underbrace{\text{char } 0}_{(0\neq 1,\ 0\neq 1+1,\ \dots)}$ è decidibile e completa.

PANORAMICA:

Oss: $T_1 \equiv T_2 \iff Mod(T_1) = Mod(T_2) \overset{es.}{\iff} \{\varphi \mid T_1 \vdash \varphi\} = \{\varphi \mid T_2 \vdash \varphi\}$

	Decidibile	Completa	α-categorica
$Th(\mathbb{R},0,1,+,\cdot)$ $\Vert$ RCF	Sì Sì	Sì Sì	No No
$Th(\mathbb{C},0,1,+,\cdot)$ $\Vert$ ACF_0	Sì Sì	Sì Sì	Sì: $\alpha \geq \aleph_1$ Sì: $\alpha \geq \aleph_1$
$Th(\mathbb{Q},0,1,+,\cdot)$	No	No	No
$Th(\mathbb{Z},0,1,+,\cdot)$	No	No	No
$Th(\mathbb{N},0,1,+,\cdot)$ $\cup$ PA	No No (*)	No No	No No
$Th(\mathbb{N},0,1,+)$	Sì	Sì	No
$Th(\mathbb{N},0,s)$	Sì	Sì	Sì: $\alpha \geq \aleph_1$

(*) gli assiomi sono decidibili

Notazione:
- RCF = real closed fields (campi reali alg. chiusi)
- ACF_0 = visti sopra
- PA = Peano

Sostanzialmente i razionali, gli interi e i numeri naturali sono più complicati dei reali e dei complessi.

Teorema di Morley ($|L_T| = \aleph_0$):

T è $\aleph_1$-categorica $\Leftrightarrow$ T è α-categorica per ogni $\alpha \geq \aleph_1$

- $Th(\mathbb{N}, s, 0)$ è $\aleph_1$-categorica, non $\aleph_0$-categorica.

Sia $T \subset Th(\mathbb{N}, s, 0)$ con i seguenti assiomi:

$$\begin{cases} \forall xy\,(sx = sy \to x = y) \\ \forall x\,(x \neq 0 \to \exists y\; sy = x) \\ \forall y\,(sy \neq 0) \end{cases}$$

Dim: • T è $\aleph_1$-categorica (quindi completa, quindi $T \equiv Th(\mathbb{N}, s, 0)$)

Sia $M \models T$. Oss: Deve esistere un modello $\neq \mathbb{N}$ per L.S.↑, ad es: $\mathbb{N} + \mathbb{Z}$

Sia $a \sim b \Leftrightarrow \exists n \in \mathbb{N},\ s^n a = b \vee s^n b = a$

$\sim$ è una relazione di equivalenza su M.

Sia $(a_i \mid i \in I)$ un insieme di rappresentanti delle varie classi di equivalenza $M = \bigcup_{i \in I} [a_i]$, $a_0 = 0$.

$[0] \cong \mathbb{N}$, $[0] = \{0, s0, ss0, \dots\} \subset M$

$[a_i] \cong \mathbb{Z}$, $[a_i] = \{\dots, ppa_i, pa_i, a_i, sa_i, ssa_i\}$ se $a_i \notin [0]$

$= \{s^k(a_i) \mid k \in \mathbb{Z}\} \cong (\mathbb{Z}, s)$

$s^{-1}x = \underbrace{p(x)}_{\text{predecessore}} = y \Leftrightarrow sy = x$

$M = \mathbb{N} \cup \dot{\bigcup}_{i \in I} \mathbb{Z} \cong \mathbb{N} \cup \bigcup_{i \in I} (\mathbb{Z} \times \{i\})$ $\qquad s(\langle k, i \rangle) = \langle k+1, i \rangle$

$|M| = \aleph_1 \Leftrightarrow |I| = \aleph_1 \Rightarrow T$ è $\aleph_1$ categorica

- Non $\aleph_0$-categorica perché $\mathbb{N} \not\cong \mathbb{N} \dot{\cup} \mathbb{Z}$

T = teoria del successore è $\aleph_1$-categorica, quindi completa,

quindi $T \equiv Th(\mathbb{N}, s, 0)$ (le conseguenze sono complete massimali)

Alla fine noi vorremmo riuscire a studiare $Th(\mathbb{N}, 0, 1, +, \cdot)$

Dunque procediamo passo passo.

Introduciamo una "nuova" teoria aritmetica:

Aritmetica di Presburger (PRE).

$L = \{0, S, +\}$

Assiomi: $Sx = Sy \to x = y$

$0 \neq Sy$

$x \neq 0 \to \exists y \ \ Sy = x$

$x + 0 = x$

$x + Sy = S(x + y)$

Induzione (Schema):

$Ind_{\varphi,x}: \forall \vec{y} \, [\varphi(0, \vec{y}) \wedge \forall x \ \varphi(x, \vec{y}) \to \varphi(Sx, \vec{y}) \to \forall x \ \varphi(x, \vec{y})]$

Posso concedere che ci siano parametri. Servono infiniti assiomi.

Teorema: PRE è completa (non $\aleph_1$-categorica $\forall \aleph_1$)

Esercizio: Nella logica del 2° ordine posso definire + in $(\mathbb{N}, S, 0)$.

(posso quantificare anche su predicati)

$\underbrace{\varphi_+(a,b,c)}_{a+b=c} \equiv \forall P$ (predicato ternario):

$[\forall x \ P(x,0,x) \wedge \forall x \ P(x,y,z) \to P(x,Sy,Sz) \to P(a,b,c)]$

Questa formula è vera in $\mathbb{N}, S, 0 \leftrightarrow a+b=c$

Idea. • Voglio verificare $2+3=5$.

Inizio da $2+0=2$: verifica $P(2,0,2)$, passo alla 2ª regola e ho $2+1=3$ cioè $P(2,S0,S2) = P(2,1,3)$. Quindi ho $P(2,S1,S3) = P(2,2,4)$ e poi $P(2,S2,S4) = P(2,3,5) = P(a,b,c)$.

• Ora voglio vedere che se $a+b \neq c$ allora non è vero che per ogni predicato succede quella cosa: prendo il grafico della somma come predicato e il 3° predicato $P(a,b,c)$ non viene verificato.

Nella logica del 2° ordine riesco pure a definire il $\cdot$.

Nella logica del 1° ordine non posso definire + in $(\mathbb{N}, S, 0)$ e non

posso definire $\cdot$ in $(\mathbb{N}, S, 0, +)$.

Invece posso definire $x^y = z$ in $(\mathbb{N}, S, 0, +, \cdot)$.

Definizione di $x^y = z$ in $(\mathbb{N}, 0, S, +, \cdot)$

(Gödel 1931)

$\langle , \rangle : \mathbb{N}^2 \longrightarrow \mathbb{N}$ bigezione

$$(x,y) \longmapsto \frac{(x+y)(x+y+1)}{2} + x$$

$(0,0) \longmapsto 0$

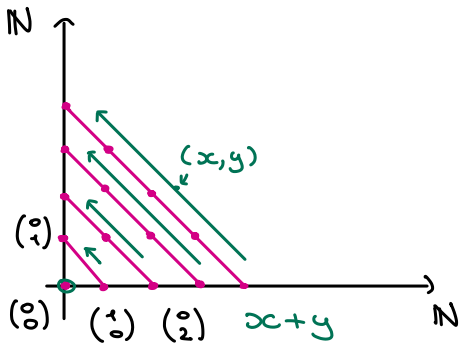
$(0,1) \longmapsto 1$

$(1,0) \longmapsto 2$

$(0,2) \longmapsto 3$

$(1,1) \longmapsto 4$

$\vdots$



Come si dimostra che è una bigezione?

Parto da $1+2+\dots+n = \frac{n(n+1)}{2}$

Posso definirla anche così:

$$\langle x,y \rangle = z \iff 2z = (x+y)(x+y+1) + 2x$$

$$\iff z = \frac{(x+y)(x+y+1)}{2} + x$$

Definisco una relazione $\overset{*}{\in}$ in $\mathbb{N}$:

$$x \overset{*}{\in} c \iff \exists a,b \; c = \langle a,b \rangle \wedge \exists n \; a = mcm\{i \mid i \leq n\} \wedge (x+1)a+1 \mid b \wedge x \leq n$$

↳ questa è definibile in $(\mathbb{N}, 0, S, +, \cdot)$

l'idea è che $c \in \mathbb{N}$ codifica $\{x \mid x \overset{*}{\in} c\}$

$x \mid b := \exists z \, (x \cdot z = b)$

$x \leq y := \exists z \, (x + z = y)$

$a = mcm\{i \mid i \leq n\} := \forall i \, (i \leq n \to i \mid a) \wedge \forall a' \, ((\forall i \leq n)(i \mid a') \to a \mid a')$.

Teorema: per ogni sottoinsieme finito $A \subseteq \mathbb{N}$ esiste $c \in \mathbb{N}$ tale che $A = \{x \in \mathbb{N} \mid \mathbb{N} \models x \overset{*}{\in} c\}$.

$$\mathbb{N} \longrightarrow \mathcal{P}_{fin}(\mathbb{N}) \quad \text{surgettiva}$$

$$c \longmapsto \{x \mid x \overset{*}{\in} c\}$$

Dim: Dato $A \subset \mathbb{N}$ sia $n \in \mathbb{N}$ un maggiorante di tutti gli elementi

di A (A è finito). Sia $c = \langle a, b \rangle$ dove $a = mcm\{i \mid i \le n\}$

$b = mcm\{(x+1)a+1 \mid x \in A\}$. Dico che $x \in A \leftrightarrow (x+1)a+1 \mid b$ ($\leftrightarrow$ ovvia, $x \overset{*}{\in} c$)

Lemma: I numeri $\{(x+1)a+1 \mid x \le n\}$ sono coprimi:

Dim: $x < y < n$ se p primo $p \mid (x+1)a+1$, $p \mid (y+1)a+1$ * se li divide entrambi allora divide la loro diff.

$\overset{(*)}{\Rightarrow} p \mid (y-x)a \Rightarrow p \mid (y-x) \vee p \mid a$ però $p \mid (y-x) \Rightarrow p \mid a$

$(y-x \le n \wedge a = mcm\{i \mid i \le n\})$. In ogni caso $p \mid a$.

Ma $p \mid (x+1)a+1 \Rightarrow p \mid 1$ Assurdo. □

Ora $\boxed{x \in A \rightarrow (x+1)a+1 \mid b}$ $b = mcm((x+1)a+1 \mid x \in A)$ → è il prodotto perché sono coprimi

Se $\boxed{x \notin A \wedge x \le n \Rightarrow (x+1)a+1 \nmid b}$ usando il fatto che se ho dei numeri coprimi $\{(x+1)a+1 \mid x \le n\}$.

$b = mcm\{(x+1)a+1 \mid x \le n \wedge x \in A\}$.

Se un numero è coprimo con certi numeri è coprimo con il loro mcm e quindi non divide il loro mcm. Ne segue che $A = \{x \mid x \overset{*}{\in} c\}$.

Esempio: $A = \{2, 4, 6\}$ lo codifico così:

prendo $n = 6$ maggiorante di A.

$a = mcm(1, \dots, 6) = 60$

$b = mcm((2+1)60+1, (4+1)60+1, (6+1)60+1)$ (coprimi)

$x \in A \leftrightarrow (x+1)60+1 \mid b \wedge x \le 6$

$\leftrightarrow x \overset{*}{\in} c \quad c = \langle a, b \rangle$

- $x^y = z \leftrightarrow$ in $(N, 0, S, +, \cdot)$ vale la seguente:

$\exists c : \langle x, y, z \rangle \overset{*}{\in} c \wedge \langle x, 0, 1 \rangle \overset{*}{\in} c \wedge \forall i < y \; \forall u \; \langle x, i, u \rangle \overset{*}{\in} c \rightarrow \langle x, i+1, u \cdot x \rangle \overset{*}{\in} c$

$\wedge$ c è minimo

$\langle x, y, z \rangle = \langle x, \langle y, z \rangle \rangle$

(cioè $\forall c' < c$ una delle condizioni non vale)

c codifica $\{\langle u, v, z \rangle \mid v \le y \; u^v = z\}$

- $x^y = z \leftrightarrow \exists$ funzione $f : \{0, \dots, y\} \rightarrow N$ tale che $\begin{cases} f(0) = 1 \\ f(i+1) = f(i) \cdot x \\ f(y) = z \end{cases}$ idea: $f(i) = x^i$

19-11-2022 Lezione 15 Prof. Berarducci

Studiare gli insiemi definibili in $(\mathbb{N}, 0, S, +, \cdot)$

Oss: 0, S sono superflui

$x = 0 \iff \forall y\ (x + y = y)$

$x = 1 \iff \forall y\ (x \cdot y = x)$

$y = S(x) \iff y = x + 1 \iff \exists z\ (z = 1 \wedge y = x + z)$

$\varphi(1) \iff \exists z\ (z = 1 \wedge \varphi(z))$

Quindi: Definibili in $(\mathbb{N}, 0, S, +, \cdot)$ = Definibili in $(\mathbb{N}, +, \cdot)$

Teo:
- $\{(x, y, z) \in \mathbb{N}^3 \mid x^y = z\}$ è definibile in $(\mathbb{N}, +, \cdot)$
- $\{(x, y) \in \mathbb{N}^2 \mid x! = y\}$ " " " "
- Se $f : \mathbb{N}^k \to \mathbb{N}$ è "calcolabile" $\{(\bar{x}, y) \in \mathbb{N}^{k+1} \mid f\bar{x} = y\} = \Gamma(f)$ è definibile in $(\mathbb{N}, +, \cdot)$

grafico di f

Funzioni calcolabili: si può fare in molti modi

1) Macchine a registri (modello di calcolo)

Registri: $x_0, x_1, x_2, \ldots$ (o $x, y, z, \ldots$ è uguale) celle di memoria ciascuna delle quali può contenere un intero in $\mathbb{N}$

Istruzioni:

- $x := y$ ⇝ se eseguo questa istruzione al tempo t, al tempo t+1 il contenuto di x è uguale al contenuto di y al tempo t (ie contenuto di y resta uguale)
- $x := 0$ ⇝ Metto 0 in x. Se la eseguo al tempo t, al tempo t+1 in x ci sarà 0
- $x := y + 1$ ⇝ Se la eseguo al tempo t, al tempo t+1 il contenuto di x è uguale al (contenuto di y al tempo t) + 1 (ie contenuto di y resta uguale)

  $x := x + 1$ incremento il contenuto
- if $x = y$ go to n ⇝ Controllo se il contenuto di x è uguale a quello di y. Se lo è la prossima istruzione da eseguire è la numero n. Se non lo è passo all'istr. successiva come per tutte le altre istruzioni.

- STOP

Programma: successione finita numerata di istruzioni

Esempio: P programma.

Specifico i registri $x_1, \dots, x_n$ di input e il registro y di output.

Posso associare una **funzione parziale** (indefinita su certi input ⇝ non si ferma)

$f_P : \mathbb{N}^n \to \mathbb{N}$

$f_P(a_1, \dots, a_n) = b$ se il programma è inizializzato con $a_1, \dots, a_n$ nei registri $x_1, \dots, x_n$ (e/o negli altri) dopo un n° finito di passi si ferma con b in y.

Se il programma non si ferma diciamo $f_P(a_1, \dots, a_n) = \uparrow$ (indefinito)

Quindi in realtà $f_P : \mathbb{N}^n \to \mathbb{N} \cup \{\uparrow\}$

Def: f è calcolabile se $f = f_P$ per qualche programma P

(con certe scelte dei registri di input/output)

Teo: $+ : \mathbb{N}^2 \to \mathbb{N}$ è calcolabile.

Input x_1, x_2. Output y.

Ricorda: possiamo definire la somma induttivamente:

$x + 0 = x$

$x + Sy = S(x + y)$

non va bene come programma: c'è una chiamata ricorsiva (due chiamate del +)

1) $K := 0$ → è un contatore

2) if $K = x_2$ go to 6 → devo fare x_2 iterazioni

3) $x_1 := x_1 + 1$ → aumento di 1 x_1

4) $K := K + 1$

5) go to 2

6) $y := x_1$

STOP

(*) questo ciclo lo ripeto x_2-volte

Esercizio: Avendo + faccio il $\cdot$ $\rightsquigarrow$ $\begin{cases} x \cdot 0 = 0 \\ x \cdot sy = x \cdot y + x \end{cases}$

Input x_1, x_2. Output y.

1) $k := 0$

2) $z := 0$ → idea $z = x_1 \cdot k$

3) if $k = x_2$ go to 7

4) $k := k + 1$

5) $z := z + x_1$ → usando il programma per il +

6) go to 3

7) $y := z$

STOP

Ricorsione primitiva:

$f : \mathbb{N}^{k+1} \to \mathbb{N}$ $\quad g : \mathbb{N}^{k} \to \mathbb{N}$ $\quad h : \mathbb{N}^{k+2} \to \mathbb{N}$

$$\begin{cases} f(\vec{x}, 0) = g(\vec{x}) \\ \quad \vec{x} = (x_1, \dots, x_k) \\ f(\vec{x}, y+1) = h(\vec{x}, y, f(\vec{x}, y)) \end{cases}$$

esempio: dipende da y e dal fattoriale di y

$!0 = 1$

$!(y+1) = (y+1) \cdot !y = h(y, !y)$

dove $h(a, b) = (a+1) \cdot b$

Teo: se g, h calcolabile $\Rightarrow$ f calcolabile

Dim: Input $x_1, \dots, x_n, y$. Output u.

$z := g(\vec{x})$ (macro usando l'ipotesi che g è calcolabile)

$k := 0$ (contatore, idea: $z = f(\vec{x}, k)$)

⊛ se $k = y$ go to ⊛⊛

$z := h(\vec{x}, k, z)$ (macro usando l'ipotesi che h è calcolabile)

$k := k + 1$

go to ⊛

⊛⊛ $u := z$

STOP

Quando scriviamo un programma non abbiamo la garanzia che termini.

Def: La classe delle funzioni primitive ricorsive è la più piccola classe $\mathcal{C}$ di funzioni $f: \mathbb{N}^k \to \mathbb{N}$ (per qualche k variabile) tale che:

1) $0 \in \mathcal{C}$ $\quad$ 0 = funzione costante $0 \to 0: \mathbb{N} \to \mathbb{N}$, $0(x) = 0$

2) $S \in \mathcal{C}$ $\quad$ $S(n) = n+1$

3) $\Pi_i^n \in \mathcal{C}$ $\quad$ $\Pi_i^n(x_1, \dots, x_n) = x_i$ $\quad$ $i \in n$

↓ funzioni proiezione

4) chiusa per composizione: se $f(\vec{x}) = g(h_1(\vec{x}), \dots, h_k(\vec{x}))$ ($\vec{x} = x_1, \dots, x_k$)

se $g, h_1, \dots, h_n \in \mathcal{C} \Rightarrow f \in \mathcal{C}$

5) chiusa per ricorsione primitiva: se f è def. per ric. primitiva da g e h

se $g, h \in \mathcal{C} \Rightarrow f \in \mathcal{C}$

Teo: Le funzioni primitive ricorsive sono calcolabili (e totali) ↓ non entrano mai in loop

Dim: ovvio

Esempio: Programma per funzione sempre indefinita:

1) $x := x+1$

2) go to 1

È calcolabile ma non primitiva ricorsiva.

Teo: Esiste una funzione calcolabile totale non primitiva ricorsiva.

Oss: In termini di programmazione le funzioni primitive ricorsive corrispondono a cicli for. Manca il while.

Minimalizzazione:

$f(x_1, \dots, x_n) = \mu z \cdot h(\vec{x}, z) = 0$

↓ minimo z tale che $h(\vec{x}, z) = 0$ e per ogni $u < z$, $h(\vec{x}, z) \neq 0$ ma definito

Teo: h calcolabile $\Rightarrow$ f calcolabile

Dim: idea. calcolo $h(\vec{x}, 0), h(\vec{x}, 1), h(\vec{x}, 2), \dots$

finché trovo $h(\vec{x}, z) = 0$ e fornisco output z

Esempio: se $h(\vec{x},0)=3$, $h(\vec{x},1)=\uparrow$, $h(\vec{x},2)=0 \Rightarrow f(\vec{x})=\uparrow$

Input $x_1,\dots,x_n$.

