3-10-2006 (1)

Calcolo dei predicati e delle proposizioni

A	B	$\neg A$	$A \vee B$	$A \wedge B$	$A \to B$	$A \leftrightarrow B$
0	0	1	0	0	1	1
0	1	1	1	0	1	0
1	0	0	1	0	0	0
1	1	0	1	1	1	1

dove A e B sono variabili proposizionali.

def (proposizione è un enunciato vero o falso) X è una proposizione se è corretto (grammaticalmente) dire: «è vero X?».

def (formula proposizionale) ($\perp$ è una formula (contraddittoria)) $\perp = A \wedge \neg A$

- A, B, C, ... (variabili) sono formule.
- $\dfrac{\varphi}{\neg\varphi}$ $\qquad \dfrac{\varphi, \ \psi}{(\varphi \wedge \psi), \ (\varphi \vee \psi), \ (\varphi \to \psi)}$

(oss è il più piccolo insieme che verifica tale proprietà.)

def (tautologia) una tautologia è una formula sempre vera (se una formula ha n variabili ci sono 2^n casi e tutti devono risultare veri).

Le tautologie giocano un ruolo nelle dimostrazioni. ESEMPIO:

Il ladro è Tizio o Caio. Non è Tizio. Quindi è Caio $\quad ((A \vee B) \wedge \neg A) \to B$. $\quad$ (ragionamento tautolo def una formula φ segue tautologicamente da altre formule $\vartheta_1 \dots \vartheta_m$ se $\vartheta_1 \wedge \dots \wedge \vartheta_m \to \varphi$ è una tautologia.

def (dimostrazione)
sia Γ un insieme di formule.
sia φ una formula
$\Gamma \vdash \varphi$ si legge da Γ segue φ.

regole per la deduzione naturale:

- $\varphi \vdash \varphi$
- $\dfrac{\Gamma \vdash \varphi}{\Gamma \cup \{\alpha\} \vdash \varphi}$
- $\dfrac{\Gamma \vdash \alpha}{\Gamma \vdash \alpha \vee \beta}$
- $\dfrac{\Gamma \cup \{\alpha\} \vdash \gamma \wedge \Gamma \cup \{\beta\} \vdash \gamma}{\Gamma \cup \{\alpha \vee \beta\} \vdash \gamma}$
- $\dfrac{\Gamma \vdash \alpha \quad \Gamma \vdash \alpha \to \beta}{\Gamma \vdash \beta}$ (modus ponens)
- $\dfrac{\Gamma \cup \{\alpha\} \vdash \beta}{\Gamma \vdash (\alpha \to \beta)}$
- $\dfrac{\Gamma \vdash \bot}{\Gamma \vdash \alpha}$ (qualsiasi)
- $\dfrac{\Gamma, \alpha \vdash \bot}{\Gamma \vdash \neg\alpha}$
- $\dfrac{\Gamma \vdash \alpha \wedge \Gamma \vdash \beta}{\Gamma \vdash \alpha \wedge \beta}$
- $\dfrac{\Gamma \cup \{\alpha\} \vdash \gamma}{\Gamma \cup \{\alpha, \beta\} \vdash \gamma}$
- $\dfrac{\Gamma \vdash \beta}{\Gamma \vdash \alpha \vee \beta}$
- $\dfrac{\Gamma \vdash \alpha \quad \Gamma \vdash \neg\alpha}{\Gamma \vdash \bot}$
- $\dfrac{\Gamma \vdash \alpha}{\Gamma, \neg\alpha \vdash \bot}$
- $\dfrac{\Gamma, \neg\alpha \vdash \bot}{\Gamma \vdash \alpha}$ (assurdo)

th $\vdash \alpha$ sse α è una tautologia.

ESEMPIO $\vdash A \to A$ $\qquad \dfrac{\emptyset\, A \vdash A}{\vdash A \to A}$

EX. $\vdash A \vee \neg A$

ESEMPIO $A \wedge B \vdash A \vee B$ $\qquad \dfrac{\dfrac{A \vdash A}{A \wedge B \vdash A}}{A \wedge B \vdash A \vee B}$

th $\{\varphi_1, \dots \varphi_m\} \vdash \psi \iff (\varphi_1 \wedge \dots \wedge \varphi_m \Rightarrow \psi)$ è una tautologia.

oss $\Rightarrow$ l'implicazione (facile) è detta correttezza
$\Leftarrow$ tale impl. è ~~dett~~ dà la completezza.

(dim) $\varphi \vdash \varphi$ (ovvio) $\qquad$ passo base

$\dfrac{\Gamma, \alpha \vdash \gamma \quad \Gamma, \beta \vdash \gamma}{\Gamma, \alpha \vee \beta \vdash \gamma}$ $\qquad$ passo ind.

~~da~~ se vale per $|\Gamma| = n$ allora vale $|\Gamma| = n+1$

5-10-2006

(soluzione EX.)

$A \vdash A$

$\neg A \vdash \neg A$

$\neg A \vdash \neg A \vee A$

$\neg(A \vee \neg A) \vdash A$ $\qquad \neg(A \vee \neg A) \vdash \neg A$

$\neg(A \vee \neg A) \vdash A \wedge \neg A$

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

$\vdash A \vee \neg A$.

def un linguaggio proposizionale L è un insieme di variabili $A, B, C, \dots$. Le L-formule proposizionali sono costruite usando $\neg \wedge \to \vee$ e

$M: L \to \{0,1\}$. M si estende ad $\tilde{M}$: L-formule $\to \{0,1\}$ usando le tavole.

ESEMPIO: $\tilde{M}(\varphi \to \psi) = \tilde{M}(\neg\varphi \vee \psi) = \max(1-\tilde{M}(\varphi), \tilde{M}\psi)$.

def ($\Gamma \models \varphi$)

Γ insieme di L-formule, φ L-formula

$\Gamma \models \varphi \overset{def}{\iff} \forall M$ L-struttura $M(\Gamma)=1 \Rightarrow M(\varphi)=1$

$(M(\Gamma)=1 \overset{def}{\iff} \forall \theta \in \Gamma \ M(\theta)=1)$.

th $\Gamma \models \varphi \iff \Gamma \vdash_{DN} \varphi$. (th di completezza)

th (di compattezza) $\Gamma \models \varphi \iff \exists \Gamma' \underset{finito}{\subset} \Gamma \ \Gamma' \models \varphi$.

EX. th (di compattezza) $\Rightarrow$ "se un grafo infinito non è tre-colorabile anche un suo sottografo finito non lo è".

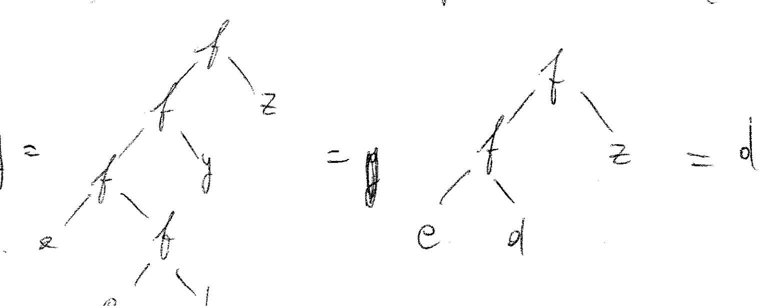
ESEMPIO $\exists x(P(x) \to \forall y\, P(y))$

caso 1 $\forall y\, P(y)$ ~~allora~~ quindi scegliendo x qualsiasi la formula val

caso 2 $\neg(\forall y\, P(y))$ ~~allora~~ quindi ~~esiste~~ $\exists x\, \neg P(x)$ e per quell'x $P(x) \to \forall y\, P(y)$ è vera a vuoto.

ESEMPIO $\forall f\ (\forall xyz\ (f(f(x,y),z)=y \to \forall ab\ a=b)$

se è vera l'ipotesi allora (scelta $x = f(a, f(c,d))$)



da cui la tesi.

OSS: si dimostra che non esiste un algoritmo per stabilire se una formula con quantificatori è sempre vera.

Regole per i quantificatori (cfr. ap. el. log.)

- valgono tutte le regole della deduzione naturale.
- in più valgono:

$$\frac{\Gamma \vdash \forall x\ \varphi(x)}{\Gamma \vdash \varphi(t)} \quad (t \text{ termine sostituibile})$$

$$\frac{\Gamma \vdash \varphi(y)}{\Gamma \vdash \forall x\ \varphi(x)}$$

dove y non è una variabile di Γ, né di φ

$$\frac{\Gamma \vdash \varphi(t)}{\Gamma \vdash \exists x\ \varphi(x)}$$

$$\frac{\Gamma, \varphi(y) \vdash \theta \quad (y \text{ non compare in } \Gamma \text{ o } \theta)}{\Gamma, \exists x\ \varphi(x) \vdash \theta}$$

$$\Gamma \vdash x = x$$

$$\frac{\Gamma \vdash \varphi(t) \quad \Gamma \vdash t = t'}{\Gamma \vdash \varphi(t')}$$

NOTA sostituibile: si dice sostituibile una t le cui variabili non sono quantificate dopo la sostituzione.