1) $z := 0$

2) $u := h(\vec{x},z)$ (macro)

3) Se $u=0$ vai al punto 5

4) $z := z+1$, vai a 2

5) $y := z$

STOP

Def: funzioni μ-ricorsive di Kleene

Sono la più piccola classe di funzioni chiuse per $0, S, \Pi_i^n$, comp., ricorsione primitiva e minimalizzazione μ.

Teo: funzioni μ-ricorsive = funzioni calcolabili (a registri)

Dim:

$\leq$) facile

$\geq$) si fa (dispense)

:= è un concetto informatico, non matematico

Precisazioni: $\mathrm{dom}(f) = \{\vec{x} \mid f\vec{x} \neq \uparrow\}$

se $\begin{cases} f(\vec{x},0) = g(x) \\ f(\vec{x},y+1) = h(x,y,f(x,y)) \end{cases} \Rightarrow \begin{cases} f(x,y)\downarrow \overset{\text{def}}{\Leftrightarrow} g(x)\downarrow \text{ e} \\ \forall i<y \ \ f(x,i)\downarrow \text{ e } h(x,y,f(x,i))\downarrow \end{cases}$

(converge, ossia è $\neq \uparrow$)

Se g ed h sono funzioni parziali definisco f in questo modo

$f(x) = g(h_1 x,\dots,h_k x)$ $\quad f x\downarrow \leftrightarrow h_1 x,\dots,h_k x\downarrow$ e $g(h_1 x,\dots,h_k x)\downarrow$

$f(x) = \mu z\, h(x,z)=0$ allora $f(x)\downarrow$ se $\exists z\ h(x,z)=0 \wedge \forall i<z\ h(x,z)\downarrow \neq 0$

Tesi di Church:

La nozione intuitiva di funzione calcolabile (esiste algoritmo) coincide con la nozione di funzione calcolabile a registri.

Ci crediamo perché:

calcolabile a registri = μ-ricorsivo

= Turing calcolabile

= λ-calcolabile

= altre definizioni ...

Esempio: $f(n)$ = n-esima cifra dello sviluppo di π è calcolabile per la Tesi di Church

"Lo so fare con le serie, lo saprò fare anche con le macchine a registri"

Oss: Calcolabile significa che esiste un programma ma ciò non implica che io lo conosca.

Ci sono funzioni calcolabili che non sappiamo calcolare.

Esercizio: $n \longmapsto p_n$ (n-esimo primo) è μ-ricorsiva (anche prim. ricorsiva)

Servono un po' di funzioni ausiliarie:

1) $p: \mathbb{N} \to \mathbb{N}$ $\quad p(0)=0$ $\quad p(n+1)=n$ predecessore

p è primitiva ricorsiva

$$\begin{cases} p(0)=0 \\ p(n+1)=h(n,p(n)) \end{cases} \quad \text{con} \quad h(x,y)=x = \pi_1^2$$

2) $x \dot{-} y = \begin{cases} x-y & \text{se } x \geq y \\ 0 & \text{se } x < y \end{cases}$ sottrazione troncata a zero

$\dot{-}$ è primitiva ricorsiva

$$\begin{cases} x \dot{-} 0 = x \\ x \dot{-} (y+1) = p(x \dot{-} y) \end{cases}$$

Def: Se $P \subseteq \mathbb{N}^n$ (P = predicato) dico che P è primitivo ricorsivo se:

$\chi_P : \mathbb{N}^n \to \{0,1\}$ è primitiva ricorsiva

$$\chi_P(\bar{x}) = \begin{cases} 1 & \text{se } \bar{x} \in P \\ 0 & \text{se } \bar{x} \notin P \end{cases}$$

3) $z(x) \equiv (x = 0)$ è primitivo ricorsivo predicato "essere zero"

$z(0) = 0$, $z(n+1) = h(n, z(n))$ con $h(x,y) = 1$

Oss: Le funzioni costanti sono primitive ricorsive

4) $\leq$ (inteso come predicato) è primitivo ricorsivo

$x \leq y \iff z(x \dot{-} y)$

5) $=$ è primitiva ricorsiva

$x = y \iff x \leq y \wedge y \leq x$ (*)

6) $\wedge$ è primitiva ricorsiva

$\chi_{\leq}(x,y) \cdot \chi_{\leq}(y,x)$ con 1 = vero, 0 = falso

(*) $\chi_{=}(x,y) = \chi_{\leq}(x,y) \cdot \chi_{\leq}(y,x) = \chi_{\leq}(x,y) \cdot \chi_{\leq}(\pi_2^2(x,y), \pi_1^2(x,y))$

7) Se $P \subseteq \mathbb{N}^k$ (come predicato) prim. ric. $\Rightarrow \neg P = \mathbb{N}^k \setminus P$ è prim. ric.

$\chi_{\neg P}(x) = 1 \dot{-} \chi_P(x)$

8) $P \vee Q \equiv \neg(\neg P \vee \neg Q)$

$\chi_{P \vee Q}(x) = 1 \dot{-} (1 \dot{-} \chi_P(x)) \cdot (1 \dot{-} \chi_Q(x))$

⋮

n) $\text{Primo}(x) \equiv \forall a\, b \leq x\, (a \cdot b = x \to a = x \vee b = x)$

i quantificatori limitati non fanno uscire dai primitivi ricorsivi

Esempi: funzioni calcolabili che non sappiamo calcolare:

1) $$f(x) = \begin{cases} 1 & \text{se non vale la congettura di Riemann} \\ 0 & \text{se vale} \quad " \quad " \quad " \quad " \end{cases}$$

2) funzione che dato n mi dice se tra n giorni piove

Lo posso fare aspettando n giorni ma non con una macchina a registri

L'idea è che con una macchina a registri io possa dimezzare i tempi delle operazioni, ma non posso far scorrere il tempo a vel. 2x!

22-11-2021 Lezione 16 Prof. Berarducci

Lo scopo finale è dimostrare che PA è incompleta.

Abbiamo visto:

- Primitive ricorsive $\subset$ Ricorsive $\subset$ μ-Ricorsive $=$ Intuitivamente Calcolabili
  totali (l'algoritmo termina sempre) — μ-Ricorsive $=$ Calcolabili a registri ← Teo — $=$ Intuitivamente Calcolabili ↑ tesi di Church

Oss: Ricorsive totali := Ricorsive $\cap$ funzioni totali

↓

Non posso definirle senza $\cap$

La funzione di Ackermann è calcolabile ma non primitiva ricorsiva:

$$Ack : \mathbb{N}^2 \to \mathbb{N}, \begin{cases} Ack(x,0) = x+1 \\ Ack(x+1,0) = Ack(x,1) \\ Ack(x+1,y+1) = Ack(x, Ack(x+1,y)) \end{cases}$$

Sfida: Calcolare $Ack(5,5)$ (È un numero enorme)

$Ack(5,5) = Ack(4, \underbrace{Ack(5,4)}_{\text{è più grande di 5}}) =$ ecc. Ci vogliono migliaia di anni!

Esercizio: Perché è intuitivamente calcolabile e perché è totale?

È totale (il calcolo di $Ack(x,y)$ termina) per induzione su $\omega x + y$ (ordinale)

$Ack(5,5) \rightsquigarrow \omega \cdot 5 + 5$

$Ack(5,4) \rightsquigarrow \omega \cdot 5 + 4$ per induzione termina $Ack(5,4) = n$

$Ack(5,5) = Ack(4,n) \rightsquigarrow \omega \cdot 4 + n < \omega \cdot 5 + 5$ per ind. termina

Senza ordinali: Induzione primaria sul I termine,

Induzione secondaria sul II termine

cioè, per induzione su x, mostro $\forall y$ $Ack(x,y)$ termina

Esercizio: Ack è μ-ricorsiva e calcolabile a registri

Teo: f è primitiva ricorsiva $\to \exists k \ \forall n > k \quad f(n) < Ack(n,n)$

- Sono primitive ricorsive:

$+, \cdot$, pred., $x \dot{-} y$, il predicato $\chi_{=0}(0)=1$, $\chi_{=0}(x+1)=0$

$\chi_{=}(x,x)=1$, $\chi_{=}(x,y)=0$ se $x \neq y$

- $\chi_{\leq}(x,y) = \begin{cases} 1 & \text{se } x \leq y \\ 0 & \text{se } x > y \end{cases}$ è primitiva ricorsiva

Dim: $x \leq y \leftrightarrow x \dot{-} y = 0$

$\chi_{\leq}(x,y) \leftrightarrow 1 \dot{-} \chi_{=0}(x \dot{-} y)$

$\chi_{=}(x,y) = \chi_{\leq}(x,y) \cdot \chi_{\leq}(y,x)$

Sommatorie:

$$f(x,y) = \sum_{z<y} h(x,z)$$

- Se h è prim. ricorsiva (ric. totale calcolabile) $\Rightarrow$ f è prim. ric. (ric. totale calcolabile)

Dim: $f(x,0) = 0$

$f(x,y+1) = f(x,y) + h(x,y)$

Produttorie:

$$f(x,y) = \prod_{z<y} h(x,z)$$

- Se h è P.R. $\Rightarrow$ f è P.R.

Dim: $f(x,0) = 1$

$f(x,y+1) = f(x,y) \cdot h(x,y)$

Minimalizzazione:

$$f(\vec{x}) = \min\{ z \mid \underbrace{h(\vec{x},z)=0 \wedge \forall i<z \; h(\vec{x},i)\downarrow \neq 0}_{*} \}$$

def. $\Vert$

$\mu z \cdot h(\vec{x},z) = 0$

Perché lo definisco così? Se provo a fare un programma per macchina a registri mi è più facile calcolare (*) che il minimo z

Esempio: $h(\vec{x},0)=3$ $h(x,1)\uparrow$, $h(x,2)=0$ $\Rightarrow$ $f(\vec{x})\uparrow$

In questa situazione non riesco a trovare il 2

Domanda: Esiste un programma "furbo" che trova il 2? No

Se la h è totale μ coincide con il vero minimo (il prog. non si ferma)

Se la h è parziale potrebbe non coincidere (come nell'esempio)

h calcolabile $\Rightarrow$ f calcolabile (in generale non P.R.)

Minimalizzazione limitata

$$f(\vec{x},y)=\begin{cases}\min\{z<y \mid h(\vec{x},z)=0 \wedge \underbrace{\forall i<z \;\; h(\vec{x},i)\downarrow \neq 0}_{\text{se } h \text{ è totale non serve}}\} \\ y\end{cases}$$

$$:= \mu z<y\,[h(\vec{x},z)=0]$$

Teo: Se h è P.R. $\Rightarrow$ f è P.R.

h è P.R. $\overset{(*)}{\Rightarrow}$ totale

Dim: $f(x,y)=\sum_{v<y}\prod_{u<v} \underbrace{sg(h(x,u))}_{0,1}$

$\underbrace{\qquad\qquad}_{c(x,v)}$

$c(x,v)$ è un parametro: potrebbe starci o non starci

$$\begin{cases} sg(0)=0 \\ sg(x+1)=1 \end{cases} \Rightarrow \text{sarebbe } \neg\chi_{=0}$$

$c(x,v)=1 \leftrightarrow \forall u<v \;\; h(x,v)\neq 0$

$c(x,v)=0 \leftrightarrow \exists u<v \;\; h(x,u)=0$

$f(x,y)$ conta quanti $v<y$ ci sono con $c(x,v)=1$

Se z è minimo tale che $h(x,z)=0$ $\Rightarrow$ se $y \geq z$ $\quad f(x,y)=z$

$y<z$ $\quad f(x,y)=y$

□

Schema:

c	h
1	}
1	}
1	} sono esattamente z
1	}
0	
0	
0	
⋮	

Predicati (o Relazioni) decidibili o P.R.

$P \subseteq \mathbb{N}^n$ scrivo $P(x_1,\dots,x_n)$ se $(x_1,\dots,x_n)\in P$

P è decidibile se $\chi_P : \mathbb{N}^n \to \{0,1\}$ è calcolabile
P.R. P.R.

Prop: Se $f:\mathbb{N}^k \to \mathbb{N}$ è calcolabile totale

$\Rightarrow \Gamma(f) = \{(x_1, \dots, x_k, y) \mid f(x_1, \dots, x_k) = y\}$ è decidibile

Dim: $\chi_{\Gamma(f)}(\vec{x}, y) = \chi_=(f(\vec{x}), y)$

Prop: P predicato P. R. $\Rightarrow \neg P$ P.R.

Dim. $\chi_{\neg P}(x) = 1 - \chi_P(x)$

Definizioni per casi

$$g(x) = \begin{cases} f_1(x) & \text{se } P(x) \\ f_2(x) & \text{se } \neg P(x) \end{cases}$$

Oss: Tutto ciò che dico su P. R. vale anche per le calcolabili totali

se f_1, f_2, P sono P. R. $\Rightarrow g$ è P. R.

Dim: $g(x) = f_1(x) \cdot \chi_P(x) + f_2(x) \cdot \chi_{\neg P}(x)$

Algebra di Book degli insiemi decidibili

$A, B \subset \mathbb{N}^k$ decidibili $\Rightarrow A \cap B$, $A \cup B$, $\sim A = \mathbb{N}^k \setminus A$ sono decidibili

Dim: $\chi_{A \cap B}(x) = \chi_A(x) \cdot \chi_B(x)$

$\chi_{\sim A}(x) = 1 \dot{-} \chi_A(x)$

$\chi_{A \cup B}(x) = 1 - (\chi_{\sim A}(x) \cdot \chi_{\sim B}(x))$

- $A \cup B = \sim(\sim A \cap \sim B)$
- $A \to B \equiv \neg A \vee B$

Quantificatori limitati

Prop: $P(\vec{x}, y) \equiv \forall z < y \; R(\vec{x}, z)$ $\rightsquigarrow$ ||definibili| > |calcolabili|

- R prim. ric. $\Rightarrow$ P è prim. ric.

Dim: $\chi_P(\vec{x}, y) = \prod_{z<y} \chi_R(\vec{x}, z)$

Prop: $P(\vec{x}, y) \equiv \exists z < y \; R(\vec{x}, z)$

Se R è P.R. $\Rightarrow$ P è P. R.

Dim: $\underbrace{\exists z < y \; R(\vec{x}, z)}_{\text{LAL}} \equiv \neg \forall z < y \; \neg R(\vec{x}, z)$

Esempio: "x è primo" è P.R.

Dim: "x è primo" $\Leftrightarrow \forall a, b \leq x \; [\underbrace{a \cdot b = x \to a = x \vee b = x}_{\text{mi basta verificare che è P.R.}}]$

(*)

$$(*)\begin{cases} \text{implies}(\chi_=(a\cdot b,x),\ \text{or}(\chi_=(a,x),\chi_=(b,x))) \\ \text{or}(x,y)=1-(1-x)(1-y)=\text{not}(\text{and}(\text{not}\,x,\text{not}\,y)) \\ \text{and}(x,y)=x\cdot y \\ \text{not}(x)=1-x \\ \text{implies}=\text{or}(\text{not}\,x,y) \end{cases}$$

leggi di De Morgan

con $x,y \in \{0,1\}$

Dunque x è primo è primitivo ricorsivo

n-esimo primo:

$n \mapsto p(n)$ = n-esimo numero primo è primitiva ricorsiva

Dim: $p(0)=2$

$p(n+1)=\text{next}(p(n))$

dove $\text{next}(x)=\mu y < 2x$ "y è primo"

C'è sempre un primo tra x e $2x$ (Bertrand)

Funzione calcolabile che non so calcolare

$$f(x)=\begin{cases} 1 & \text{se esiste } y>x : y \text{ e } y+2 \text{ sono primi} \\ 0 & \text{altrimenti} \end{cases}$$

Calcoliamo:

$f(0)=1$, $f(1)=1$, $f(2)=1$, $f(3)=1$, ..., $f\left(2^{2^{2^{2^{100}}}}\right) \overset{(*)}{=} ?$

Non si sa se esistono infiniti numeri primi gemelli.

Quindi non so calcolare $(*)$.

Però f è calcolabile.

Dim: • Se esistono infiniti primi gemelli $\Rightarrow f$ è costante $\Rightarrow f$ è calc.

• Se NON " " " " $\Rightarrow f$ è costante $=1$ fino ad un certo punto e poi costante $=0$ da lì in poi $\Rightarrow f$ è calcolabile

Oss: La dim. usa il 3° escluso $\rightarrow$ NON è intuizionista

Codifiche:

Una successione $(a_n \mid n \in \mathbb{N})$ di numeri naturali ha supporto finito se $\{n \mid a_n \neq 0\}$ è finito.

Esiste una bigezione tra $\mathbb{N}$ ~ succ. a supporto finito

Oss: $|\{\text{successioni}\}| = 2^{\aleph_0}$

Sol: $\prod_{n \in \mathbb{N}} p(n)^{a_n} \longleftrightarrow (a_n \mid n \in \mathbb{N})$

Siccome la successione è a supporto finito, per n abb. grande $a_n = 0 \Rightarrow$

$\Rightarrow p(n)^{a_n} = 1$ e per convenzione il prodotto è finito.

È biunivoca perché riesco a tornare facilmente indietro (fattorizzo).

Domanda: questa bigezione è calcolabile? Non ha senso perché ho def. la calcolabilità solo da $\mathbb{N}^k$ a $\mathbb{N}$. Però ha senso chiedersi se certe funzioni associate a questa bigezione sono calcolabili.

Estrazioni di componenti:

$\pi : \mathbb{N}^2 \to \mathbb{N}$ questa la so calcolare

$\pi(s,i) = (s)_i$ = l'esponente di $p(i)$ nella scomposizione in primi di s.

π è calcolabile (P.R.)

$\pi(s,i) = \mu k < s \; \underbrace{p(i)^{k+1} \nmid s}$

P.R. $a \mid b \leftrightarrow \exists z \leq b \; (a \cdot z = b)$

Esempio: $\pi(100,2) = 2$

$100 = 2^2 \cdot 5^2 = 2^2 \cdot 3^0 \cdot 5^{\boxed{2}} \to p(0) = 2,\ p(1) = 3,\ p(2) = 5$

Codifica coppie:

$\langle x,y \rangle = \frac{(x+y+1)(x+y)}{2} + x$ è P.R.

$\langle x,y \rangle = z \Leftrightarrow 2z = (x+y+1)(x+y) + 2x$

$\langle x,y \rangle = \mu z < (x+y+1)^5 \cdot [2z = (x+y+1)(x+y) + 2x]$

↓ minimo e unico z

Decodifica:

$P_1 \langle x, y \rangle = x \quad P_2 \langle x, y \rangle = y$ sono P.R.

Dim: $P_1(n) = \mu x \leq n \, (\underbrace{\exists y \leq n \;\; n = \langle x, y \rangle}_{\text{P.R.}})$

Idem per P_2.

Esercizio: Fibonacci è P.R.

$f(0) = 0 \,, \; f(1) = 1 \,, \; f(n+2) = f(n) + f(n+1)$

Dim: idea: la funzione $\langle f(n), f(n+1) \rangle \longrightarrow \langle f(n+1), f(n+2) \rangle$ è P.R.

$g(n) = \langle f(n), f(n+1) \rangle$

$g(0) = \langle 0, 1 \rangle \in \mathbb{N}$

$g(n+1) = \langle f(n+1), f(n+2) \rangle$

$= \langle P_2(g(n)), \; P_1(g(n)) + P_2(g(n)) \rangle$

$= H(g(n))$

$H(x) = \langle P_2 x, \; P_1 x + P_2 x \rangle$

□

Ricorsione sul decorso dei valori:

$f(n) = h(n, \underbrace{\langle f_0, f_1, \dots, f_{(n-1)} \rangle}_{\text{codificato con un singolo numero}})$ → dipende da tutti i valori precedenti

h P.R. ⇒ f P.R.

26-11-2024 lezione 17 Prof. Berarducci

Torno alla $\aleph_1$-categoricità di $TR(\mathbb{N}, 0, S)$

Considero la teoria con assiomi:

$$T_{0,S} = \begin{cases} \forall xy \, (Sx = Sy \to x = y) \\ \forall x \, (x \neq 0 \to \exists y \; Sy = x) \\ \forall y \, (Sy \neq 0) \\ \forall x \, (\varphi, x) : \forall \vec{y} \, [\varphi[0/x] \wedge \forall u \, \varphi[u/x] \to \varphi[Su/x] \to \forall z \, \varphi[z/x]] \end{cases}$$

↳ Schema di induzione

$VL(\varphi) \subseteq \{\vec{y}, x\}$

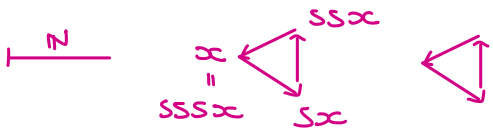
Teo: $T_{0,S}$ è $\aleph_1$-categorica, quindi completa, quindi $T_{0,S} \equiv Th(\mathbb{N}, 0, S)$

Senza schema di induzione non è $\aleph_1$-categorica:

Modelli: ① $\mathbb{N} \dot\cup \underbrace{\mathbb{Z}/(2) \dot\cup \dots \dot\cup \mathbb{Z}/(2)}_{\aleph_1\text{-copie}} \dot\cup \mathbb{Z}$ (con o senza l'induzione questi ci possono essere)

Grafo: 

② $\mathbb{N} \dot\cup \underbrace{\mathbb{Z}/(3) \dot\cup \dots \dot\cup \mathbb{Z}/(3)}_{\aleph_1\text{-copie}} \dot\cup \mathbb{Z}$

Grafo: 

⚠ ① $\not\equiv$ ② $\Rightarrow$ $T_{S,0}$ senza induzione non è $\aleph_1$-categorica

$T_{S,0}$ (con induzione) $\vdash$ non ci sono cicli

$\forall n \in \mathbb{N} \quad T_{S,0} \vdash \forall x \, (\underbrace{ssss \dots s}_{n\text{-volte}}(x) \neq x)$

Ad esempio, $n=2$:

$\varphi_2(x) \equiv$ "x non appartiene a un ciclo di lunghezza 2"

$\equiv (ssx \neq x)$

1) $T_{S,0} \vdash \varphi_2(0)$ perché $0 = ss0 \Rightarrow \exists x \; 0 = sx \Rightarrow \bot$

2) $T_{S,0} \vdash \forall u \, [\varphi_2(u) \to \varphi_2(su)]$ perché se $ss(su) = su$ ma s è iniettiva $\Rightarrow ssu = u \Rightarrow \bot$

Ind. ↑

3) $T_{S,0} \vdash \varphi_0(0) \wedge \forall u \, [\varphi_2(u) \to \varphi_2(su)] \to \forall u \, \varphi_2(u)$

4) $T_{S,0} \vdash \forall u \, \varphi_2(u)$

Cor: $T_{S,0}$ (con induzione o senza cicli) è $\aleph_1$-categorica.

$M \models T_{S,0}$, considero un $a \in M \setminus \underbrace{\{s^n 0 \mid n \in \mathbb{N}\}}_{=\mathbb{N}}$ "non standard" e una mappa:

$\mathbb{Z} \longrightarrow M$

$n \longmapsto \begin{cases} (s^n a) & \text{se } n > 0 \\ p^{|n|} a & \text{se } n < 0 \end{cases}$ cioè $\quad -1 \mapsto p(a) =$ l'unico x : $sx = a$, $\; 0 \mapsto a$, $\; 1 \mapsto sa$

Questa mappa è iniettiva perché non ci sono cicli.

Sia $a \sim b$ se $\exists n \; s^n a = b \vee s^n b = a$. È una relazione di equivalenza su $M \setminus \mathbb{N}$. Scelgo un rappresentante a_i in ciascuna classe $i \in I$

$M \cong \mathbb{N} \cup \bigcup_{i \in I} [a_i]$, $[a_i] \cong \mathbb{Z}$, allora $|M| = \aleph_1 \iff |I| = \aleph_1$

Dunque l'unico modello di cardinalità $\aleph_1$ è $\mathbb{N} \cup \aleph_1$-copie di $\mathbb{Z}$

Quindi $T_{s,0}$ è $\aleph_1$-categorica.

Quindi $T_{s,0}$ è completa

$\Rightarrow T_{s,0} = Th(\mathbb{N}, 0, s)$

$\Rightarrow Th(\mathbb{N}, 0, s)$ $\aleph_1$-categorica

Domanda: Come mai con l'induzione riesco a escludere copie di $\mathbb{Z}/(n)$ in un modello M di $T_{s,0}$ ma non a escludere copie di $\mathbb{Z}$?

$\varphi_2(x) \equiv$ "x non appartiene a cicli di lunghezza 2"

Io riesco a scrivere

$\varphi_{\mathbb{Z}}(x) \equiv$ "x non appartiene a una copia di $\mathbb{Z}$"

non lo riesco a scrivere

Nella logica del secondo ordine la scrivo:

$\varphi(x) \equiv \forall P \; [P(0) \wedge (\forall u \; P(u) \to P(su)) \to P(x)]$ dice x è standard

$Th(\mathbb{N}, s, 0)^{2° \text{ ordine}}$ è categorica

Unico modello $\cong \mathbb{N}$ (non possono essere non-standard)

$Th(\mathbb{N}, s, 0)^{2° \text{ ordine}} \vdash \forall P \; (P0 \wedge \forall u \; (Pu \to P(su)) \to \forall x \; P(x))$

Precisazioni:

- Come faccio a dire che i modelli ① $= M_1$ e ② $= M_2$ del 1° esempio non sono isomorfi? Sia x in M_1 e y in M_2, allora per la teoria dei gruppi ho $ssx = x$ e $ssy = y$. Sia φ un isomorfismo:

$\varphi : M_1 \xrightarrow{\cong} M_2$

$x \longmapsto y$

$Sx \longmapsto Sy$

$SSx = x \longmapsto y \neq SSy$

Sostanzialmente segue dal fatto che

$\mathbb{Z}/(2) \not\cong \mathbb{Z}/(3) \Rightarrow M_1 \not\cong M_2$

- Ciò che abbiamo detto se φ_2 vale anche per φ_m con $m \in \mathbb{N}$
- Lo zero del modello è solo lo zero di $\mathbb{N}$, è diverso dallo zero di $\mathbb{Z}/(2)$. Cosa significa $\dot\cup$?

$$\mathbb{N} \dot\cup \bigcup_{i \in \mathbb{N}_1} \mathbb{Z}/(2) = \mathbb{N} \cup [\mathbb{N}_1 \times \mathbb{Z}/(2)]$$

(formalmente)

con $S : M \to M$ definito così. $S(n) = n+1$ se $n \in \mathbb{N}$

$S(\alpha, 0) = (\alpha, 1)$ con α ordinale

$S(\alpha, 1) = (\alpha, 0)$ $\quad \{0,1\} \in \mathbb{Z}/(2)$

Lo zero del modello è lo zero di $\mathbb{N}$!

$0^M = 0^N$

Gli elementi del modello sono fatti così:

$M = \{0, 1, 2, \dots, (0,0), (0,1), (1,0), (1,1), \dots\}$

$0, 1, 2, \dots$: S S S $\dots$ → $\mathbb{N}$

$(0,0), (0,1)$: S, S → $\mathbb{N}_1 \times \mathbb{Z}/(2)$ cioè tanti cicli → non hanno un nome

$(1,0), (1,1)$: S, S → $\mathbb{N}_1 \times \mathbb{Z}/(2)$ cioè tanti cicli → non hanno un nome

$= 0^M$ è l'unico a non avere un predecessore

→ NON vale lo schema di induzione, gli altri assiomi sì

Esempio: $Th(\mathbb{N}, 0, S, +) \geq T_{S,0,+}$

Assiomi di $T_{S,0,+}$

$$\begin{cases} \forall x \; 0 \neq Sx \\ \forall xy \; Sx = Sy \to x = y \\ \forall x \; x + 0 = x \\ \forall xy \; x + Sy = S(x+y) \\ \forall x \; x \neq 0 \to \exists y \; Sx = y \end{cases}$$

$T_{S,0,+}$ è completa (non α-categorica) → devo dim. la completezza in un altro modo

quindi $T_{0,S,+} \equiv Th(\mathbb{N}, 0, S, +)$

quindi $Th(\mathbb{N}, 0, S, +)$ è decidibile.

Domanda: Cosa succede se aggiungo il $\cdot$?

$Th(\mathbb{N}, 0, S, +, \cdot) \geq PA$

Assiomi di PA

$\forall x \; 0 \neq Sx$

$\forall xy \; Sx = Sy \to x = y$

$\forall x \; x + 0 = x$

$\forall xy \; x + Sy = S(x + y)$

$\forall x \; x \neq 0 \to \exists y \; Sx = y$

$\forall x \; x \cdot 0 = 0$

$\forall xy \; x \cdot Sy = x \cdot y + x$

Schema di induzione

Gödel: PA non è completa, quindi esistono formule φ vere in $\mathbb{N}$ nel linguaggio $L = \{0, S, +, \cdot\}$ non dimostrabili in PA.

Come lo dimostro? Strategia:

Teo: $\{\varphi \mid \varphi \text{ vera in } \mathbb{N}\} = Th(\mathbb{N}, 0, S, +, \cdot)$ non è decidibile

Se coincidesse con i teoremi di PA sarebbe decidibile. $\lightning$.

Funzioni Calcolabili:

- Insiemi / Predicati decidibili $\supseteq$ Primitivi ricorsivi
  - ↓ quelli la cui funzione caratteristica è calcolabile
  - ↳ la cui f. caratteristica è primitiva ricorsiva
- Predicati → funzioni → funzioni caratteristiche → insiemi
- I sottoinsiemi decidibili di $\mathbb{N}^k$ sono:

① Un'algebra di Boole (chiusi per $\cup, \cap, \tilde{}$ (complementare)) $\rightsquigarrow \wedge, \vee, \neg$

② Sono stabili per quantificatori limitati

$M(\vec{x}, y) \equiv \forall z < y \; R(\vec{x}, z)$ R decidibile → M decidibile

idem per

$M(\vec{x}, y) \equiv \exists z < y \; R(\vec{x}, z)$

Dim: Considero $P(\vec{x}, u, y) \equiv \forall z < y \; R(\vec{x}, z, u)$

$M(\vec{x}, y) \equiv P(\vec{x}, y, y)$ (R decid. ⇒ P decid. ⇒ M decid.)

Esempio: $f(x) = \mu z \, [h(x, z) = 0]$

$f(x, y) = \mu z < y \, [h(x, z) = 0]$

h calcolabile → f calcolabile e h P.R. → f P.R.

Predicati semi-decidibili:

$S \subseteq \mathbb{N}^m$ è semi decidibile se esiste un predicato decidibile $R \subseteq \mathbb{N}^{m+1}$ tale che $S(x_1, \dots, x_m) \equiv \exists y \; R(x_1, \dots, x_m, y)$ con $(x_1, \dots, x_m) \in S$

Oss: R decidibile $\Rightarrow$ R semi-decidibile

$R(\vec{x}) \equiv \exists y R(\vec{x}) \equiv \exists y \, (y=y \wedge R(\vec{x}))$

Prop (Teorema di Post):

Sia $A \subseteq \mathbb{N}^m$. Se A e $\sim A = \mathbb{N}^m \setminus A$ sono semi-decidibili $\Rightarrow$ A è decidibile

Dim $A(\vec{x}) \equiv \exists y \, R(\vec{x}, y)$ $\quad \neg A(x) \equiv \exists y \, S(\vec{x}, y)$ con R, S decidibili

$f(x) = \mu y [R(\vec{x}, y) \vee S(\vec{x}, y)]$

$= \mu y [h(\vec{x}, y) = 0]$ con $h = \chi_{R \vee S}(\vec{x}, y)$

f è calcolabile (perché fatta con μ).

f è totale.

$A(\vec{x}) \equiv R(\vec{x}, f(\vec{x}))$

è composizione di f caratt. totali

$\chi_A(\vec{x}) = \chi_R(\vec{x}, f(\vec{x}))$ □

Semidecidibile = Ricorsivamente enumerabile:

Def: $S \subseteq \mathbb{N}$ è ricorsivamente enumerabile (r.e.) se o è vuoto oppure $S = \mathrm{Im} f$ con f calcolabile totale cioè S me lo scrivo come $S = \{f(0), f(1), f(2), \dots\}$

Un sottoinsieme di un insieme numerabile è numerabile.

Ma un sottoinsieme di un insieme ricorsivamente enumerabile non è detto che sia ricorsivamente enumerabile.

Teorema: Se S è r.e. $\Rightarrow$ S è semidecidibile

Dim: Sia $S \subseteq \mathrm{Im} f$ con f calcolabile $\overset{\text{uso def. di Im}}{\Rightarrow}$ $S = \{ y \mid \exists x \; f(x) = y \}$

$f(x) = y$ decidibile perché è $\chi_=(f(x), y)$ ed è calcolabile

Teorema: S semidecidibile $\Rightarrow$ S ric. enum.

Dim: $S = \{x \mid \exists x \; R(x, y)\}$ con R decidibile

1) Se $S=\emptyset \Rightarrow S$ è R.E. per def.

2) Se $S\neq\emptyset$ fisso $a\in S$ e def. $g:\mathbb{N}^2\to\mathbb{N}$ tc $g(x,y)=\begin{cases} x & \text{se } R(x,y) \\ a & \text{se } \neg R(x,y)\end{cases}$

$\text{Im}g=S$, g è totale e calcolabile ma va da $\mathbb{N}^2$ a $\mathbb{N}$.

La voglio da $\mathbb{N}\to\mathbb{N}$. Quindi $f:\mathbb{N}\to\mathbb{N}$, $f=g\circ\gamma$ cioè

$\mathbb{N} \xrightarrow[\cong]{\gamma} \mathbb{N}^2 \xrightarrow{g} \mathbb{N}$, infatti $\mathbb{N}^2\cong\mathbb{N}$ $(\aleph_0\cdot\aleph_0=\aleph_0)$

f

$f(n)=g(P_1(n),P_2(n))$ perché $f(\langle x,y\rangle)=g(x,y)$, $\text{Im}f=S$

↳ $n=\langle a,b\rangle$, $P_1(n)=a$, $P_2(n)=b$

Teo: Se $A=\text{Im}f$ con $f:\mathbb{N}\to\mathbb{N}$ str. crescente $\Rightarrow A$ è decidibile

Dim: $n\in A \Leftrightarrow \underbrace{\exists x<n}_{\text{limitato}}\ \underbrace{[f(x)=n]}_{\text{decidibile}}$ — decidibile

Teo: Se $A=\text{Im}f$ con $f:\mathbb{N}\to\mathbb{N}$ deb. crescente $\Rightarrow A$ è decidibile

Dim:

- A finito $\Rightarrow A$ decidibile
- A infinito $\Rightarrow$ sia $g(n)=\mu x\,[f(x)>n]$ → g è totalmente calcolabile perché A è infinito

$n\in A \Leftrightarrow \underbrace{\exists x\le g(n)\,[f(x)=n]}_{\text{decidibile}}$

29-11-2024 Lezione 18 Prof. Berarducci

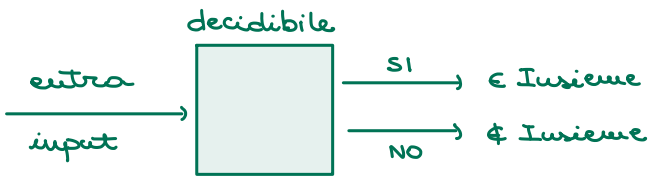
Notazione:

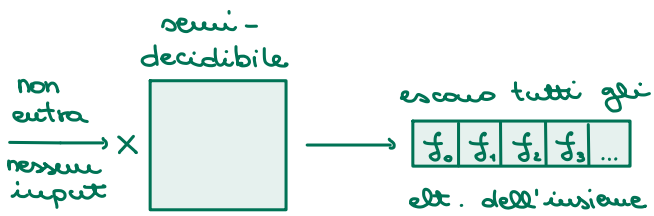
- $\forall x<y\ \ \varphi \equiv \forall x\,(x<y\to\varphi)$
- $\exists x<y\ \ \varphi \equiv \exists x\,(x<y\wedge\varphi)$

Oss: I predicati decidibili sono chiusi per $\wedge,\vee,\neg,\underbrace{\exists x<y,\forall x<y}_{\text{limitati}}$

Teo: I predicati semidecidibili sono chiusi per $\wedge,\vee,\exists x,\forall x<y$

Idea (Post):





Dim: Sia S semidecidibile $\Rightarrow \exists R$ decidibile tale che $S = \exists y R$ cioè

$S(x) \equiv \exists y\, R(x,y) \qquad x = (x_1, \dots, x_n)$

$\wedge$ $\exists y\, R_1(x,y) \wedge \exists y\, R_2(x,y) \qquad R_1, R_2$ decidibili

$\equiv \exists y \exists z\, [R_1(x,y) \wedge R_2(x,z)]$ (in tutte le strutture)

$\vee$ $\exists y R_1(x,y) \vee \exists y R_2(x,y) \equiv \exists y\, [R_1(x,y) \vee R_2(x,y)]$ (in tutte le str.)

$\exists$ $\exists z \exists y\, R(x,y,z) \equiv \exists t\, (\underbrace{\exists z < t \;\; \exists y < t \;\; R(x,y,z)}_{\text{decidibile}})$

$\forall x < y$ $\forall x < y\, (\exists z\, \underbrace{R(x,y,z,\_)}_{\text{decidibile}}) \equiv \exists t\, \underbrace{\forall x < y \;\; \exists z < t\, R(x,y,z,\_)}_{\text{decidibile}}$ (in $\mathbb{N}$)

$\mathbb{N} \models \forall y\, \underbrace{\forall x < y\, (\exists z\, R(x,y,z,..))}_{\text{dipende da } y \text{ e altre var}} \equiv \exists t\, \forall x < y\, \exists z < t\, R(x,y,z,\dots)$

da x e z no perché sono legate

$\forall y\, [\varphi(y,\dots) \leftrightarrow \psi(y,\dots)]$

Dim: Fisso $y \in \mathbb{N}$, devo dim. $\varphi(y,\dots) \leftrightarrow \psi(y,\dots)$

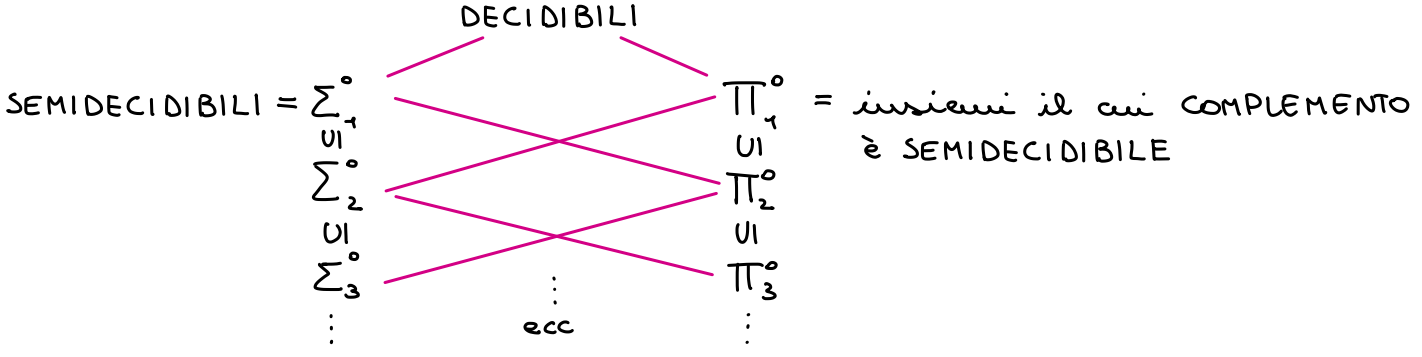
$\varphi(y,\dots)$ finita con $\forall x < y \Rightarrow$ di x ce ne sono una quantità finita (cioè esattamente y). Per ciascun x c'è un $z = z_x$: $R(x,y,z,\dots)$, basta prendere $t = \max\{z_x \mid x < y\}$

Oss: La stessa dim. non funziona in $\mathbb{R}$.