Linguaggi del primo ordine

def un linguaggio L è un insieme di simboli divisi in tre ~~gruppi~~ tipi:

i) simboli di costante
ii) simboli di funzione
iii) simboli di predicato.

un simbolo è una terna (nome, numero di argomenti (arietà), tipo)

def variabili, simboli di costante e simboli di def una L-formula atomica è del tipo termine = termine o (rel) predicato di termini.

~~le L-formule~~ se α e β sono formule allora anche $\neg\alpha$, $(\alpha \wedge \beta)$, $(\alpha \vee \beta)$, $(\alpha \to \beta)$ $\forall x\, \alpha$, $\exists x\, \alpha$ lo sono

def (L-strutture, i.e. interpretazioni)

ESEMPIO: sia (1): $\forall x\, P(x) \to \exists y\, (f(x,y) = c)$

(1) è vera nella struttura $(\mathbb{R}, x \neq 0, x \cdot y, 1)$ (sopra: P, $f(x,y)$, c)

e falsa in $(\mathbb{Z}, x \neq 0, \cancel{x}y, 1)$.

una L-struttura consiste di un dominio non vuoto dom(M) (spesso denotato semplicemente con M); una funzione che associa ad un simbolo di costante c un elemento ~~di~~ $c^{\mathrm{dom}(M)} \in$ dom(M), ad un simbolo di funzione f una funzione $f^M : (\mathrm{dom}(M))^n \to \mathrm{dom}(M)$, ed un simbolo di predicat. ~~P~~ un sottoinsieme $P^M \subset M^n$.

Semantica di Tarski

idea informale: sia M una struttura e φ una formula

se $\varphi = \forall x\, \theta(x)$ allora $M \models \varphi \overset{def}{\iff}$ ~~per~~ ogni $a \in M$ $M \models \theta$

ed analog. il caso di $\exists$

Il problema è che $\theta(x)$ non è necess. una L-form

def (valutazione)

sia V l'insieme delle variabili, sia M una L-struttura; una valutazione in M è una funzione che assegna a certe variabili elementi di M.

notazione: $v = (a_1/x_1, \dots a_n/x_n)$ è la valutazione $v(x_i) = a_i \in M$.

def (variabili libere di una L-formula φ)

per induzione

~~VL(∀x α)~~ se α è atomica $VL(\alpha)$ = tutte le var. α

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

$VL(\alpha \wedge \beta) = VL(\alpha) \cup VL(\beta)$ ed analog. per $\vee$ $\to$ $\neg$.

def ~~(L-struttura M)~~

sia M una L-struttura

Un L-termine con parametri da M è una coppia $\langle t, v\rangle = t(v)$ con t L-termine, v valutazione

Una L-formula con parametri è $\langle \varphi, v\rangle = \varphi(v)$, φ L-formula, v valutazione

semantica dei termini

siano M una L-struttura, t un L-termine, v una valutazione in M dom(v) ⊃ Var(t) allora $M(t(v)) \in \mathrm{dom}(M)$ e

se $t = x$ var. allora $M(x(v)) = v(x) \in M$

se $t = c$ cost allora $M(c(v)) = c^M \in M$.

se $t = f(t_1, \dots t_n)$ allora $M(f(t_1, \dots t_n)(v)) = f^M(M(t_1(v)), \dots M(t_n(v)))$

semantica delle formule

M L-struttura, φ L-formula, v valutazione, $\mathrm{dom}(v) \supset VL(\varphi)$ allora

$M(\varphi(v)) \in \{0,1\}$ e

se $M((\varphi_1 \vee \varphi_2)(v)) = \max\, M(\varphi_1(v)), M(\varphi_2(v))$

$M((\forall x\,\varphi)(v)) = \inf_{a\in dom(M)} M(\varphi(v, a/x))$

$M((\exists x\,\varphi))(v) = \sup_{a\in dom(M)} M(\varphi(v, a/x))$

(per cui $M \models (\exists x\,\varphi)(v) \Leftrightarrow \exists a \in dom(M)\ M \models \varphi(v, a/x)$)

-(Δ) $M((t_1 = t_2)(v)) = 1 \Leftrightarrow M(t_1(v)) = M(t_2(v))$.