Infatti funziona in $\mathbb{N}$ perché c'è un numero finito di predecessori.

Gerarchia aritmetica:

È una gerarchia di insiemi, fatta così:



dove Σ^0_{n+1} si ottiene applicando $\exists$ davanti a Π^0_n

dove Π^0_{n+1} si ottiene applicando $\forall$ davanti a Σ^0_n

Esercizio: Tutti i Σ^0_n, Π^0_n sono stabili per $\wedge, \vee, \forall x<y, \exists x<y$

Esempio: $\{n \mid \forall x\, \exists y\, R(x,y,n)\} \in \Pi^0_n$ con R decidibile

Inoltre Σ^0_n è chiuso per $\exists$, e Π^0_n è chiuso per $\forall$

Forma normale prenessa:

Esercizio. Data una L-formula φ esiste una L-formula $\Theta \vDash \forall x [\varphi \leftrightarrow \Theta]$ dove $VL(\varphi), VL(\Theta) \subset \{\vec{x}\}$ e Θ ha tutti i quantificatori all'inizio.

Esempio: $\exists x\, \varphi(x) \to \exists x\, \psi(x)$

$\equiv \exists x\, \varphi(x) \to \exists z\, \psi(z)$

$A \to B \equiv \neg A \vee B$

$\equiv \neg \exists x\, \varphi(x) \vee \exists z\, \psi(z)$

$\neg \exists \equiv \forall \neg$

se è V o F non importa

$\equiv \boxed{\forall x\, \neg \varphi(x)} \vee \exists z\, \psi(z)$

$\equiv \exists z [\boxed{\forall x\, \neg \varphi(x)} \vee \psi(z)]$

$\equiv \exists z\, \forall x\, [\neg \varphi(x) \vee \psi(z)]$

$\equiv \exists z\, \forall x\, [\varphi x \to \psi(z)] \equiv \forall x\, \exists z\, [\varphi x \to \psi z]$

alternativamente:
$\forall x [\neg \varphi(x) \vee \exists z\, \psi(z)]$
$\equiv \forall x\, \exists z [\neg \varphi(x) \vee \psi(z)]$

Codifiche:

Coppie $\longrightarrow$ è una bigezione primitiva ricorsiva

$$\mathbb{N}^2 \to \mathbb{N} \qquad \text{coppia}(x,y) = \frac{(x+y+1)(x+y)}{2} + x$$

Def: $f: \mathbb{N}^n \to \mathbb{N}^k$ è calcolabile $\Leftrightarrow f = (f_1, \dots, f_k)$ con $f_i: \mathbb{N}^n \to \mathbb{N}$ calc.

(idem per primitiva ricorsiva)

$\pi_1[\text{coppia}(x,y)] = x \qquad \pi_1(n) = \mu x<n\, [\exists y<n\ n = \text{coppia}(x,y)]$ è P.R.

Successioni a supporto finito.

$(a_i \mid i \in \mathbb{N})$ tale che $\{i \mid a_i \neq 0\}$ è finito.

$\mathbb{N} \ni \ulcorner (a_i \mid i \in \mathbb{N}) \urcorner = \prod_i p(i)^{a_i}$ (codifica) $\qquad \ulcorner (1,2,0,3,0,0,0,\dots) \urcorner = 2^1 \cdot 3^2 \cdot 5^0 \cdot 7^3$

$(a_i \mid i \in \mathbb{N}) \longmapsto \ulcorner (a_i \mid i \in \mathbb{N}) \urcorner$ è biiezione

$\parallel$

succ. di $\mathbb{N}$ a sup. finito $\longmapsto \mathbb{N}$

Proiezioni:

$\pi : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$

$\pi(\underbrace{\ulcorner (a_n \mid n \in \mathbb{N}) \urcorner}_{s}, i) = a_i$ dove $(a_n \mid n \in \mathbb{N})$ è a supp. finito

$\pi(s,i) = \mu t < s \; \underbrace{p(i)^{t+1} \nmid s}_{\text{prim. ricorsivo}}$ ($p(i)$ = i-esimo n° primo) $\qquad a \mid b \leftrightarrow \exists c \leq b \; (ac = b)$

Insiemi finiti (di numeri naturali):

$\ulcorner \{a_1, \dots, a_n\} \urcorner = 2^{a_1} + \dots + 2^{a_n}$ con $a_1, \dots, a_n$ distinti

$\ulcorner \{3,4,7\} \urcorner = 2^3 + 2^4 + 2^7 \underset{(*)}{=} 10011000$ in binario

(*) Codice binario:

$(2^3 + 2^4 + 2^7)/2 = 2^2 + 2^3 + 2^6 + 0$ $\rightsquigarrow$ metto 0 in fondo (n° componente)

$(2^2 + 2^3 + 2^6)/2 = 2 + 2^2 + 2^5 + 0$ $\rightsquigarrow$ metto 0 a sinistra ((n-1)° componente)

$(2 + 2^2 + 2^5)/2 = 1 + 2 + 2^4 + 0$ $\rightsquigarrow$ metto 0 a sx

$(1 + 2 + 2^4)/2 = 0 + 1 + 2^3 + 1$ (3 con resto di 1) $\rightsquigarrow$ metto 1 a sx

$(1 + 2^3)/2 = 0 + 2^2 + 1$ $\rightsquigarrow$ metto 1 a sx

$2^2/2 = 2 + 0$ $\rightsquigarrow$ metto 0 a sx

$2/2 = 1 + 0$ $\rightsquigarrow$ metto 0 a sx

$1/2 = 0 + 1$ $\rightsquigarrow$ metto 1 a sx

Esercizio: $a \overset{*}{\in} b \Leftrightarrow b$ codifica un insieme contenente a

$\overset{*}{\in}$ è un predicato primitivo ricorsivo su $\mathbb{N}^2$

Dim: $a \overset{*}{\in} b \Leftrightarrow \exists c, t \leq b \; (b = c + 2^a + 2^a t \wedge c < 2^a)$

Codifica successioni finite:

insiemi succ. strett. crescenti

$(a_1, \dots, a_n) \xmapsto{\text{big}} \{a_1,\ a_1+a_2+1,\ a_1+a_2+a_3+2,\ \dots,\ \sum_{i\le n} a_i + n-1\}$

$\ulcorner\urcorner$ codifica

$\ulcorner\urcorner$ codifica

$K = 2^{a_1} + 2^{a_1+a_2+1} + \dots + 2^{\sum_{i\le n} a_i + (n-1)}$

Esempio: $(5,3,4) \mapsto \{5, 9, 14\} \xmapsto{\ulcorner\urcorner} 2^5 + 2^9 + 2^{14} = 10000\,1000\,100000$ in binario:

($9 = 5+3+1$, $14 = 5+3+4+2$)

Dim. che $\ulcorner\urcorner$ è big.

Dato K trovo l'insieme $\{b_1, b_2, \dots\}$ codificato da K

Lo scrivo in ordine crescente: posso assumere $b_1 < b_2 < \dots < b_n$

Prendo $a_1 = b_1$, $a_2 = b_2 - b_1 - 1$, $a_3 = b_3 - b_2 - 1$, ...

$\ulcorner(a_1, \dots, a_n)\urcorner = K$

Codifica dei programmi a registri:

Istruzione	Codifica	
$R_n := 0$	$4n$	$\equiv 0 \mod 4$
$R_n := R_{n+1}$	$4n+1$	$\equiv 1 \mod 4$
$R_m := R_n$	$4\,\text{Coppia}(m,n) + 2$	$\equiv 2 \mod 4$
if $R_m = R_n$ go to K	$4\,\text{Tripla}(m,n,K) + 3$	$\equiv 3 \mod 4$

STOP $\equiv$ (if $R_n = R_N$ go to istruzione inesistente)

Programma = successione $I_1, \dots, I_s$ di istruzioni.

$\ulcorner\text{Programma}\urcorner = \ulcorner(\ulcorner I_1\urcorner, \dots, \ulcorner I_s\urcorner)\urcorner$

Dato un programma P a registri di input $R_1, \dots, R_n$ e registro di output R_0.

Sia $\varphi_P^n : \mathbb{N}^n \to \mathbb{N}$ la funzione parziale calcolata da P (con input/output)

- Se $\ulcorner P\urcorner = e \in \mathbb{N}$, scrivo φ_e^n invece φ_P^n
- Se $n = 1$ scrivo φ_e invece di φ_e^1

$\{\varphi_e \mid e \in \mathbb{N}\}$ = tutte le funzioni calcolabili parziali di una variabile

$e \mapsto \varphi_e$ non è iniettiva (la stessa funzione può essere calcolata da più programmi)

La mia prima funzione non calcolabile:

$$f(n) = \begin{cases} \varphi_n(n) + 1 & \text{se } \varphi_n(n) \downarrow \\ 0 & \text{altrimenti} \end{cases}$$

Teorema: f è totale ma non calcolabile

Dim: Se lo fosse $\exists e$ $f = \varphi_e$

φ_e è totale perché coincide con f,

quindi $\varphi_e(e) \underset{\text{converge}}{\downarrow} \Rightarrow f(e) = \varphi_e(e) + 1 = f(e) + 1$ $\perp$. □

"I Reali non sono numerabili"

Teorema: $g(n) = \begin{cases} \varphi_n(n) + 1 & \text{se } \varphi_n(n) \downarrow \\ \uparrow & \text{altrimenti} \end{cases}$ $\Rightarrow$ g è calcolabile parziale non estendibile a una totale calcolabile

Idea: Per calcolare $g(n)$:

1) Prendo n
2) Lo decodifico
3) Trovo il programma P con $\ulcorner P \urcorner = n$
4) Eseguo P su input n
5) Aspetto

6a) Se si ferma aggiungo 1

6b) Se non si ferma continuo ad aspettare

Sto usando Church.

Funzione universale: (è una specie di sistema operativo)

Teorema: Esiste una funzione $U : \mathbb{N}^2 \to \mathbb{N}$ calcolabile parziale tale che

$\forall e, n \quad U(e, n) = \varphi_e(n)$ (dove $U(e,n) \uparrow$ se $\varphi_e(n) \uparrow$)

È chiaro che fissato e, la funzione $n \mapsto \varphi_e(n)$ è calcolabile (perché è calcolabile dal programma con indice = codice e)

Quello che dico è che $(e,n) \mapsto \varphi_e(n)$ è calcolabile.

Dim Teo precedente:

$g(n) = \varphi_n(n) + 1 = U(n,n) + 1$ quindi è calcolabile parziale (dove $\uparrow + 1 = \uparrow$)

Teorema (Problema della fermata):

$K_0 = \{ n \mid \varphi_n(n) \downarrow \}$ allora K_0 non è decidibile.

Dim: Se lo fosse, lo sarebbe f con $f(n) = \begin{cases} \varphi_n(n) + 1 & \text{se } n \in K_0 \\ 0 & \text{se } n \notin K_0 \end{cases}$

e abbiamo visto che f non è calcolabile.

Corollario: $K = \{ (x,y) \mid \varphi_x(y) \downarrow \}$ non è decidibile

Dim: Sia $f : \mathbb{N} \to \mathbb{N}^2$, $n \mapsto (n,n)$

$n \in K_0 \leftrightarrow f(n) \in K$

($\varphi_n(n) \downarrow$) $\leftrightarrow (n,n) \in K$

$\varphi_n(n) \downarrow$

cioè $\chi_{K_0}(n) = \chi_K(f(n))$ se K è decidibile $\to K_0$ è decidibile $\perp$

Riduzione many-one:

Def: $A \leq_m B$ $A, B \subseteq \mathbb{N}$

$\overset{\text{def}}{\longleftrightarrow}$ se $\exists f : \mathbb{N} \to \mathbb{N}$ calcolabile totale tale che:

$\forall n \quad n \in A \Leftrightarrow f(n) \in B$

Teo: B decidibile $\Rightarrow$ A decidibile

Dim: $\chi_A(n) = \chi_B(f(n))$

03-12-2021 Lezione 19 Prof. Berarducci

Riduzione di Turing:

$A, B \subset \mathbb{N}$, $A \leq_T B$ se χ_A è calcolabile con oracolo B, cioè una macchina a registri con un'operazione in più: $x := \chi_B(y)$ ← istruzione oracolo

Oss: $A \leq_m B \Rightarrow A \leq_T B$

$A \leq_T \mathbb{N} \setminus A$ però in generale $A \not\leq_m \mathbb{N} \setminus A$

Teo: $\exists A, B \subset \mathbb{N}$ $A \not\leq_T B \wedge B \not\leq_T A$

Li posso anche prendere entrambi semidecidibili (Friedberg, Muchnik)

Forma normale di Kleene:

$\varphi_e^n : \mathbb{N}^n \to \mathbb{N}$ funzione parziale calcolata dal programma a registri con codice $e \in \mathbb{N}$ (con registri di input $x_1, \dots, x_n$, output x_0)

Teorema:

1) $U^n : (e, \vec{x}) \mapsto \varphi_e^n(\vec{x})$ è calcolabile (parziale)

2) $\{(e, \vec{x}, y, t) \mid \varphi_e^n(\vec{x})\downarrow_{\le t} = y\}$ è (P.R.) decidibile
↳ bound al n° di passi di calcolo

Dim. Ovvia (Tesi di Church)

3) $\{(e, \vec{x}, t) \mid \varphi_e^n(x)\downarrow_{\le t}\}$ è decidibile (P.R.)

Corollario: Ogni funzione calcolabile si può calcolare con la ricorsione primitiva e un solo uso del μ (applicato a funzioni P.R.)

Fisso la codifica delle coppie $P_1(\langle x, y\rangle) = x$, $P_2(\langle x, y\rangle) = y$

Dim: $\varphi_e(\vec{x}) = P_2\big(\underset{(t,y)}{\mu z}\ \underbrace{\varphi_e(\vec{x})\downarrow_{P_1(z)} = P_2(z)}\big)$

tempo ↙ ↳ output — P.R. nelle var $e, \vec{x}, \vec{z}$, per (2)

Cor: Un insieme è semidecidibile $\Leftrightarrow$ è il dominio di una funzione calc. parz.

Dim: $\Leftarrow$) $W_e = \mathrm{dom}(\varphi_e) = \{x \mid \varphi_e(x)\downarrow\}$ sto usando il predicato di Kleene, funzione universale

semidecidibile (ho messo $\exists$)

$x \in W_e \Leftrightarrow \exists t\ \underbrace{\varphi_e(x)\downarrow_t}$

decidibile in e, x

$\Rightarrow$) $A \subset \mathbb{N}$ semidecidibile

$A = \{x \mid \exists y\ R(x,y)\}$ con R decidibile

$A = \mathrm{dom}(f)$ con $f(x) = \mu y R(x,y)$

Ritorno al problema della fermata:

$W_0, W_1, W_2, \dots \subset \mathbb{N}$ $\quad W_n = \mathrm{dom}\,\varphi_n^1$

tutti i sottoinsiemi semidecidibili di $\mathbb{N}$

$K_0 = \{e \mid e \in W_e\} = \{e \mid \varphi_e(e)\downarrow\} = \{e \mid \overbrace{\exists t\ \underbrace{\varphi_e(e)\downarrow_t}}\}$

semidecidibile — decidibile

↳ è semidecidibile

Se K_0 fosse decidibile, per Post, anche il complemento lo sarebbe.

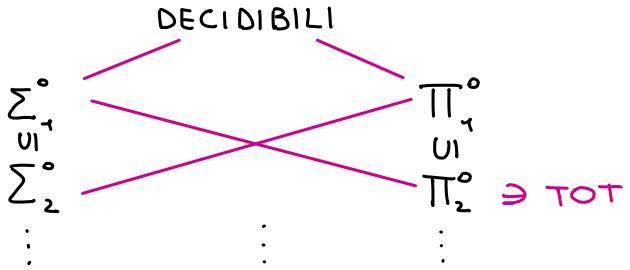
$\neg K_0 = \{e \mid e \notin W_e\}$ sarebbe decidibile, quindi semidecidibile

$\Rightarrow \exists a \quad \neg K_0 = W_a$ però $a \in W_a \iff a \in K_0$

Ora ho che $a \in W_a \iff a \in K_0$
$\Updownarrow$
$a \in \neg K_0 \Rightarrow a \notin K_0$
$\}\ \perp \quad \Rightarrow K_0$ non è decidibile

Torno alla gerarchia aritmetica:

$TOT = \{x \mid \varphi_x$ è totale$\}$ è Π_2^0 non inferiore cioè non Σ_1^0



Dim:

$TOT = \{x \mid \forall y\ \varphi_x(y)\downarrow\}$

$= \{x \mid \forall y\ \exists t\ \varphi_x(y)\downarrow_t\}$

$\varphi_x(y)\downarrow_t$ Decidibile

$\exists t$ Σ_1^0 semidecidibile perché ho messo $\exists$

$\forall y$ Π_2^0 perché ho messo $\forall$

Se $TOT \in \Sigma_1^0 \Rightarrow$ TOT semidec. $\Rightarrow$ TOT ric. enum. $\Rightarrow \exists h$ calc. tot. $TOT = \{h(n) \mid n \in \mathbb{N}\}$

$D(n) = \varphi_{h(n)}(n) + 1$ con D funzione diagonale

D è calcolabile totale → perché $h(n) \in TOT$

↓

perché la ottengo con la f. universale

Sia e tale che $D = \varphi_e$

Sia K tale che $e = h(K)$

$D(K) = \varphi_{h(K)}(K) + 1 = D(K) + 1$ ↯

Cor: Calcolabile Totale $\supsetneq$ Primitiva ricorsiva

intuitivamente: perché i codici dei programmi primitivi ricorsivi li riesco a enumerare.

Teorema s.m.n.:

Dati $m,n \in \mathbb{N}$ esiste una funzione $s: \mathbb{N}^{m+1} \longrightarrow \mathbb{N}$ calcolabile totale tale che $\forall \vec{x}, \vec{y}, e \quad \varphi_e^{m+n}(x_1, \dots, x_n, y_1, \dots, y_m) = \varphi^e_{s(e,\vec{x})}(y_1, \dots, y_m)$

(Cioè parte dell'input lo incorporo nel programma)

Esempio: Se ho un programma P_e con codice e per calcolare $+: \mathbb{N}^2 \to \mathbb{N}$ allora posso ottenere un programma P_c con codice c per calcolare $y \mapsto 3+y$.

Inoltre $c = s(e,3)$ con s primitiva ricorsiva. "È intuitivamente ovvio"

II Teorema del punto fisso:

Sia $h: \mathbb{N} \to \mathbb{N}$ calcolabile totale. Allora esiste $e \in \mathbb{N}$ tale che $\varphi_e = \varphi_{h(e)}$

Dim: Pongo $e = s(a,a)$ dove $\varphi_e(x,y) = \varphi_{s(e,x)}(y)$ s calcolabile tot. e scelgo a in modo opportuno.

Voglio $\varphi_{s(a,a)}(y) = \varphi_{h(s(a,a))}(y) \quad \forall y$

$\varphi_{s(a,a)}(y) \overset{\text{def. } s}{=} \varphi^2_a(a,y)$

Basta scegliere a in modo che $\forall x,y \quad \varphi^2_a(x,y) = \varphi_{h(s(x,x))}(y)$

Questa a esiste perché la funzione $(x,y) \mapsto \varphi_{h(s(x,x))}(y)$ è calcol. parziale perché si ottiene dalla f. universale applicata a questi due input.

È il criterio dell'autoduplicazione.

Teorema: Ack (funzione di Ackermann) è calcolabile

$A = Ack$

$A(0,y) = y+1$

$A(x+1,0) = A(x,1)$

$A(x+1,y+1) = A(x, A(x+1,y))$

Modifico la def. nel modo seguente:

$$\begin{cases} B(0,y) = y+1 \\ B(x+1,0) = C(x,1) \\ B(x+1,y+1) = C(x, C(x+1,y)) \end{cases}$$

C calcolabile $\Rightarrow$ B calcolabile

Inoltre so calcolare un programma per B se ho un programma per C.

$C = \varphi_e \Rightarrow B = \varphi_{h(e)}$ con h calcolabile totale

Per punto fisso $\Rightarrow \exists e \ \varphi_e = \varphi_{h(e)} \Rightarrow$

$\Rightarrow B = C \Rightarrow B = Ack = \varphi_e$

$C \to B$
$\varphi_e \to \varphi_{h(e)}$
$\exists e \ \varphi_e = \varphi_{h(e)}$

Dettagli per costruire la h.

$B(0,y) = y+1 \qquad = y+1$

$B(x+1,0) = C(x,1) \qquad = \varphi_e(x+1)$

$B(x+1,y+1) = C(x, C(x+1,y)) = \varphi_e(x, \varphi_e(x+1,y))$

$B(x,y) =$ if $x=0$ then $y+1$

if $x \neq 0, y=0$ then $\varphi_e(x+1)$

if $x \neq 0, y \neq 0$ then $\varphi_e(x, \varphi_e(x+1,y))$

$= f(e,x,y)$ con f calcolabile $\Rightarrow \exists a$ tc $f = \varphi_a$ con $B = \varphi_{h(e)}$

$f(e,x,y) = \varphi_a(e,x,y) \overset{\text{Teo s.m.n.}}{=} \varphi_{s(a,e)}(x,y) = \varphi_{h(e)}(x,y)$

Programma che stampa se stesso:

Esiste e tale che $\forall x \ \varphi_e(x) = e$

Dim:

Dato $c \in \mathbb{N}$ sia $h(c)$ il programma che stampa c cioè $\varphi_{h(c)}(x) = c \ \forall x$

h è calcolabile totale.

Per punto fisso $\Rightarrow \exists e$ tc $\varphi_{h(e)} = \varphi_e \Rightarrow \varphi_e(x) = \varphi_{h(e)}(x) = e$ □

È come se riuscissi a scrivere istruzioni del tipo "stampa te stesso" (o fai qlcs su te stesso)

Esempi:

$$f(x) = \begin{cases} 1 & \text{se } f x = 0 \\ 0 & \text{se } f x \neq 0 \end{cases}$$

Ma f non sta menzionando il suo programma, sta menzionando f.

$$f(x) = \begin{cases} 1 & \text{se il programma di } f \text{ è dispari} \\ 0 & \text{altrimenti} \end{cases}$$

Questo si può fare.

Esercizio: Ogni insieme semidecidibile infinito $A \subseteq \mathbb{N}$ contiene un sottoinsieme infinito decidibile $B \subset A$.

Dim: Sia f calcolabile totale, $A = \{f(n) \mid n \in \mathbb{N}\}$

Definisco $g(0) = f(0)$

$$g(n+1) = g(T(n)) \quad \text{dove } T(n) = \mu k \text{ tc } f(k) > g(n)$$

$$= f(\mu k\, f(k) > g(n))$$

↑ per costruzione

$\Rightarrow g(n+1) > g(n)$ ed è calcolabile

$B = \mathrm{Im}(g) \subset A$ ← { g è calcolabile; $\exists$ min perché A è ∞

Ho dunque un insieme enumerato da funzione calcolabile crescente

$\Rightarrow$ è decidibile.

Collegamenti tra PA e calcolabilità:

Def: $f : \mathbb{N}^k \to \mathbb{N}$ totale è binumerabile in PA se esiste una formula $\varphi(x_1, \dots, x_k, y)$ in $L = \{0, S, +, \cdot\}$ tale che

$f(a_1, \dots, a_k) = b \Rightarrow PA \vdash \varphi(\underline{a}_1, \dots, \underline{a}_k, \underline{b})$ dove $\underline{n} = S^n(0)$

$f(a_1, \dots, a_k) \neq b \Rightarrow PA \vdash \neg\varphi(\underline{a}_1, \dots, \underline{a}_k, \underline{b})$

Al posto di PA posso mettere qualsiasi teoria che ha 0, S nel suo ling.

Teorema: f è binumerabile in PA $\Leftrightarrow$ è calcolabile totale

Inoltre se f è calcolabile totale esiste $\varphi(\bar{x}, y)$ che la binumera in PA e inoltre $PA \vdash \exists! y\, \varphi(\bar{x}, y)$, $M \models PA$ $M = \mathbb{N}^f$

06-12-2024 lezione 20 Prof. Berarducci

Def: T L-Teoria $L \geq \{0, S, \dots\}$ coerente

$f : \mathbb{N}^k \to \mathbb{N}$ totale f è binumerabile in T se esiste una L-formula

$\varphi(\bar{x}, y)$ $\bar{x} = x_1, \dots, x_k$ tale che $\forall a_1, \dots, a_k \in \mathbb{N}$

1) $f(a_1, \dots, a_k) = b \Rightarrow T \vdash \varphi(\underline{a_1}, \dots, \underline{a_k}, \underline{b})$

2) $f(a_1, \dots, a_k) \neq b \Rightarrow T \vdash \neg\varphi(\underline{a_1}, \dots, \underline{a_k}, \underline{b})$

dove $\underline{a} = \underbrace{sss\dots(0)}_{a\text{-volte}}$

Def: f è biunmerabile funzionalmente se vale 1, 2 e 3:

3) se $f(a_1, \dots, a_k) = b \Rightarrow T \vdash \forall y [\varphi(\underline{a_1}, \dots, \underline{a_k}, y) \leftrightarrow y = \underline{b}]$

Oss: (3) → (1) ∧ (2) se $T \nvdash \underline{b'} \neq \underline{b}$ per $b \neq b'$

Def: f è rappresentabile in T se vale 1, 2, 3 e 4

4) $T \vdash \forall x_1, \dots, x_n \; \exists! y \; \varphi(x_1, \dots, x_n, y)$ dove

$\exists! y \; \theta(y) \equiv \exists y [\theta(y) \wedge \forall z (\theta(z) \leftrightarrow z = y)]$

Def: f è numerabile in T (T coerente) se vale:

0) $f(\bar{a}) = b \leftrightarrow T \vdash \varphi(\underline{a_1}, \dots, \underline{a_n}, \underline{b})$

Oss: (1) + (2) → (0)

Oss: 1) e 2) mi dicono che nel modello che prendo f mi definisce il grafico di f ma solo sui numeri standard e non mi dice nulla sui numeri non standard

3) Mi dice che se l'input è standard ⇒ l'output è standard ed è necessariamente quello giusto

4) Mi definisce una funzione sia sugli standard che sui non standard ma $f|_{standard} = f$

Teorema (1): le funzioni calcolabili totali sono biunmerabili funzionalmente in Q (PA-schema di induzione) e viceversa.

Q di Robinson

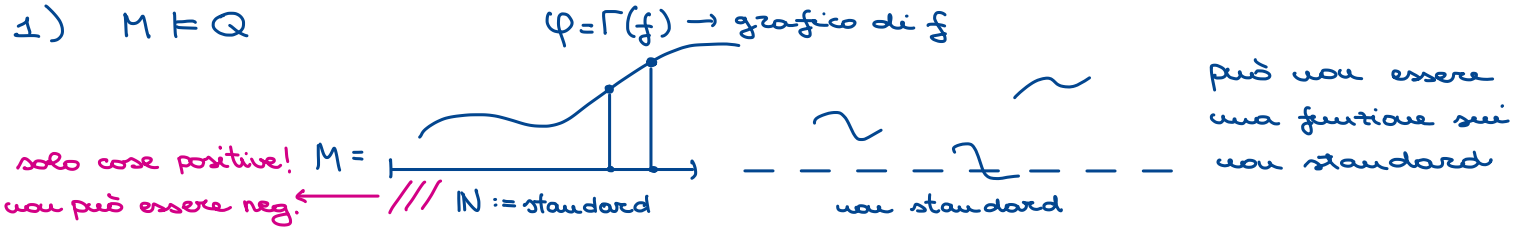
(si comporta bene solo se l'input è standard)

Teorema (2): le funzioni calcolabili totali sono rappresentabili in PA.

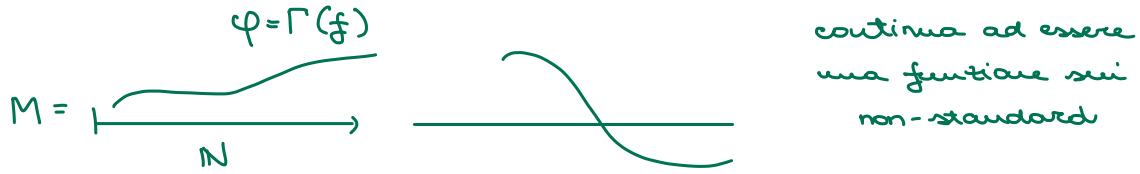
(Mi da una funzione anche se l'input è non standard)

Idea in schemi:

1) $M \vDash Q$



2) $M \vDash PA$



Servono alcuni lemmi per dimostrare il Teorema.

Lemma: $L=\{0,S,+,\cdot\}$ $\forall a,b,c \in \mathbb{N}$ $a+b=c$ $Q \vdash \underline{a}+\underline{b}=\underline{c}$ $\underline{a}=S^a(0)$ (numerale di $a \in \mathbb{N}$)

Esempio: $Q \vdash \underline{2}+\underline{3}=\underline{5}$ cioè $Q \vdash SSO+SSSO=SSSSSO$

Dim (Lemma):

Per induzione su $b \in \mathbb{N}$ nella metateoria.

NB: In Q non vale l'induzione, ma nella metateoria $\mathbb{N}$ è il solito $\mathbb{N}$, dunque vale l'induzione ed è legittimo usarla.

Se $b=0$ uso l'assioma $x+0=x$

Se $b=c+1$ uso l'assioma $x+Sy=S(x+y)$

esempio in Q: $SSO+SSSO = S(SSO+SSO) = SS(SSO+SO) = SSS(SSO)=5$ (* uso gli assiomi)

formalmente, $a+b=c \Rightarrow a+(b-1)=(c-1) \xRightarrow{\text{ind.}} Q \vdash \underline{a}+\underline{b-1}=\underline{c-1} \Rightarrow$

$\Rightarrow Q \vdash \underline{a}+S(\underline{b-1}) = S(\underline{a}+\underline{b-1}) = S(\underline{c-1}) = \underline{c}$

($\underline{a}+S(\underline{b-1})$ = $\underline{a}+\underline{b}$)

Lemma. $a+b \neq c \Rightarrow Q \vdash \underline{a}+\underline{b} \neq \underline{c}$

Uso l'assioma $0 \neq Sx$

Es: $2+1 \neq 4 \Rightarrow Q \vdash \underline{2}+\underline{1} \neq 4$ in Q $\underline{2}+\underline{1}=\underline{3} \neq \underline{4}$

Dim ($\underline{3} \neq \underline{4}$): Se per assurdo avessi $\underline{3}=\underline{4}$ allora avrei che $\not{S}SSO = \not{S}SSSO$, $\not{S}SO = \not{S}SSO$, $\not{S}O = \not{S}SO$, $O = SO$, ↳ $\bot$

Dim (Lemma): Vedi Dispense

↳ Si fa analogamente a prima

Analogamente per il $\cdot$ si dimostra:

Lemma:

- $\mathbb{N} \models a \cdot b = c \Rightarrow Q \vdash \underline{a} \cdot \underline{b} = \underline{c}$
- $\mathbb{N} \models a \cdot b \neq c \Rightarrow Q \vdash \underline{a} \cdot \underline{b} \neq \underline{c}$

Si dimostra per induzione su $b \in \mathbb{N}$ nella metateoria.

Uso gli assiomi $\begin{cases} x \cdot 0 = 0 \\ x \cdot Sy = x \cdot y + x \end{cases}$

Dim: Esercizio / Dispense

Corollario: $+, \cdot$ sono binumerabili in Q

Corollario: Per ogni termine chiuso t esiste un unico $n \in \mathbb{N}$, $Q \vdash t = \underline{n}$.

Inoltre n è l'unico tale che $\mathbb{N} \models t = \underline{n}$.

Es: $Q \vdash \underbrace{(SS0 + SS0)}_{t} \cdot (S0 + S0) = \underbrace{SSSS(0)}_{\text{numerale}}$

Lemma: $\mathbb{N} \models a = b \Rightarrow Q \vdash \underline{a} = \underline{b}$ serve solo ax-logico $x = x$

$\mathbb{N} \models a \neq b \Rightarrow Q \vdash \underline{a} \neq \underline{b}$ es: $Q \vdash \underline{2} \neq \underline{3}$ (come prima)

Esercizio: $Q \not\vdash \forall x y \quad \begin{cases} x + y = y + x \\ x \cdot y = y \cdot x \end{cases}$ Chiaramente lo dimostra per x, y standard però non per i non standard

Avevamo visto un modello non standard di Q (polinomi) ma ce ne è uno più semplice: $M \models Q$ $M = \mathbb{N} \cup \{\infty_1, \infty_2\}$ definiti $+, \cdot$ $S\infty_1 = \infty_2$, $S\infty_2 = \infty_1$

Somma e prodotto si comporteranno normalmente sui num. standard ma se ∞_1 e ∞_2 faranno pasticci, cioè non saranno commutativi.

In PA va tutto meglio.

Numeri standard: $M \models Q$ $a \in M$ a è standard se $\exists n \in \mathbb{N}$ tale che $a = (\underline{n})^K$. I numeri standard di $M \models Q$ sono $\cong (\mathbb{N}$ con solita $+, \cdot)$

Def: $x \leq y :\leftrightarrow \exists z (z + x = y)$

Esercizio:
- Se $M \models PA$ $\leq$ è un ordine totale su M
- Se $M \models Q$ non è detto che $\leq$ sia un ordine totale

Es: $\mathbb{N} \cup \{\omega_1, \omega_2\}$ $\omega_1 < \omega_2$ e $\omega_2 < \omega_1$ ma $\omega_1 \neq \omega_2$

manca la simmetria!

Oss: Se $+$ è associativo $\leq$ è transitivo:

$x \leq y \wedge y \leq t$

$z_1 + x = y \quad z_2 + y = z \rightarrow z_2 + (z_1 + x) = z$

$x \leq z$? $\qquad (z_2 + z_1) + x = z$

In PA è ok, in Q no.

Lemma: $\forall n \in \mathbb{N} \quad Q \vdash \forall x \, (x \leq n \leftrightarrow \overbrace{x = \underline{0} \vee .. \vee x = \underline{n}}^{\theta_n})$

In un modello di Q un numero minore di un numero standard è standard

Dim: Per ind su n nella metateoria.

Devo definire θ_n nella metateoria.

$\Rightarrow$) P.B. $n=0$: Sia $M \models Q$. Sia $x \in M$. Se $x \leq 0$ (in M) $\Rightarrow \exists z \; z + x = 0$.

Voglio mostrare $x = 0$. Se per assurdo $x \neq 0 \Rightarrow \exists y \quad x = s(y)$.

Per questi t, y ho $t + s(y) = 0$

$\|$

$s(t + y)$ Assurdo.

P.I. $n > 0$: Ragiono in Q. Suppongo $x \leq n$

Sia z tale che $z + x = \underline{n}$.

Se $x = \underline{0}$ ho finito ($\Rightarrow x = \underline{0} \vee .. \vee x = \underline{n}$)

Se $x \neq \underline{0}$ scrivo $x = s(y)$ ho $z + s(y) = \underline{n}$

Ma allora $s(z + y) = \underline{n} \Rightarrow z + y = \underline{n-1} \Rightarrow y \leq \underline{n-1} \Rightarrow y = \underline{0} \vee \ldots \vee y = \underline{n-1} \Rightarrow$

$\Rightarrow \; sy = \underline{1} \vee \ldots \vee sy = n \Rightarrow x = \underline{1} \vee \ldots \vee x = \underline{n}$

$\Leftarrow$) facile.

Corollario: $\forall n \in \mathbb{N} \quad Q \vdash \forall x \, (x \leq \underline{n+1} \leftrightarrow x \leq \underline{n} \vee x = \underline{n+1})$

$x \leq \underline{n+1} \leftrightarrow x = \underline{0} \vee \ldots \vee x = \underline{n} \cup x = \underline{n+1}$

$\leftrightarrow x \leq \underline{n} \quad \vee \quad x = \underline{n+1}$

Corollario: Sia $n \in \mathbb{N}$, sono equivalenti:

1) $\forall a \leq n \quad Q \vdash \varphi(\underline{a})$

2) $Q \vdash \underbrace{\forall x \leq \underline{n} \ \varphi(x)}_{\forall x\,(x \leq \underline{n} \to \varphi(x))}$

In generale $\forall a \ Q \vdash \varphi(\underline{a})$ $\not\Leftrightarrow$ $Q \vdash \forall x \, \varphi(x)$

Cioè i quantificatori limitati passano dalla metateoria alla teoria.

Dim: 1) $\Leftrightarrow Q \vdash \varphi(\underline{0})$ e ... e $Q \vdash \varphi(\underline{n})$

$\Leftrightarrow Q \vdash [\varphi(\underline{0}) \wedge \dots \wedge \varphi(\underline{n})]$

$\Leftrightarrow Q \vdash \forall x\,[x = \underline{0} \vee \dots \vee x = \underline{n} \to \varphi(x)]$

$\hookleftarrow Q \vdash \forall x\,[x \leq \underline{n} \to \varphi(x)]$

$\Leftrightarrow$ 2)

Lemma: Sia $a \in \mathbb{N}$, sono equivalenti:

1) $\exists x \leq n \quad Q \vdash \varphi(x)$

2) $Q \vdash \underbrace{\exists x \leq \underline{n} \ \varphi(x)}_{\exists x\,(x \leq \underline{n} \wedge \varphi(x))}$

Dim: entrambe equivalgono a $Q \vdash \varphi(\underline{0}) \vee \dots \vee \varphi(\underline{n})$

Lemma (15.37). $M \models Q$, $\emptyset \neq A \subset M$ contenente un numero standard

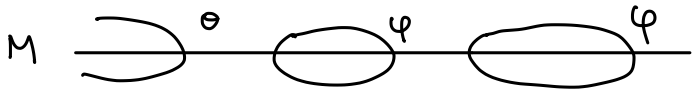
$\Rightarrow$ A ha un "minimo" elemento

Dim: Il minimo di A lo trovo in $A \cap$ (standard di M)

Esercizio: Se $M \models PA$ $\emptyset \neq A \subset M$ definibile $\Rightarrow$ A ha un minimo

$A = \{x \mid M \models \varphi(x, b)\}$.

Se A non ha minimo, sia $\Theta(x,b) \equiv \forall y\,(\varphi(y,b) \to x < y)$



Se A non ha minimo Θ contiene 0 ed è chiuso per successione

$\Rightarrow \forall y \ \Theta(y,b) \Rightarrow A = \emptyset$

- $\forall b\,[\Theta(0,b) \wedge \forall x \ \Theta(x,b) \to \Theta(Sx, b) \to \forall x \ \Theta(x,b)]$

  ↳ Schema di induzione

Formule Δ_0 limitate:

Sono quelle che hanno solo quantificatori limitati.

Una L-formula $L=\{0, S, +, \cdot\}$ è Δ_0 se tutti i suoi $\forall, \exists$ sono limitati cioè occorrono solo in contesti del tipo $\forall x \leq t\, \theta$, $\exists x \leq t\, \theta$ dove t è un termine non contenente la x.

Def. T coerente, una formula chiusa φ è **determinata** in T se $T \vdash \varphi$ o $T \vdash \neg\varphi$, altrimenti dico che φ è **indipendente**.

Oss: T è completa se tutte le formule sono determinate.

Teorema: le Δ_0-chiuse sono determinate in Q.