EX φ chiusa (i.e. $VL(\varphi) = \emptyset$) ~~allora~~ implica p.o. v, v' valutazioni in M. $M \models \varphi \Leftrightarrow M \models \varphi(v')$

def $M \models \varphi \Leftrightarrow$ per qualche v $M \models \varphi(v)$?

<u>conseguenza logica</u>

sia T una L-teoria (insieme di L-formule chiuse) e sia φ una L-formula chiusa allora $T \models \varphi \overset{def}{\Longleftrightarrow} \forall$ L-struttura M

$Mod(T) \overset{def}{=} \{M \mid \forall \theta \in T\ M \models \theta\} \subset Mod(\varphi) \overset{def}{=} \{M \mid M \models \varphi\}$.

oss se T è contraddittoria $Mod(T) = \emptyset$ è incluso in ogni $Mod(\varphi)$.

NOTA: espansione del linguaggio
sia $L' \supset L$ e siano φ L-formula chiusa ed M una L'-struttura allora

$M \models \varphi \Longleftrightarrow M|_L \models \varphi$.

def T è completa nel linguaggio L se p.o. L-formula chiusa φ $T \models \varphi$ o $T \models \neg\varphi$.

Riassunto:
$T \models \varphi \overset{def}{\Longleftrightarrow} \forall$ L-struttura $(M \models T \Rightarrow M \models \varphi)$
(dove T = L-teoria = insieme di L-formule chiuse)

oss ~~cioè~~ è utile per negare non per provare per provare si usa la D.N.
($T \vdash_{DN} \varphi \overset{def}{\Longleftrightarrow}$ φ si può dedurre da T con le regole della deduzione naturale)

<u>Regole D.N.</u>

$$\frac{T \vdash \forall x\,\varphi}{T \vdash \varphi(t/x)}$$
($\forall e$)

(t L-termine sostituibile per x in φ i.e. non ci sono var. z in t t.c. $\forall x\,\varphi$ contiene una sottoformula $\exists z\,\theta$ (o $\forall z\,\theta$) contenente un'occorrenza libera di x in φ.)

($\vdash\forall$) $$\frac{T \vdash \varphi(y/x)}{T \vdash \forall x\,\varphi}$$ (y non occorre libera in T, φ)

($\vdash\exists$) $$\frac{T \vdash \varphi(t/x)}{T \vdash \exists x\,\varphi}$$ (t L-termine sostituibile) (ex. provare e capire perché ?)

($\exists\vdash$) $$\frac{T, \varphi(y/x) \vdash \psi}{T, \exists x\,\varphi \vdash \psi}$$ (y non libera in T o ψ)

($\vdash =$) $T \vdash t = t$

($=e$) $$\frac{T \vdash \phi(t/x) \qquad T \vdash t = t'}{T \vdash \phi(t'/x)}$$ t, t' sostituibili per x in ϕ.

(RAA) $$\frac{T, \neg\alpha \vdash \bot}{T \vdash \alpha}$$ $$\frac{T, \alpha \vdash \bot}{T \vdash \neg\alpha}$$

RAA si usa in dimostrazioni tipicamente non co-
struttive p. es. $\neg\forall x\, Px \vdash \exists x\, \neg Px$

EX $\neg\forall x\, P(x) \vdash_{DN} \exists x\, \neg P(x)$

$$\neg P(a) \vdash \neg P(a) \qquad (Ax)$$

$$\neg\exists x\, \neg P(x),\ \neg P(a) \vdash \neg P(a) \qquad (Wk)$$

$$\neg\exists x\, \neg P(x),\ \neg P(a) \vdash \exists x\, \neg P(x)$$

$$\text{"} \quad \text{"} \quad \text{"} \vdash \neg\exists x\, \neg P(x)$$

$$\text{"} \quad \text{"} \quad \text{"} \vdash \bot$$

$$\neg\exists x\, \neg P(x) \vdash P(a) \qquad \text{RAA}$$

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

$$\neg\forall x\, P(x),\ \neg\exists x\, \neg P(x) \vdash \forall x\, P(x) \qquad \text{WK}$$

$$\text{"} \quad \text{"} \vdash \neg\forall x\, P(x)$$

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

$$\vdash \neg\forall x\, P(x) \to \exists x\, \neg P(x)$$

EX $\vdash \exists x\, (Px \to \forall y\, Py)$

$$\neg P(a),\ P(a) \vdash \bot$$

ESEMPIO di uso RAA — th B.-W.