Dim: 1) le atomiche sono determinate in $Q \vdash t_1 = t_2$ o $Q \vdash t_1 \neq t_2$

Siano $n_1, n_2 \in \mathbb{N}$ $\quad Q \vdash t_1 = \underline{n}_1$ e $Q \vdash t_2 = \underline{n}_2$

- se $n_1 = n_2 \Rightarrow Q \vdash \underline{n}_1 = \underline{n}_2 \Rightarrow Q \vdash t_1 = t_2$
- se $n_1 \neq n_2 \Rightarrow Q \vdash \underline{n}_1 \neq \underline{n}_2 \Rightarrow Q \vdash t_1 \neq t_2$

2) Congiuntione, disgiunzione, negazione di determinata è determinata

es: φ, ψ determinata: ho 4 possibilità

$$\begin{cases} Q \vdash \varphi \text{ e } Q \vdash \psi \\ Q \vdash \varphi \text{ e } Q \vdash \neg\psi \\ Q \vdash \neg\varphi \text{ e } Q \vdash \psi \\ Q \vdash \neg\varphi \text{ e } Q \vdash \neg\psi \end{cases} \Rightarrow \begin{cases} Q \vdash \varphi \vee \psi \\ Q \vdash \varphi \vee \psi \\ Q \vdash \varphi \vee \psi \\ Q \vdash \neg(\varphi \vee \psi) \end{cases}$$

Considero • $\underbrace{\forall x \leq t\, \varphi(x)}_{\text{chiusa}} \in \Delta_0 \quad \Rightarrow t$ chiuso

sia $n \in \mathbb{N}$ tale che $Q \vdash t = \underline{n}$

$$Q \vdash [\forall x \leq t\, \varphi(x)] \longleftrightarrow \underbrace{\varphi(0) \wedge \varphi(1) \wedge \ldots \wedge \varphi(n)}_{\text{congiunzione di det. è det.}}$$

- idem per $\exists x \leq t\, \varphi(x)$ perché equivale a $\varphi(\underline{0}) \vee \ldots \vee \varphi(\underline{n})$

esempio: $\forall x \leq \overset{\text{chiuso}}{\uparrow} \underline{2}\ \exists y \leq \overset{\text{aperto}}{\uparrow} x\, \varphi(x,y) \Leftrightarrow \bigwedge_{n \leq 2} \exists y \leq \underline{n}\, \varphi(x,y)$

$$\Leftrightarrow \bigwedge_{n\le 2} \bigvee_{k\le 2} \varphi(n,k)$$

Def: formule Σ^0_1 sono la più piccola classe di formule contenente le Δ_0 e chiusa per $\wedge, \vee, \exists, \forall x \le t$

$(\Sigma^0_1)^{\mathbb{N}}$ ≡ sono i sottoinsiemi di $\mathbb{N}^k$ definibili con una formula Σ^0_1 interpretata in $\mathbb{N}$

Analogamente $(\Delta_0)^{\mathbb{N}}$ ... Δ_0

Teorema: $(\Delta_0)^{\mathbb{N}} \subset$ Primitivi Ricorsivi $\subset$ Decidibili $\subset (\Sigma^0_1)^{\mathbb{N}}$

$(\Sigma^0_1)^{\mathbb{N}}$ = semidecidibili = $\exists$ decidibile = Σ^0_1

Ho due def. di Σ^0_1.

$L = \{0, s, +, \cdot\}$

Def: Le formule Π^0_1 sono la più piccola classe di formule contenente le Δ_0 e chiusa per $\wedge, \vee, \forall, \exists x \le t$

Oss: $\varphi \in \Pi^0_1 \leftrightarrow \neg\varphi$ equivale (in Q) a una Σ^0_1

Es: $\underbrace{\neg \exists x\ \Delta_0}_{\Sigma^0_1} \leftrightarrow \underbrace{\forall x\ \underbrace{\neg \Delta_0}_{\Delta_0}}_{\Pi^0_1}$

Teo: Se una formula chiusa $\varphi \in \Sigma^0_1$ è vera in $\mathbb{N} \Rightarrow$ è dim. in Q

Dim: Per ind. sul n° di connettivi di φ

- $\varphi = \alpha \wedge \beta$, $\varphi = \alpha \vee \beta$, $\varphi = \forall x \le t\, \alpha$ (facili es.)
- $\varphi = \exists x\, \theta(x)$

$\mathbb{N} \vDash \varphi \Leftrightarrow \mathbb{N} \vDash \exists x\, \theta(x) \Leftrightarrow \exists a \in \mathbb{N}\ \ \mathbb{N} \vDash \theta(a)$

$\Rightarrow \exists a \in \mathbb{N}\ \ Q \vdash \theta(a)$

↓ ind.

$\Rightarrow Q \vdash \exists x\, \theta(x)$

$\Rightarrow Q \vdash \varphi$

Congettura di Goldbach

"Ogni numero pari ≥ 4 è somma di due primi"

$8 = 5+3$, $10 = 5+5$, $12 = 7+5$, ...

Goldbach $\in \Pi^0_1$ * mi dice che x è pari

$\forall x \, (\overbrace{\exists y \leq x \, (x = y+y)}^{*} \rightarrow \exists p, q \leq x \;\; (p \text{ primo} \wedge q \text{ primo} \wedge x = p+q))$

p primo $\equiv \forall u, v \leq p \;\; (uv = p \rightarrow u = p \vee v = p)$

Se Goldbach è falsa $\Rightarrow Q \vdash \neg$ Goldbach

Se Goldbach è vera potrebbe essere indipendente

Se dim. (nella metateoria) che Goldbach è indip. da Q

$\Rightarrow$ (nella metateoria) dimostro Goldbach.

10-12-2024 lezione 21 Prof. Berarducci

Riepilogo: Già visto • $\varphi \in \Delta_0$ e $\mathbb{N} \models \varphi \Rightarrow Q \vdash \varphi$

$\mathbb{N} \models \neg\varphi \Rightarrow Q \vdash \neg\varphi$

• $\varphi \in \Sigma^0_1$ $\mathbb{N} \models \varphi \Leftrightarrow Q \vdash \varphi$

$\Leftarrow$ perché $\mathbb{N} \models Q$

Esempio: Goldbach $\in \Pi^0_1$ quindi se $\mathbb{N} \models \underbrace{\neg \text{Goldbach}}_{\Sigma^0_1} \Rightarrow Q \vdash \neg$ Goldbach

Teorema: Se f è calcolabile totale $\Rightarrow f$ è binumerabile in Q

Esempio: $x \mapsto 2^x$ è binumerabile in Q $L_Q = \{0, s, +, \cdot\}$

$x, y \mapsto x^y$

Lo faccio in PA anziché in Q

Lemma: Data $\varphi(x)$, $PA \vdash \forall n \overbrace{\exists m \, cm\{x < n \mid \varphi(x)\}}^{\theta(n)}$

$\exists M \, \forall x < n \, (\varphi(x) \rightarrow \underbrace{x \mid M}_{\exists t \; xt = M})$

$\wedge \, \forall M' [(\forall x < n \; \varphi(x) \rightarrow x \mid M') \rightarrow M \mid M']$

Dim: Lavoro in PA e lo dim. per ind. su n.

$\theta(0)$ vale a vuoto

Suppongo che valga $\theta(n)$ mostro $\theta(sn)$.

Chiamo $M = mcm\{x < n \mid \varphi(x)\}$.

$$M_{x+1} = \begin{cases} \text{mcm}\{M, Sn\} & \text{se } \varphi(n) \\ M & \text{se } \neg\varphi(n) \end{cases}$$

M_{+1} testimonia $\theta(Sn)$

Esercizio: $PA \vdash \forall a\, b\, \exists c\ [c = \text{mcm}(a,b)]$

idea → un multiplo comune esiste ed è $a \cdot b$.

Per trovare il minimo prendo $\min\{c \mid c \neq 0 \wedge a|c \wedge b|c\}$

Avendo fatto il caso base e il passo induz., per ind. $PA \vdash \forall x\, \theta(x)$

Lemma: $PA \vdash \forall n\, \forall d$ (se d è divisibile per tutti i numeri positivi $< n \Rightarrow$

$\Rightarrow \forall j < n$ $(i+1)d + 1$ e $(j+1)d + 1$ sono relativamente primi)

Es: $n = 10$ $\quad d = 10!$

$$\underbrace{1d+1 \quad 2d+1 \quad 3d+1, \ldots, 9d+1}_{\text{sono relativamente primi tra loro}}$$

Dim (Lemma): Lavoro in PA, dimostro che i numeri $(i+1)d+1$ $(i<n)$

sono primi tra loro.

Sia p primo, supp. per assurdo $p|(i+1)d+1$, $p|(j+1)d+1$ con $i<j<n$

$\Rightarrow$ p divide la loro differenza cioè $p|(j-i)d$.

(PA dimostra che se un primo divide un prodotto divide uno dei due)

$\underbrace{p|(j-1) \vee p|d}_{p|d}$, però $j-i<n$ quindi $j-i \mid d$ però $p|(i+1)d+1$, $p|d$

$\Rightarrow p|1$ $\perp$.

Def: $x \overset{*}{\in} (a,b,c)$ se $\begin{cases} x<c \\ b = \text{mcm}\{i \mid 0<i<c\} \\ (x+1)b+1 \mid a \end{cases}$

Teorema: Data $\varphi(x)$ $PA \vdash \forall n\ \exists a,b,c$ tali che $\forall x\ x \overset{*}{\in} (a,b,c) \leftrightarrow x<n \wedge \varphi(x)$

idea: (a,b,c) codifica $\{x<n \mid \varphi(x)\}$

Dim (Teo): $c = n$ $\quad b = \text{mcm}\{i \mid 0<i<c\}$ $\quad a = \text{mcm}\{(i+1)b+1 \mid (i<c) \wedge \varphi(i)\}$

$$\left\{ \begin{array}{l} 0 \longrightarrow 1b+1 \\ 1 \longrightarrow 2b+1 \\ \vdots \\ x \longrightarrow (x+1)b+1 \\ \vdots \\ n \longrightarrow (n-1)b+1 \end{array} \right\} \text{a due a due primi tra loro}$$

(*) $\rightarrow$) se $x \overset{*}{\in} (a,b,c) \overset{\text{def. di } \overset{*}{\in}}{\Longrightarrow} x<c=n$, $b=\text{mcm}\{i \mid 0<i<n\}$, $(x+1)b+1 \mid a$

$\overset{*}{\Rightarrow} \varphi(x)$

(*) Se $\neg\varphi(x)$, $(x+1)b+1$ sarebbe coprimo con tutti i numeri $(i+1)b+1$ tali che $\varphi(i)$ e quindi $(x+1)b+1$ è coprimo con il loro prodotto cioè con a. $\perp$

(Uso PA $\vdash$ se un numero è coprimo con una serie di altri numeri coprimi tra loro è coprimo con il loro mcm)

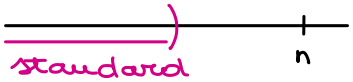
$\leftarrow$) Sia $x<n \wedge \varphi(x)$ dico che $x \overset{*}{\in} (a,b,c)$

$(x+1)b+1 \mid a$ (per def di a) quindi vale $x \overset{*}{\in} (a,b,c)$

Oss: $M \models PA$ PCM limitato superiormente da $n \in M$ (n possib. non standard)

- non è detto che $\exists \text{mcm}\{i \mid i \in P\}$
- esiste se P è definibile
- Se P invece fosse $P=\{i \mid i \in M \text{ standard}\}$, $\text{mcm}\{i \mid i \in P\}$ non esiste

Però invece esiste $\text{mcm}\{i \mid i<n\}$



l'mcm dei numeri solo standard non esiste.

L'idea è che avendo l'induzione si possano trattare i numeri non standard come se fossero standard a condizione che siano cose definibili.

Esercizio: $PA \vdash \forall a,b \ \exists c = \{a,b\} \ (\forall x \ x \overset{*}{\in} c \leftrightarrow x=a \vee x=b)$

Def: $x \overset{*}{\in} c \longleftrightarrow x \overset{*}{\in} (c_1,c_2,c_3)$ dove c codifica (c_1,c_2,c_3), $c=\langle\langle c_1,c_2\rangle,c_3\rangle$,

$\langle a,b\rangle = \frac{(a+b+1)(a+b)}{2} + a$

Teorema (versione con parametri):

Data $\varphi(x,y)$ $PA \vdash \forall y [\forall n \ \exists a,b,c \text{ tc } \forall x \ x \overset{*}{\in} (a,b,c) \leftrightarrow x<n \wedge \varphi(x,y)]$

Dim: Come prima

Ho fatto la codifica entro PA degli insiemi definibili limitati $\{x<n \mid \varphi(x)\}$ dove $\varphi(x)$ può contenere altre variabili che sono come parametri.

Codifica delle successioni "finite":

(La lunghezza può essere non standard)

Sia $F(x,y)$ formula, dico che F è funzionale se $PA \vdash \forall x \, \exists! y \, F(x,y)$

In quel caso scrivo $F(x)=y$ invece di $F(x,y)$

Data una formula funzionale $F(x,y)$ in PA

$PA \vdash \forall n \;\; \exists$ codifica $(F(i) \mid i<n)$

funzione $\longmapsto$ Modello

$\{i \mid i<n\}$

idea $\rightarrow$ identifico $(F(i) \mid i<n)$ con $\{\langle i, F(i)\rangle \mid i<n\}$

Per induzione su n esiste il $\max_{i<n} \langle i, F(i)\rangle = M$

$\{\langle i, F(i)\rangle \leq M \mid i<n\}$

Trovo (a,b,c) tale che $PA \vdash \forall n [\forall x \; x \overset{*}{\in} (a,b,c) \leftrightarrow \exists i<n \; x = \langle i, F(i)\rangle]$

Oss: (In $\mathbb{N}$) $\forall x, y \in \mathbb{N} \quad 2^x = y \iff \exists f : \{i \mid i \leq x\} \longrightarrow \mathbb{N}$

$f(0) = 1$

$f(x) = y$

$\forall i<x \quad f(i+1) = 2 f(i)$

"esiste una successione finita di lunghezza x" $\iff \exists$ successione $\{f_i \mid i \leq x\}$

$f_0 = 1 \qquad f_x = y \qquad \forall i<x \quad f_{i+1} = 2 f_i$

Dim: $\Rightarrow$) Prendo $f_i = 2^i$

$\Leftarrow$) Dato f per induzione su $i \leq x$ $f_i = 2^i$

Chiamo f testimone di $2^x = y$

Def (in PA): "$2^x = y$" $\iff \exists a,b,c$ tale che (a,b,c) testimonia $2^x = y$

"$2^x = y$" $\iff \exists a,b,c$ tale che: ($\exists a,b,c$ testimone di $2^x = y$)

$\langle x, y\rangle \overset{*}{\in} (a,b,c) \wedge \langle 0, 1\rangle \overset{*}{\in} (a,b,c) \wedge \forall i<x \; \overset{*}{\forall} q \; \langle i, q\rangle \overset{*}{\in} (a,b,c) \Rightarrow$

$\Rightarrow \langle i+1, 2q\rangle \overset{*}{\in} (a,b,c)$

$\wedge\ \forall p \overset{*}{\in} (a,b,c)\ \exists i \le x\ \overbrace{\exists z}^{*}\ p = \langle i,z\rangle \wedge \overbrace{\forall i,z,z'\ \langle i,z\rangle \overset{*}{\in} (a,b,c) \wedge \langle i,z'\rangle \overset{*}{\in} (a,b,c)}^{*} \to z = z'$

* li limito con $\langle a,b,c\rangle$

"$2^x = y$" $\leftrightarrow (\exists a,b,c)\ \Delta_0$ è una formula Σ_1^0

È chiaro che in $\mathbb{N}$ la formula $2^x = y$ def. $\{(a,b) \in \mathbb{N}^2 \mid 2^a = b\}$

Cosa succede in modelli non standard:

$PA \vdash$ "$2^0 = 1$" $\quad \forall x\ \exists! y$ "$2^x = y$"

Quindi diciamo 2^x l'unico y tale che "$2^x = y$"

$\forall x,y$ "$2^x = y$" $\to$ "$2^{x+1} = 2\cdot y$" cioè $PA \vdash \forall x\ [2^{x+1} = 2 \cdot 2^x]$

Dim: Sia $c = (c_1, c_2, c_3)$ un testimone di "$2^x = 2y$"

(idea: c codifica $\{\langle i, 2^i\rangle \mid i \le x\}$)

Allora per trovare un testimone di "$2^{x+1} = y$" prendo $c' =$ "$c \cup \{\langle x, y\rangle\}$"

Esercitio: $PA \vdash \forall a\ \forall b\ \exists$ "$a \cup b$"

$$\forall a\ \forall b\ \exists c\ \forall x\ [x \overset{*}{\in} c \leftrightarrow x \overset{*}{\in} a \vee x \overset{*}{\in} b]$$

Dim (Esercitio): c codifica $\{\underset{\max(a,b)}{\underset{\wedge}{x}} \mid \underbrace{x \overset{*}{\in} a \vee x \overset{*}{\in} b}_{\varphi(x)}\}$

Esercitio: $PA \vdash \forall a\ \exists b\ \forall x\ (x \overset{*}{\in} b \leftrightarrow x = a)$

idea: $b = \{a\}$ $\quad b$ codifica $\{x \le a \mid x = a\}$

Così come ho fatto "$2^x = y$" potrei fare $x! = y$ o qualunque funt. P.R.

$x! = y \leftrightarrow \exists (f_i \mid i \le x)\ f_0 = 1 \wedge f_x = y \wedge \forall i < x\ f_{i+1} = f_i (i+1)$

$\leftrightarrow$ esiste la codifica di tale successione

$\leftrightarrow \exists c = (c_1, c_2, c_3)$ tale che c codifica una successione $(f_i \mid i \le x)$

tale che $f_0 = 1 \wedge f_x = y \wedge \forall i < x\ f_{i+1} = f_i (i+1)$

dove $f_i =$ l'unico z tc $\langle i, z\rangle \overset{*}{\in} c$

Codifica insiemi definibili limitati:

$$\langle x,y\rangle = z \leftrightarrow \frac{(x+y+1)(x+y)}{2} + x = z$$

$$\leftrightarrow (x+y+1)(x+y) + 2x = 2z$$

- $\langle\ ,\ \rangle : \mathbb{N}^2 \longrightarrow \mathbb{N}$ è biunivoca, primitiva ricorsiva con proiezioni P.R.
- $\langle x,y,z\rangle = \langle\langle x,y\rangle,z\rangle$
- $x \overset{*}{\in} \langle a,b,c\rangle \iff x<c \wedge b$ è mcm dei numeri positivi $<c \wedge (x+1)b+1 \mid a$

Prop: Data $\varphi(x)$ $PA \vdash \forall n\ \exists a\ \ x \overset{*}{\in} a \leftrightarrow (x<n \wedge \varphi(x))$

idea: a codifica $\{x<n \mid \varphi(x)\}$

Def (PA):
- $a \cup b$ = minimo c tale che $\underbrace{\forall t}_{\le c}\ (t \overset{*}{\in} c \leftrightarrow t \overset{*}{\in} a \vee t \overset{*}{\in} b)$
- $\{x\}$ = minimo c tale che $\forall t\ (t \overset{*}{\in} c \leftrightarrow t = x)$
- $a \setminus \{x\}$ = minimo c tale che $\forall t\ (t \overset{*}{\in} c \leftrightarrow t \in a \wedge t \neq x)$

Def (PA):
- s codifica una funzione se $\forall i,a,b \le s$:

  $\langle i,a\rangle \overset{*}{\in} s \wedge \langle i,b\rangle \overset{*}{\in} s \to a=b$
- $i \in dom(s) \leftrightarrow \exists a\ \langle i,a\rangle \overset{*}{\in} s$
- s codifica una successione $\leftrightarrow$ s codifica una funzione $\wedge$

  lunghezza di s $\wedge\ \exists n\ \forall i \in dom(s) \leftrightarrow i<n$

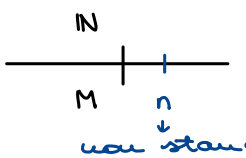
Queste sono tutte abbreviazioni per formule aritmetiche equivalenti a formule Δ_0 (perché $x \in c \to x \le c$, tutti i quantificatori li posso limitare)

Esplicito meglio:

$$\underbrace{a \cup b = c}_{\Delta_0} \leftrightarrow \forall t\ (t \overset{*}{\in} c \leftrightarrow t \overset{*}{\in} a \vee t \overset{*}{\in} b) \wedge \forall c'<c\ \neg\forall t\ (t \overset{*}{\in} c' \leftrightarrow t \overset{*}{\in} a \vee t \overset{*}{\in} b)$$

Def (PA): $[s]_i := a :\leftrightarrow$ s codifica una successione $\wedge\ i \in dom(s) \wedge \langle i,a\rangle \overset{*}{\in} s$

L'i-esimo elemento della successione codificata da s è a.