EX RAA equivale a $\dfrac{T, A \vdash B \qquad T, \neg A \vdash B}{T \vdash B}$

24-10-2006

th T coerente ($T \nvdash_{DN} \bot$) allora T ha modello.

(dim) Lemma T coerente $\Rightarrow$ $T \cup \{\phi\}$ è coerente
oppure $\Rightarrow$ $T \cup \{\neg\phi\}$ è coerente

Lemma $T \cup \{\phi(c)\}$ coerente $\iff$ $T \cup \{\exists x\, \phi(x)\}$ coer.
e c è una cost che non compare in T e ϕ

Lemma I insieme lin. ord. e $(T_i \mid i \in I)$ è
t.c. $\forall i$ T_i L-th. $\forall j$ $i < j \to T_i \subset T_j$. Inol-
tre se $\forall i$ T_i è coerente allora
$\bigcup \{T_i\}_{i\in I}$ lo è.

(dim) $\bigcup\{T_i\} \vdash \bot \overset{def}{\iff} \exists\, T' \subseteq_{finito} \bigcup\{T_i\}$ $\ T' \vdash_{DN} \bot$
$\exists i$ ~~tc~~ $T' \subset T_i$ $\ T_i \vdash \bot$

def (insieme di Hintikka), th. di Hintikka)

prop una ~~insieme~~ th. di Hintikka ammette un modello.

se T L-th è coer. allora esiste ~~una~~ $L' \supset L$ L'-th
$T' \supset T$ allora:

① T' è coer, massimale (tra le L'-th coeren)
per ogni L'-enunciato φ $\varphi \in T'$ o $\neg\varphi \in T'$.

② $\exists x\, \varphi(x) \in T' \Rightarrow \exists c \in L'$ $\ \varphi(c) \in T'$

③ $\neg\forall x\, \varphi(x) \in T' \Rightarrow \exists c \in L'$ $\ \neg\varphi(c) \in T'$

③ (usa lemma successivo):
$T \cup \{\neg\forall x\, \varphi(x)\}$ coer. $\iff$ $T \cup \{\neg\varphi(c)\}$ coer.
$c \notin T$, $\varphi(x)$.

caso (finito o) numerabile ($|L| \leq \aleph_0$)

$|L\text{-formule}| = \aleph_0$ sia $C = \{c_i \mid i \in \mathbb{N}\}$ un insieme di costanti non in L allora $\overset{\text{allora}}{\vee}$ $L' = L \cup C$ è numerabile e $|L'\text{-formule}| = \aleph_0$ (L'-formule $= \{\varphi_i \mid i \in \mathbb{N}\}$.

sia $T = T_0$ $\quad T_{n+1} = \begin{cases} \{\varphi_n\} \cup T_n & \text{se è coerente} \\ \{\neg\varphi_n\} \cup T_n & \text{se è coerente}^{(*)} \end{cases}$

si definisce $T' = \bigcup \{T_n\}_{n \in \omega}$.

* Inoltre se $\varphi_n \in T_{n+1}$ è della forma $\exists x\, \theta(x)$ si sceglie $c_i \notin L(T_n)$ e $\varphi(c_i) \in T_{n+1}$.

Per i lemmi precedenti T' è coer., massim e di Henkin, ~~…~~, quindi T' è di Hintikka è di conseguenza ha un modello.

ESEMPIO (insieme di Hintikka)

$\{ \exists x\, P(x) \vee \neg Q(x) \wedge \forall x\, Q(x)$

$\exists x\, P(x) \vee \neg Q(x), \quad \forall x\, Q(x)$

$P(c) \vee \neg Q(c)$

$P(c) \quad \circ \quad \neg Q(c) \quad Q(c)$

$c = c\ ,\ Q(c) \}$

OSS $\forall x\, P(x) \to Q(x)$ non appartiene all'insieme, per cui gli insiemi di Hintikka non sono (necessariamente) massimali.

(metodo dei tableaux alternativo a DN: si procede biforcando, se si trova un modello in esso vale anche per il punto di partenza)

OSS il metodo di tableaux non termina necessariamente p.es. $\forall x\, \exists y\, P(x,y)$)

il ... ha modelli sse il metodo

dei tableaux porta a contraddizione su ogni ramo.

th $T \models \varphi \Rightarrow T \vdash_{DN} \varphi$ (completezza)

(dim) $T \nvdash \varphi \Rightarrow T \cup \{\neg\varphi\}$ coer.

per cui esiste un modello $M \models T, \neg\varphi$ vale a dire $T \not\models \varphi$.

OSS la correttezza ($\Leftarrow$) si dimostra ricorrendo ad idee di metateoria del tutto simili a ciò che si vuole dimostrare!

Cor $T \models \varphi \Rightarrow \exists T' \subset_{\text{finito}} T \quad T' \models \varphi$ (th. di compattezza 1)

Cor T non ha modelli implica che esiste $T' \subset_{\text{finito}} T$ t.c. T' non ha modelli (cpt. 2)

se ogni $T' \subset_{\text{finito}} T$ ha un modello allora anche la th T ce l'ha (cpt 3),

ESEMPIO $L = \{0, 1, \cdot, +, \overset{\sigma}{\vee}<\}$ e sia $\mathbb{N}$ la L-str. con i simboli interpr. come suggerito dal nome. $\overset{\text{sia}}{\vee}$ $T = th(\mathbb{N}) = \{\varphi \mid \mathbb{N} \models \varphi\} \supset PA$.

Sia ora $L' = L \cup \{c\}$ e $T' = \omega + 1$

(accenno all'algoritmo Davisson-Robinson-Putnam)

NOTA ~~In~~ Nella logica del II ord. non vale la correttezza e dunque neanche la completezza, per cui le dimostrazioni non possono essere desunte da un insieme di regole.

26-10-2006

<u>th</u> (cenno di completezza ~~non~~ numerabile)

(dim) <u>th</u> sia $|X| = k$ allora $X = \{a_i \mid i < k\}$ e $\forall \alpha$.

$\alpha < k \quad |\{a_i \mid i < \alpha\}| < k$

sia $|L| = k > \aleph_0$ e $C = \{c_i \mid i < k\}$

T_0 come nel caso numerabile

se $i+1$ è successore di T_i allora T_{i+1} come al caso numerabile.

se λ ord. limite $T_\lambda = \bigcup_{i \in \lambda} T_i$

PA $\quad L = \{0, \sigma, +, \cdot\}$

$Q \subset PA$ (Q teoria di Robinson)

$0 \neq \sigma(x)$

$\forall x y \quad \sigma(x) = \sigma(y) \rightarrow x = y$

$x \neq 0 \Rightarrow \exists y \ \sigma(y) = x$

$x + 0 = x$

$x + \sigma(y) = \sigma(x+y)$

$x \cdot 0 = 0$

$x \cdot \sigma(y) = xy + x$

Modelli (oltre a $\mathbb{N}$) per la teoria Q:

$\mathbb{Z}[x]^+ \stackrel{def}{=} \{0\} \cup \{\sum_0^m a_i x^i \mid a_m > 0\}$

<u>EX</u> la teoria Q di Robinson ha un modello in cui + non è commutativo.

<u>EX</u> $\exists \varphi$ ~~tale~~ ~~in~~ $\mathbb{N} \models \varphi$, $Q \nvdash \varphi$.

$\forall x \ \exists y \quad x = 2y \ \vee \ x = \sigma(2y)$

~~... assiomi~~

induzione $(\forall x\, \varphi)$ (1° ordine)

$$\forall y \; \big((\varphi(0,y) \wedge \forall u (\varphi(u,y) \to \varphi(\sigma(u), y)) \to \forall x\, \varphi(x,y) \big)$$

induzione (un solo assioma, ma 2° ordine)

$$Q + \forall P \, (P_0 \wedge \forall x (P_x \to P_{\sigma(x)})) \to \forall y \; P_y \,]$$

Th l'unico modello di PA^2 (peano del 2° ordine) è $\mathbb{N}$.

NOTA il problema di PA^2 è che in una logica del 2° ord ~~PA~~ non esiste un concetto soddisfacente di $\vdash$. Infatti $PA^2 \vdash \varphi \Rightarrow PA^2 \models \varphi$ (ma non è detto il viceversa).

EX ~~Th~~ $PA^1 \models \forall x \exists y \, (2y = x \vee 2y+1 = x)$ $(= P(x))$

$Q \vdash P(0)$

$Q \vdash$ ~~$\forall x$~~ $P(x) \to P(\sigma(x))$

$PA \vdash \forall x \; P(x)$

OSS $\omega + 1$ soddisfa PA^1, ma non è isom. a $\mathbb{N}$.