Il modello potrà codificare solo le successioni di lunghezza standard.

Teorema: $\forall n \in \mathbb{N} \quad \forall a_1, \dots, a_n \in \mathbb{N} \quad \exists s \in \mathbb{N}$ tc $\mathbb{N} \models s$ codifica $\langle a_0, \dots, a_n \rangle$

cioè $[s]_0 = a_0, \dots, [s]_n = a_n$

Teorema: $PA \vdash \forall S \quad \forall a \quad \forall n$ (s codifica una successione di lunghezza n con

$n = lh(s) \rightarrow \exists s'$ tc s' codifica una successione di lunghezza $n+1$

$\forall i < n \; [s]_i = [s']_i \; , \; [s']_n = a$) $\quad s' = s^\frown \langle a \rangle$

"Dim" (idea): $s' = s \cup \{ \langle n, a \rangle \}$ dove $\cup, \{ \}$ sono definiti in termini di $\overset{*}{\in}$

Teorema: $PA \vdash \exists S \; (S = \langle \rangle)$ (cioè $\forall x \; (x \overset{*}{\notin} S)$)

Dim: $s = \langle a, b, 0 \rangle$ con a, b qualsiasi

Corollario: $\forall n \; \forall a_1, \dots, a_n \quad PA \vdash \exists s \; \forall i < \underline{n} \; ([s]_i = a_i)$

Teorema: $PA \vdash$ posso modificare una successione cambiandogli un elem. come voglio $\forall s \; \forall i < lh(s) \; \forall a \; \exists s' \; \forall j \neq i$

$[s']_i = a \quad [s']_j = [s]_j$

idea: $s' = s[a \mapsto i]$

Dim: $s' = (s \setminus \{ \langle i, [s]_i \rangle \}) \cup \{ \langle i, a \rangle \}$

Teorema: $PA \vdash \forall S \; \forall S'$ se s e s' codificano successioni

$\exists s'', \quad s'' = s^\frown s'$ (concatenazione)

cioè $\forall i < lh(s) \quad [s'']_i = [s]_i$

$\forall j < lh(s') \quad [s'']_{lh(s)+j} = [s']_j$

Def (PA): $a^x = y \leftrightarrow$ "$\exists s$ (illimitato) s codifica una successione di lunghezza $x+i$" (Σ_1^0)

$\forall i < x \quad [s]_{i+1} = a[s]_i$ (Δ_0)

$[s]_0 = 1$

$[s]_x = y$

idea: $[s]_i = a^i$

Abbreviazione: $[s]_{i+1} = 2[s]_i \iff \exists u \; v \; ([s]_{i+1} = u \wedge [s]_i = v \wedge u = 2v)$

$f(g(x)) = t \iff \exists u \; g(x) = u \wedge f(u) = t$

es: $\Theta(2^x) = \exists u\,(2^x = u \wedge \Theta(u))$

Prop: $PA \vdash 2^0 = 1 \wedge \forall x\, \exists! y\ 2^x = y \wedge \forall x\, 2^{x+1} = 2^x \cdot 2$

cioè $\forall u, v\ (2^x = u \wedge 2^{x+1} = v \to v = 2u)$

Dim (Esistenza di y): Sia s la successione che testimonia $2^x = y \Rightarrow$

$\Rightarrow s' = s \cup \{\langle x+1, 2y\rangle\}$ testimonia $2^{x+1} = 2^x \cdot 2$

(Unicità di y): Per induzione su x (fare i dettagli x es.)

Quindi posso comportarmi come se PA avesse un simbolo di funzione per 2^x. Scrivo $\Theta(2^x) := \exists y\,(y = 2^x \wedge \Theta(y))$.

Tutte le funzioni P.R. f sono rappresentabili in PA.

Teorema: Se f è P.R. $f: \mathbb{N}^k \to \mathbb{N} \Rightarrow \exists$ formula $\varphi_f(\bar{x}, y)$

$\forall a_1, \dots, a_k, b$ (biunivocalità ✓)

1) $f(a_1, \dots, a_k) = b \quad PA \vdash \varphi_f(\underline{a_1}, \dots, \underline{a_k}, \underline{b})$

2) $f(a_1, \dots, a_k) \neq b \quad PA \vdash \neg\varphi_f(\underline{a_1}, \dots, \underline{a_n}, \underline{b})$

Questo lo so fare anche Q ↑

funzionale

3) $Q \vdash \forall y\,[\varphi_f(\underline{a_1}, \dots, \underline{a_k}, y) \leftrightarrow y = \underline{b}]$ (anche PA)

4) $PA \vdash \forall x_1, \dots, x_n\ \exists! y\ \varphi_f(x_1, \dots, x_n, y)$ (Q no)

In pratica Q dimostra che φ_f definisce una funzione sui numeri standard che coincide con f.

PA dimostra che φ_f definisce una funzione che estende f ai numeri non standard.

$Q \vdash 1), 2), 3)$ ma non vec. ie 4)

Se diamo 4) per buono $\Rightarrow$ 4) → 1), 2)

$f(a) = b \Rightarrow PA \vdash \varphi_f(\underline{a}, \underline{b}) \to \mathbb{N} \models \varphi_f(\underline{a}, \underline{b}) \Rightarrow Q \vdash \varphi_f(\underline{a}, \underline{b})$

$f(a) \neq b \Rightarrow \exists c \neq b \quad f(a) = c \Rightarrow PA \vdash \varphi(\underline{a}, \underline{c}) \wedge \underline{c} \neq \underline{b}$

$\Rightarrow Q \vdash \neg\varphi(\underline{a}, \underline{b})$

Il punto 3) va dim. a parte per Q

Dim: Supp che $f(x+1, \bar{y}) = h(x, y, f(x,y))$

$f(0, \bar{y}) = g(\bar{y})$

f è definita per ricorsione primitiva da h, g

Per induzione posso assumere che h, g siano rappresentabili da formule φ_h, φ_g come sopra.

"$f(x,y)=z$" $:\leftrightarrow \exists s$ codifica una successione (idea: $[s]_i = f(i, \bar{y})$)

"$[s]_0 = g(\bar{y})$" cioè $\varphi_g(\bar{y}, [s]_0)$

$\forall i < x$ ("$[s]_{i+1} = h(i, y, [s]_i)$") $\quad [s]_x = z$

dove al posto di "$f(x,y)=t$" $\leftrightarrow \varphi_f(x,y,t)$

"$u = h(i,y,t)$" $\leftrightarrow \varphi_h(i,y,t,u)$ etc ...

Chiusura per composizione:

$f(\bar{x}) = h(g_1(\bar{x}), \dots, g_k(\bar{x}))$

"$f(\bar{x})=y$" $\leftrightarrow \exists u_1, \dots, u_k$ ("$g_1(\bar{x}) = u_1$" $\wedge \dots \wedge$ "$g_k(\bar{x}) = u_k$" $\wedge$ "$h(u_1, \dots, u_k) = y$")

Per farlo funzionare in Q è importante la proprietà funzionale

Es: $h(3) = 4 \quad g(4) = 8 \Rightarrow (g \circ h)(3) = 8$

$Q \vdash (g \circ h)(3) = 8 \leftrightarrow \exists u [h(3) = u \wedge g(u) = 8]$

$f(x) = \mu y \; h(x,y) = 0$

Se h è rappresentabile in PA posso rappresentare f

"$f(x)=y$" $\leftrightarrow$ "$h(x,y)=0$" $\wedge \forall u < y \; \exists t$ ("$h(x,y) = t+1$")

lo scrivo così invece che $h(x,y) \neq 0$ se no non è Σ_1^0

Teorema: Tutte le funzioni ricorsive totali sono rappresentabili in PA da formule Σ_1^0

Codifiche di termini e formule di PA:

$L = \{0, s, +, \cdot\}$ $\quad \# : L \to \mathbb{N}$ iniettiva

Oss: in realtà $\# : L \cup \{v, \wedge, \vee, \neg, \to, \forall, \exists\} \to \mathbb{N}$ iniettiva (v variabile)

- codifica dei termini : $\ulcorner\ \urcorner$: L-termini $\longrightarrow \mathbb{N}$ iniettiva

$\ulcorner v_i \urcorner = \langle \#(v), i \rangle$

$\ulcorner t_1 + t_2 \urcorner = \langle \#(+), \ulcorner t_1 \urcorner, \ulcorner t_2 \urcorner \rangle$

$\ulcorner t_1 \cdot t_2 \urcorner = \langle \#(\cdot), \ulcorner t_1 \urcorner, \ulcorner t_2 \urcorner \rangle$

$\ulcorner s(t) \urcorner = \langle \#(s), \ulcorner t \urcorner \rangle$.

Oss: # codifica l'alfabeto e $\ulcorner\ \urcorner$ (:= numeri di Gödel) le parole.

- codifica formule:

$\ulcorner t_1 = t_2 \urcorner = \langle \#(=), \ulcorner t_1 \urcorner, \ulcorner t_2 \urcorner \rangle$

$\ulcorner \alpha \vee \beta \urcorner = \langle \#(\wedge), \ulcorner \alpha \urcorner, \ulcorner \beta \urcorner \rangle$

$\ulcorner \forall v_i \varphi \urcorner = \langle \#(\forall), \ulcorner v_i \urcorner, \ulcorner \varphi \urcorner \rangle$ etc

Codifico $\langle x, y \rangle = 2^{x+1} \cdot 3^{y+1}$, $\langle x, y, t \rangle = 2^{x+1} 3^{y+1} 5^{t+1}$

Teorema: $\{ \ulcorner t \urcorner \mid t \text{ termine di PA} \}$ è P.R. (decidibile)

Teorema: $\{ \ulcorner \varphi \urcorner \mid \varphi \text{ formula di PA} \}$ è P.R.

Teorema: $\{ \langle \ulcorner \varphi \urcorner, d \rangle \mid d \text{ codifica una dim. di } \varphi \text{ in PA} \} := Prov_{PA}$

$Prov_{PA} \subset PA$ ed è prim. ricorsivo

Teorema: $\{ \ulcorner \varphi \urcorner \mid \varphi \text{ è un teorema di PA} \}$ è Σ_1^0 semidecidibile

$\exists d \, (\underbrace{\langle \ulcorner \varphi \urcorner, d \rangle \in Prov_{PA}}_{\text{P.R.} \to \Sigma_1^0 \text{ definibile}})$ ($\exists$: Σ_1^0)

Teorema: $num : \mathbb{N} \to \mathbb{N}$

$num(n) = \ulcorner s^n 0 \urcorner$ $\quad num(2) = \ulcorner SS0 \urcorner$

num è primitiva ricorsiva

Dim: $num(n+1) = \langle \#(s), num(n) \rangle$

Teorema: $\exists$ $sub : \mathbb{N}^3 \to \mathbb{N}$ prim. ricorsiva

$sub(\ulcorner \varphi \urcorner, i, \ulcorner t \urcorner) = \ulcorner \varphi[t/v_i] \urcorner$ φ formula, t termine

Def: $sub_0(x, y) = sub(x, 0, y)$

Def: $\exists$ $D : \mathbb{N} \to \mathbb{N}$ prim. ric. $D(\ulcorner \varphi \urcorner) = \ulcorner \varphi(\overline{\ulcorner \varphi \urcorner} / v_0) \urcorner$

$\varphi = \varphi(v_0)$

$D(\ulcorner \varphi(\ulcorner \overline{\varphi} \urcorner) \urcorner)$

$D(x) = sub_0(x, num(x))$

Lemma di diagonalizzazione:

Sia $\varphi(x)$ una formula $VL(\varphi(x)) < \{x\} \Rightarrow$ esiste formula β chiusa

$Q \vdash \beta \leftrightarrow \varphi(\ulcorner \overline{\beta} \urcorner)$

idea: β dice "io ho la proprietà $\varphi(x)$"

Corollario: $L = \{0, S, +, \cdot\}$, $True = \{\ulcorner \theta \urcorner \mid \mathbb{N} \models \theta\}$ non è L-definibile.

!!

(Teo di Tarski)

Dim: Se $True = \{n \mid \mathbb{N} \models \varphi(n)\}$ per assurdo

Per diagonalizz. $\exists \beta \quad Q \vdash \beta \leftrightarrow \neg\varphi(\ulcorner \overline{\beta} \urcorner)$

$\mathbb{N} \models \beta \leftrightarrow \neg\varphi(\ulcorner \overline{\beta} \urcorner)$

Assurdo perché $\mathbb{N} \models \beta \leftrightarrow \varphi(\ulcorner \overline{\beta} \urcorner)$. □

17-12-2022 lezione 23 Prof. Berarducci

Lemma di diagonalizzazione:

Per ogni $\varphi(x)$ L-formula esiste una L-formula chiusa β tale che:

$Q \vdash \varphi(\ulcorner \overline{\beta} \urcorner) \leftrightarrow \beta$

Dim: $L = \{0, S, +, \cdot\}$

Sia $D : \mathbb{N} \to \mathbb{N}$ $D(\ulcorner \alpha \urcorner) = \ulcorner \alpha(\overline{\ulcorner \alpha \urcorner}/v_0) \urcorner$ (↑ numero di Gödel)

D è P.R. (e in particolare, calcolabile totale)

esempio: $\alpha = \neg(x \neq 0)$ $x = v_0$

$\ulcorner \alpha \urcorner = \langle \#(\neg), \langle \#(=), \ulcorner v_0 \urcorner, \ulcorner 0 \urcorner \rangle \rangle \in \mathbb{N}$ mettiamo sia 33

$D(\ulcorner \alpha \urcorner) = D(33) = \ulcorner \neg(\overline{33} \neq 0) \urcorner$ questo sarà un altro numero

$\Rightarrow D$ è binumerabile funzionalmente in Q da una formula $\delta(x, y)$ cioè

$D(a) = b \Rightarrow Q \vdash \forall y [\delta(\underline{a}, y) \leftrightarrow y = \underline{b}]$

Per trovare β: cerco β della forma $\alpha(\ulcorner \bar{\alpha} \urcorner) = \alpha(\ulcorner \overline{\alpha} \urcorner / \sqrt{0})$

idea! voglio $Q \vdash \varphi(\overline{\ulcorner \alpha(\ulcorner \overline{\alpha} \urcorner) \urcorner}) \leftrightarrow \alpha(\ulcorner \alpha \urcorner)$

ci sono 3 tipi di oggetti: numeri $\mathbb{N}$, termini $\underline{n}$, formule

Scelgo $\alpha(x) := \forall y [\delta(x,y) \to \varphi(y)]$

$\forall n \in \mathbb{N} \quad Q \vdash \alpha(\underline{n}) \leftrightarrow \forall y [\delta(\underline{n}, y) \to \varphi(y)]$

$Q \vdash \forall y \ \delta(\underline{n}, y) \leftrightarrow y = \overline{D(n)}$

$Q \vdash \alpha(\underline{n}) \leftrightarrow \varphi(\overline{D(n)})$ Scelgo $n = \ulcorner \alpha \urcorner$

$Q \vdash \alpha(\ulcorner \alpha \urcorner) \leftrightarrow \varphi(\overline{D(\ulcorner \alpha \urcorner)})$

$\leftrightarrow \varphi(\overline{\ulcorner \alpha(\overline{\ulcorner \alpha \urcorner}) \urcorner})$

Pongo $\beta = \alpha(\overline{\ulcorner \alpha \urcorner})$.

In particolare: $PA \vdash \varphi(\ulcorner \beta \urcorner) \leftrightarrow \beta$, $\mathbb{N} \models \varphi(\overline{\ulcorner \beta \urcorner}) \leftrightarrow \beta$ □

Teorema di Tarski sulla indefinibilità della verità

Non esiste alcuna $\mathcal{L}$-formula $True(x)$ tale che $\mathbb{N} \models True(\ulcorner \beta \urcorner) \leftrightarrow \beta$

$\leftrightarrow \mathbb{N} \models \beta$

Dim: Se no, prendo: $\beta \quad Q \vdash \neg True(\overline{\ulcorner \beta \urcorner}) \leftrightarrow \beta$

Teorema: Invece esiste una formula $Teo_{PA}(x) \in \Sigma_1^0$

$[\mathbb{N} \models Teo_{PA}(\ulcorner \beta \urcorner)] \leftrightarrow (PA \vdash \beta)$

Quindi $PA \vdash \beta \Rightarrow \mathbb{N} \models \beta$ (non vale $\Leftarrow$)

Cioè esiste β tale che $\mathbb{N} \models \beta$ ma $PA \nvdash \beta$.

Lemmi Tecnici:

Ricorsione nel decorso dei valori:

Data $h: \mathbb{N}^2 \to \mathbb{N}$ primitiva ricorsiva (risp. calcolabile totale)

esiste $f: \mathbb{N} \to \mathbb{N}^2$ primitiva ricorsiva (risp. calcolabile totale)

$f(x) = h(x, \underbrace{\langle f(0), f(1), \dots, f(x-1) \rangle}_{\text{codifica della successione } (*)})$

(*) $s = \langle a_1, \dots, a_n \rangle = \prod_{i<n} p_i^{a_i+1}$

$\Pi(s,i) = \mu t \leq s\,(p_i^{t+1} \nmid s) = a_i$

Π è P.R. ma per questa codifica serve $x, y \mapsto x^y$
$i \longmapsto p_i$

Dim (f è P.R.):

$f^{\#}(x) = \langle f(0), \dots, f(x-1) \rangle$ $\quad f^{\#}(0) = \langle\ \rangle$ $\quad f(0) = h(x, \langle\ \rangle)$

$f^{\#}(x+1) = f^{\#}(x) \frown \langle f(x) \rangle$ es: $x, y \mapsto x \frown y$ (concatenazione) è P.R. (facile)

$f^{\#}(x+1) = f^{\#}(x) \frown \langle h(x, f^{\#}(x)) \rangle = H(x, f^{\#}(x))$
↳ P.R.

$\Rightarrow f^{\#}$ è P.R. $\Rightarrow f$ è P. R. perché $f(x) = h(x, f^{\#}(x))$ □

Lemma $\ulcorner Ter \urcorner$:

$\ulcorner Ter \urcorner = \{ \ulcorner t \urcorner \in \mathbb{N} \mid t \text{ è un } L\text{-termine} \}$ è P.R.

$L = \{0, s, +, \cdot\}$

$Ter(n)$:= codifica un termine

$Ter(n) \leftrightarrow n = \ulcorner 0 \urcorner \vee \exists k\ Ter(k) \wedge n = \langle \#(s), k \rangle$

$\vee\ \exists k_1, k_2\ \ Ter(k_1) \wedge Ter(k_2) \wedge n = \langle \#(+), k_1, k_2 \rangle$

$\vee$ idem con $\#(\cdot)$

Tutti i k sono $< n$.

Tutti i quantificatori sono limitati.

Se passo alla funzione caratteristica $\chi_{Ter}(n) = H(n, \langle \chi_{Ter}(0), \dots, \chi_{Ter}(n-1) \rangle)$

Teorema: Esiste $sub: \mathbb{N}^3 \to \mathbb{N}$ P.R. tale che $sub(\ulcorner \varphi \urcorner, i, \ulcorner t \urcorner) = \ulcorner \varphi(t/v_i) \urcorner$

φ formula o termine, t termine

$v_i[t/i] = t$

$v_j[t/j] = v_i$ se $j \neq i$

$(t_1 + t_2)[t/i] = t_1[t/i] + t_2[t/i]$

etc...

$(\varphi \vee \psi)[t/i] = \varphi[t/i] \vee \psi[t/i]$

etc...