NOTA $\exists M \quad M \models PA^1 \quad M \not\cong \mathbb{N} \quad |M| = \aleph_0$

$T = PA^{(1)} + \{c > 0, \dots c > \dots\}$ ha modello (esterzo) quindi è coerente (correttezza) e per completezza T ha un modello (di classi di equivalenza) di termini (numerabile). (Lowenheim-Skolem verso il basso in forma debole).

si definisce $x \leq y \leftrightarrow \exists z \, (x + z = y)$

EX $PA^1 \vdash$ ($\leq$ è un ordine lineare)

ESERCIZI (completezza) 31-10-2006

1) se un grafo non è 3-colorabile, anche un sotto grafo finito non lo è.

2) (a) ogni ordine parziale finito può essere reso totale

(b) la stessa cosa vale per ordini infiniti

3) Non esiste una teoria T nel $L = \{E\}$ rel. bin. t.c. $Mod(T) = \{$grafi connessi$\}$.

(def un grafo $G = (V, E)$ è connesso sse ① $\forall x y \; E(x,y) \to E(y,x)$ ② $\forall x \neg E(x,x)$ ③ $\forall x y \in V \; \exists n \in \mathbb{N} \; \exists a_1, \dots a_n \in V$ $x = a_1 E a_2 E \dots E a_n = y$. $(\Leftrightarrow \neg \exists A, B \subset V \; A \cap B = \emptyset, \; A \cup B = V$ $\forall x \in A \; \forall y \in B \; \neg E(x,y))$)

(il 3° EX è simile all'esistenza di un modello diverso dai naturali)

th Q di Robinson $\{0, \sigma, +, \cdot\} = L$

$PA = (Q +$ ~~PA~~ schema d'induzione)

$\mathbb{N}, \; \mathbb{Z}^+[x] \models Q$

$\mathbb{N} \models PA \quad \mathbb{Z}[x]^+ \not\models PA$

$\exists$ ~~m~~ $M \not\cong \mathbb{N} \quad M \models PA$

th di Rosser (raffinamento del th di Goedel). Qualunque teoria T che contiene Q coerente r.e.

assiomatizz. ~~...~~ incompleta

Idea problemi ~~...~~ cardinali $2^{230402457}$ ~~...~~ è primo?

In questo caso ~~non~~ esiste un algoritmo per rispon-

~~nel cubo di per risolvere nel~~ cubo di 18

Rubik esistono ~~esiste~~ un algoritmo per sapere se si può risolvere in 18 mosse

problemi $\Pi_1^0 = \forall$ concreti vale a dire

$\forall m\ \exists$ un primo tra n e $2n$. (infatti fissato n il problema è concreto)

Π_1^0 sono nella forma $\forall x\ P(x)$ dove x varia su $\mathbb{N}$, $\mathbb{Q}$, Grafi finiti e P è t.c. c'è un algoritmo che dato in input x stabilisce se $P(x)$ o $\neg P(x)$ (cioè $\{x \mid P(x)\}$ è decidibile)

(NOTA: il dominio degli input è l'insieme delle parole finite Σ^* su un alfabeto Σ finito per cui è numerabile).

Per ora un calcolatore è una macchina di Turing, un algoritmo un insieme di istruzioni eseguibili da un calcolatore

def sia D un dominio ammissibile (per es $D = \mathbb{N}, \mathbb{Q}$ o più in gen. $D = \Sigma^*$) sia $P \subset D$. P è decidibile se esiste un algoritmo eseguibile su un calcolatore ideale se dato in input $x \in D$ fornisce in output 0 se ~~$\neg P(x)$~~ $x \notin P$ ed 1 se $x \in P$.

def una funzione $f: \mathbb{N} \to \mathbb{N}$ è calcolabile se esiste un algoritmo A che dato n in input, termina dopo un numero finito di passi e fornisce $f(n)$ in output.

per dimostrare che un Π_1^0 è falso basta esibire un controesempio; se è vero serve una dimostrazione.

Π_2^0 $\forall x\ \exists y\ P(x,y)$ $\quad P \subset D^2$ decidibile

ESEMPIO: esistono infiniti primi di Mersenne

$\forall n\ \exists p$ p primo $\wedge$ $2^p - 1$ è primo e $2^p - 1 > n$

In tali problemi sia la falsità che la verità deve essere dimostrata

ESEMPIO (Π_1^0): congettura di Fermat

$\forall n$ $\quad 2^{2^n} + 1$ è primo

$2^{2^5} + 1 = 641 \times 6700417$.