Se $j \neq i$ $\quad (\forall v_j \varphi)[t/i] = \forall v_j (\varphi[t/i])$

Se $j = i$ $\quad (\forall v_i \varphi)[t/i] = \forall v_i \varphi$

$sub(\ulcorner v_i \urcorner, i, y) = y$

$sub(\ulcorner v_j \urcorner, i, y) = \ulcorner v_j \urcorner$ se $i \neq j$

$sub(\ulcorner t_1 + t_2 \urcorner, i, y) = \langle \#(+), sub(\ulcorner t_1 \urcorner, i, y), sub(\ulcorner t_2 \urcorner, i, y) \rangle$

etc ...

$sub(\ulcorner \alpha \vee \beta \urcorner, i, y) = \langle \#(\vee), sub(\ulcorner \alpha \urcorner, i, y), sub(\ulcorner \beta \urcorner, i, y) \rangle$

$$sub(\ulcorner \forall v_j \varphi \urcorner, i, y) = \begin{cases} \langle \#(\forall), \ulcorner v_j \urcorner, sub(\ulcorner \varphi \urcorner, i, y) \rangle \\ \ulcorner \forall v_j \varphi \urcorner \quad \text{se } i = j \end{cases}$$

etc ...

Oss: Questa è una def. di sub per ricorsione sul decorso dei valori.

Lemma:

$num: \mathbb{N} \to \mathbb{N}$ è P. R.

$n \mapsto \ulcorner S^n 0 \urcorner$

$$\begin{cases} num(0) = \ulcorner 0 \urcorner \\ num(n+1) = \langle \#(S), num(n) \rangle \end{cases}$$

$D(n) = sub(n, 0, num(n)) \Rightarrow D(\ulcorner \alpha \urcorner) = \ulcorner \alpha(\overline{\ulcorner \alpha \urcorner}/v_0) \urcorner$

D è P.R.

Lemma: $\{ \ulcorner \varphi \urcorner \mid \varphi$ è una L-formula $\}$ è P.R.

Similmente a come lo fatto i termini.

Lemma. $\{ \ulcorner \varphi \urcorner \mid \varphi$ è un assioma di PA $\}$ è P.R.

Dim: Schema di induzione di PA

$x = v_0$

$Ind_{\varphi, x}: \forall \vec{y} \mid \varphi(0) \wedge \forall x [\varphi(x) \to \varphi(Sx)] \to \forall x \varphi(x)]$

Le codifiche di questo tipo di formule formano un insieme IND prim. ric.

$Ind(n) \leftrightarrow \exists k < n$ "k codifica una formula" $\wedge$

$n = \langle \#(\to), \langle \#(\wedge), sub(k, 0, \ulcorner 0 \urcorner), \langle \#(\forall), \langle \#(\to), k, sub(k, 0, \ulcorner S v_0 \urcorner) \rangle, \langle \#(\forall), \ulcorner v_0 \urcorner, k \rangle \rangle$

Oss: $\{\ulcorner\varphi\urcorner \mid PA \vdash \varphi\} = \{\ulcorner\varphi\urcorner \mid \exists d \ PA \vdash_d \varphi\}$

$PA \vdash_d \varphi$ significa d codifica una dim di φ dalle regole di inferenza e dagli assiomi di PA.

$Prov_{PA} = \{\langle d, \ulcorner\varphi\urcorner\rangle \mid PA \vdash_d \varphi\}$ è P.R.

Dettagli: $d = \langle \ulcorner(T_1, \varphi_1)\urcorner, \dots, \ulcorner(T_k, \varphi_k)\urcorner\rangle$

$\forall i \le k$ "(T_i, φ_i)" o segue da una o due coppie precedenti tramite una regola o "$\varphi_i \in T_i$" o "$\underbrace{\varphi_i \in \text{assiomi di PA}}_{Ax_{PA}(\varphi_i)}$"

Oss: $$\frac{T \vdash \varphi \qquad T \vdash \varphi \to \psi}{T \vdash \varphi}$$

Siccome $P = \{\ulcorner\varphi\urcorner \mid \varphi \in \text{Assioma di PA}\}$ è P.R.

Esiste una formula $Ax_{PA}(x)$ tale che

$$\begin{cases} n \in P \Rightarrow Q \vdash Ax_{PA}(\underline{n}) \\ n \notin P \Rightarrow Q \vdash \neg Ax_{PA}(\underline{n}) \end{cases} \qquad \begin{cases} Ax_{PA} \text{ binumera in } Q \text{ le codifiche} \\ \text{degli assiomi di PA} \end{cases}$$

$Ax_{PA}(x) = \varphi(x, y)$

dove $\varphi(x,y)$ binumera funzionalmente in Q la funzione caratt. degli assiomi

A partire da $Ax_{PA}(x)$ costruisco la formula $Teo_{PA}(x) \in \Sigma_1^0$.

Corollario: $\exists \varphi$ vera in $\mathbb{N}$ con $PA \nvdash \varphi$

(Prima versione del Teo di Gödel passando per il Teo della indef. della verità.

Difetto: chi è φ?

2ª dim più costruttiva.

I Teorema di Gödel (1931):

$\exists G \quad PA \nvdash G \ , \ PA \nvdash \neg G$

Dim: Per il Lemma di diagonalit. $\exists G$, $\underbrace{PA \vdash G \leftrightarrow \neg Teo_{PA}(\ulcorner\overline{G}\urcorner)}_{(*)}$

G dice "io non sono dimostrabile"

- Se $PA \vdash G \Rightarrow \exists d \in \mathbb{N} \quad PA \vdash_d G$ → in $\mathbb{N}$: $G \equiv \neg Teo_{PA}(\ulcorner\overline{G}\urcorner)$

$\Rightarrow \exists d \in \mathbb{N} \quad Q \vdash Prov_{PA}(\underline{d}, \ulcorner \overline{G} \urcorner)$

$Prov_{PA}(x,y)$ binumera in Q $\{(d, \ulcorner G \urcorner) \mid PA \vdash_d G\}$

$\Rightarrow Q \vdash \underbrace{\exists y \; Prov_{PA}(\underline{y}, \ulcorner \overline{G} \urcorner)}_{\text{def } "Teo_{PA}(\ulcorner \overline{G} \urcorner)"} \Rightarrow PA \vdash Teo_{PA}(\ulcorner \overline{G} \urcorner)$ (*)

$\Rightarrow PA \vdash \neg G$ per def di G $\Rightarrow PA \vdash \bot$

$\bot$ perché PA è coerente quindi $PA \nvdash G$

- $PA \nvdash \neg G$:

Se $PA \vdash \neg G \Rightarrow \mathbb{N} \models \neg G$

$\Rightarrow \mathbb{N} \models Teo_{PA}(\ulcorner \overline{G} \urcorner)$ (def. di G)

$\Rightarrow \exists d \quad \mathbb{N} \models Prov_{PA}(\underline{d}, \ulcorner \overline{G} \urcorner)$

$\Rightarrow \exists d \quad PA \vdash_d G$

$\Rightarrow PA \vdash G$

$PA \vdash \bot$ Assurdo

20-12-2021 Lezione 24 Prof. Berarducci

(Slides da 148 a 165 circa)

Prop: Q è essenzialmente indecidibile

Dim: Per assurdo se esiste $T \supset Q$ coerente, stesso linguaggio con T decidibile.

Allora $Teo_T = \{\ulcorner \varphi \urcorner \mid T \vdash \varphi\}$ è decidibile $\Rightarrow$ esiste una formula Σ^0_1 $\overline{Teo_T}(x)$ che lo binumera in Q Sia $\theta : Q \vdash \neg \overline{Teo_T}(\ulcorner \theta \urcorner) \leftrightarrow \theta$

$T \vdash \theta \Rightarrow \ulcorner \theta \urcorner \in Teo_T \Rightarrow Q \vdash \overline{Teo_T}(\ulcorner \theta \urcorner) \Rightarrow Q \vdash \neg\theta \Rightarrow T \vdash \neg\theta \Rightarrow \bot$

$T \nvdash \theta \Rightarrow \ulcorner \theta \urcorner \notin Teo_T \Rightarrow Q \vdash \neg\overline{Teo_T}(\ulcorner \theta \urcorner) \Rightarrow Q \vdash \theta \Rightarrow T \vdash \theta \Rightarrow \bot$ □

Corollario: PA, $Th(\mathbb{N}, +, \cdot)$ sono indecidibili
↳ incompleta ↳ completa

Cose mancanti:

Prop: f calcolabile totale $\Rightarrow f$ binum. funzionalm. in Q da Σ^0_1

$f(x) = \mu y \, h(x,y) = 0$

Induttivamente h binumerabile funzionalmente in Q.

$$\underbrace{\text{“}f(x)=y\text{”}}_{\varphi_f(x,y)} :\equiv \underbrace{\text{“}h(x,y)=0\text{”}}_{\varphi_h(x,y,0)} \wedge \forall u<y\ \exists v\ \underbrace{\text{“}h(x,u)=v+1\text{”}}_{\Sigma_1^0}$$

$\Rightarrow \varphi_f$ binumera funzionalmente f in Q

$$f(a)=b \Rightarrow \mathbb{N} \vDash \underbrace{\text{“}f(\underline{a})=\underline{b}\text{”}}_{\Sigma_1^0} \Rightarrow Q \vdash \text{“}f(\underline{a})=\underline{b}\text{”}$$

$$Q \vdash \forall z\,[\text{“}f(a)=z\text{”} \longleftrightarrow z=\underline{b}]$$

In $M \vDash Q$, $\text{“}f(a)=z\text{”} \leftrightarrow \text{“}h(\underline{a},z)=0\text{”} \wedge \forall u<z\ \exists v\ \text{“}h(x,u)=v+1\text{”}$

$z \leq \underline{b} \ \vee\ z \geq \underline{b}$

z non può essere $> \underline{b}$ perché se no prendo $u=\underline{b}$ e ottengo l'assurdo

$\exists v$ “$h(\underline{u},\underline{b})=v+1$” ma sapevo “$h(\underline{a},\underline{b})=0$”.

Quindi $z \leq \underline{b}$, quindi $\exists n \in \mathbb{N}$ tc in M $z=\underline{n}$ quindi “$h(\underline{a},\underline{b})=0$” e “$n<\underline{b}$” contraddicendo la binumerabilità funzionale di h in 0.

$h(a,n) \neq 0 \Rightarrow Q \vdash \text{“}h(\underline{a},\underline{n}) \neq 0\text{”}$

Def: T Teoria nel linguaggio $L=\{0,S,+,\cdot\}$ è ω-coerente se non esiste alcuna L-formula $\varphi(x)$ tale che:

$$T \vdash \exists x\,\varphi(x) \qquad T \vdash \neg\varphi(\underline{0})$$

$$T \vdash \neg\varphi(\underline{1})$$

$$T \vdash \neg\varphi(\underline{2})$$

$$\vdots$$

$$\forall n \in \mathbb{N}\ T \vdash \neg\varphi(\underline{n})$$

Osservazione: $\mathbb{N} \vDash T \Rightarrow T$ è ω-coerente $\Rightarrow T$ coerente

(se T è incoerente $\Rightarrow T$ dimostra ogni cosa)

Esercizio:

$\{\ulcorner\theta\urcorner \mid PA \vdash \theta$ è ω-coerente$\}$ è definibile

$\{\ulcorner\theta\urcorner \mid \mathbb{N} \vDash \theta\}$ non è definibile

Gödel, 1931:

$T \supset Q$ ricorsivamente assiomatizzata

ω-coerente $\Rightarrow$ T incompleta (esiste θ $T \nvdash \theta$, $T \nvdash \neg\theta$)

Dim: Sia $\tau(x) \in \Sigma^0_1$ binumera $\{\ulcorner\theta\urcorner \mid \theta \in T\}$ in Q da $\overline{Prov_T}(x,y) \in \Sigma^0_1$

Sia $Teo_T(y) \equiv \exists x\, Prov_T(x,y)$

Sia $G : Q \vdash G \leftrightarrow \neg Teo_T(\overline{\ulcorner G \urcorner})$ (esiste per il punto fisso)

dico $T \nvdash G$, $T \nvdash \neg G$

① Se $T \vdash G \Rightarrow \exists n\ T \vdash_n G \Rightarrow \exists n\ (n, \ulcorner G \urcorner) \in Prov_T$

$\Rightarrow \exists n\ Q \vdash \overline{Prov_T}(\bar{n}, \overline{\ulcorner G \urcorner}) \Rightarrow Q \vdash \exists x\, \overline{Prov}(x, \ulcorner G \urcorner)$

$Q \vdash Teo(\overline{\ulcorner G \urcorner}) \Rightarrow Q \vdash \neg G \Rightarrow T \vdash \neg G \Rightarrow T \vdash \bot$

(Uso la coerenza di T non la ω-coerenza)

Quindi $T \nvdash G$.

② Dico che $T \nvdash \neg G$.

Visto che $T \nvdash G$ $\forall n$ $T \nvdash_n G$ $\forall n\ T \vdash \neg Prov_T(\bar{n}, \ulcorner \bar{G} \urcorner)$

$\forall n$ $(n, \ulcorner G \urcorner) \notin Prov_T \Rightarrow \forall n\ Q \vdash \neg Prov_T(\bar{n}, \ulcorner \bar{G} \urcorner)$ ①

Se per assurdo $T \vdash \neg G \Rightarrow T \vdash Teo_T(\overline{\ulcorner G \urcorner})$

$\Rightarrow T \vdash \exists x\ Prov_T(x, \overline{\ulcorner G \urcorner})$ ②

Contro la ω-coerenza di T.

Esempio di Teoria coerente non ω-coerente (Premessa):

$PA \vdash G \leftrightarrow \neg Teo(\ulcorner G \urcorner) \Rightarrow PA \nvdash G$, $PA \nvdash \neg G$

Ma $\mathbb{N} \models G$ o $\mathbb{N} \models \neg G$? Quale delle due?

Siccome $PA \nvdash G \Rightarrow \forall n$ $(n, \ulcorner G \urcorner) \notin Prov_{PA}$

$\forall n$ $Q \vdash \neg Prov(\bar{n}, \overline{\ulcorner G \urcorner})$

$\forall n \in \mathbb{N}$ $\mathbb{N} \models \neg Prov_{PA}(\bar{n}, \overline{\ulcorner G \urcorner})$

$\mathbb{N} \models \forall n\ \neg Prov_{PA}(\bar{n}, \overline{\ulcorner G \urcorner})$

$$\mathbb{N} \models \neg \exists n \; Prov_{PA}(\overline{n}, \ulcorner \overline{G} \urcorner)$$

$$\mathbb{N} \models \neg Teo_{PA}(\ulcorner G \urcorner)$$

$$\mathbb{N} \models G$$

Nella metateoria ho visto che T coerente $\Rightarrow$ $T \nvdash G$ dove $G : T \vdash G \leftrightarrow \neg Teo \ulcorner \overline{G} \urcorner$

(T coerente: ric. assiomatic. $\supset Q$; $\Rightarrow$: è dim. in PA)

$PA \vdash$ "T coerente" $\rightarrow$ "$T \nvdash G$"

$PA \vdash \neg Teo_T(\ulcorner \bot \urcorner) \rightarrow \neg Teo_T(\ulcorner \overline{G} \urcorner)$

$\downarrow$ per def. di G

G

Vale il $\leftrightarrow$: $PA \vdash \neg Teo_{PA}(\ulcorner \bot \urcorner) \leftrightarrow G \equiv con(PA) = \neg Teo_{PA}(\ulcorner \bot \urcorner)$

($con(PA)$: Π^0_1)

Se $PA \vdash \neg Teo_{PA}(\ulcorner \bot \urcorner) \Rightarrow PA \vdash G$

Quindi $PA \nvdash \neg Teo_{PA}(\ulcorner \bot \urcorner)$ cioè $PA \nvdash$ "PA è coerente"

2° Teorema di Gödel

La formula che dice "io non sono dimostrabile" equivale alla coerenza di Peano.

Esempio di Teoria coerente non ω-coerente:

$PA + \neg Con(PA)$ è coerente

(Con: coerenza)

$PA + \neg G$ è coerente ma ω-incoerente

$\downarrow$

perché $PA \nvdash G \Rightarrow PA + \neg G$ coerente

ma $\neg G$ equivale a $Teo(\ulcorner \overline{G} \urcorner) \leftrightarrow \exists x \; Prov(x, \ulcorner \overline{G} \urcorner)$ allora abbiamo che

$PA + \neg G \vdash \exists x \; Prov(x, \ulcorner \overline{G} \urcorner)$ perché $\forall n$ fissato $PA \nvdash_n G$, $Q \vdash \neg Prov(n, \ulcorner \overline{G} \urcorner)$

$PA + \neg G \vdash \neg Prov(n, \ulcorner G \urcorner)$

A quell'epoca si cercava una Teoria coerente per la matematica. Gödel dice che la coerenza non basta: $PA + \neg Con(PA)$ è coerente ma non affidabile.

Oggi so che la condizione che mi serviva in più è la verità, che a quel punto non esisteva ancora.

Interpretabilità:

Qualunque cosa interpreti Q allora quel qualcosa è indecidibile.

Se $Q \lhd T \supset S$ (sottoteoria di T nello stesso linguaggio) $\Rightarrow$ S è indecidibile

↳ interpretabile

Corollario: $\{\varphi \mid \vdash \varphi\}$ $\quad L = \{\in\}$ ↗ binaria

L'insieme delle formule logicamente valide in un linguaggio binario è indecidibile.

$Q \lhd \mathcal{ZF}$ $\quad L = \{\in\}$

$\cup$

$\varnothing$ $\quad L = \{\in\} \Rightarrow \varnothing$ è indecidibile

Problema della fermata (per dire che Q è indecidibile):

$K_0 = \{n \mid \varphi_n(n) \downarrow\}$

K_0 è Σ^0_1 definibile in $\mathbb{N}$

$K_0 = \{n \mid \exists t \ \underbrace{\varphi_n(n) \downarrow_{\leq t}}\}$

prim. ric. $\Rightarrow$ Σ^0_1 definibile in $\mathbb{N}$ binumerabile in Q da "$\underbrace{\varphi_x(x) \downarrow_{\leq y}}_{\Sigma^0_1}$"

$\Rightarrow$ "converge con meno di t passi"

$n \in K_0 \Rightarrow \mathbb{N} \vDash \exists t$ "$\varphi_{\underline{n}}(\underline{n}) \downarrow_{\leq t}$"

$\Rightarrow Q \vdash \exists t$ "$\varphi_{\underline{n}}(\underline{n}) \downarrow_{\leq t}$"

Poiché $\mathbb{N} \vDash Q$ vale il $\Leftrightarrow$:

$n \in K_0 \Leftrightarrow Q \vdash \exists t$ "$\varphi_{\underline{n}}(\underline{n}) \downarrow_{\leq t}$"

Quindi se so decidere Q so decidere K_0. ↯

K_0 si riduce ai teoremi di Q.

↳ $K_0 \leq_m \{\ulcorner \theta \urcorner \mid Q \vdash \theta\}$

↓

c'è una f. calcolabile tc $n \in K_0 \Leftrightarrow f(n) \in Q$

$f(n) = \ulcorner \exists t$ "$\varphi_n(n) \downarrow_{\leq t}$" $\urcorner$ è il numero di Gödel

Avendo le f calcolabili ci creo problemi indecidibili e li trasferisco dentro Q.

a) $\Box\varphi = Teo_{PA}(\ulcorner \overline{\varphi} \urcorner)$

b) $\Box$ = "φ è necessario" (per i filosofi)

regole per a):

1) $PA \vdash \varphi \Rightarrow PA \vdash \Box\varphi$

è formalizzabile in Σ^0_1 e le cose vere in Σ^0_1 sono dimostrabili in Q

2) $PA \vdash \Box\varphi \to \Box\Box\varphi$ (Peano dimostra il punto 2)

3) $PA \vdash \Box(\alpha \to \beta) \to (\Box\alpha \to \Box\beta)$

4) = 1) + 2) + 3) $PA \nvdash \neg\Box\bot$ cioè $PA \nvdash Con(PA)$

↓

2° Teorema di Gödel