ESEMPIO (Π_1^0): congettura di Riemann

essa è equival. a $\forall n \underbrace{\sum_{d \mid n} d}_{\text{grado di precisione}} \leq H_n + \log(H_n)\, e^{H_n}$

dove $H_n = \sum_{i=1}^{n} \frac{1}{i}$

ESEMPIO (Π_1^0) Th dei colori

$\forall G$ grafo planare finito è 4-colorabile.

OSS i problemi concreti possono essere irrisolti solo per mancanza di tempo.

<u>Gerarchia aritmetica</u>

$\Pi_1^0 = \forall$ concreto $\qquad \Sigma_1^0 = \exists$ concreto

$\Pi_2^0 = \forall\exists$ concreto $\quad \Sigma_2^0 = \exists\forall$ concreto

$\Pi_3^0 = \forall\exists\forall$ " $\quad \Sigma_3^0 = \exists\forall\exists$ " ...

Hilbert all'inizio del 900 auspicava l'esistenza di un ~~modello~~ sistema di assiomi $\forall$ (z.r.si assiomatizzato) $T = (ZF, ?, ...)$ t.c. $\forall$ problema Π_2^0, φ, c'è un controesempio, o una dimostrazione in T (e non entrambi). Gödel dimostrò che ciò non è possibile ed inoltre dato un qualsiasi sist. di assiomi T esiste un problema Π_1^0 vero, ma non dimostrabile nel sistema T.

(Q dimostra tutti i problemi concreti veri
PA dimostra alcune verità Π_k^0
ZF dimostra qualcosa in più)

3-11-2006

def un insieme $A \subset \mathbb{N}^k$ si dice decidibile se esiste $\chi_A : \mathbb{N}^k \to \{0,1\}$ è calcolabile.

def $A \subset \mathbb{N}^k$ è Π_1^0 sse $A = \{x \mid \forall y\ \theta(x,y)\}$ con θ decid.

def $A \subset \mathbb{N}^k$ è Π_2^0 sse $A = \{x \mid \forall u \exists v\ \theta(x,u,v)\}$ con θ ".

def A è aritmetico se $A \in \bigcup \{\Pi_n^0\}_{n\in\omega}$

th A è aritmetico sse A è definibile in $(\mathbb{N}, +, \cdot, 0, 1)$

(i.e. $A = \{x \mid \mathbb{N} \models \varphi(x)\}$ φ L-form. $L = \{+, \cdot, 0, 1\}$.

oss Basta mostrare $\{$decidibili$\} \subset \{$definibili$\}$.

(infatti questo implica $\{$aritmetici$\} \subset \{$definibili$\}$.

th esiste una L-formula $\varphi(x,y)$ t.c. $\{(x,y) \in \mathbb{N}^2 \mid \mathbb{N} \models \varphi(x,y)\} =$

(dim) ~~funzione~~ una $f : \mathbb{N}^k \to \mathbb{N}$ è definibile sse ~~il suo graf~~ è definibile $\{(x,y) \in \mathbb{N}^{k+1} \mid f(x) = y\}$ è def.

lemma esiste una funzione definibile $\beta : \mathbb{N}^3 \to \mathbb{N}$ (~~β di Gödel~~) t.c. $\forall n$ $\forall (b_i)_{0\le i\le n}$ $\exists e, d$

$\beta(e,d,0) = b_0 \quad \beta(e,d,1) \ldots \quad \beta(e,d,n) = b_n$

(digressione sulle codifiche)

(dim) una tale β è f. es. la β di Gödel

$\beta(e,d,i) \longmapsto z \iff \exists q\ (e = q[(i+1)d+1] + z \ \wedge$
$\wedge\ 0 \le z < (i+1)d+1)$

th (cinese dei resti)

dato $b_0, \ldots b_n \in \mathbb{Z}$ se $\{a_0, \ldots a_n\} \in \mathbb{Z}$ sono rel. primi allora esiste x t.c. $x \equiv b_i \pmod{a_i}$

lemma $\forall n$ ~~$\forall x$~~ $\in \mathbb{N}$ $\exists d > x$ t.c.

$d+1,\ 2d+1, \ldots\ nd+1$ sono rel. primi

(dim) $d = y! \quad y > n \quad y > x$

scegliendo $y > b_0, \ldots b_n, n$ e $d = y!$ si soddisfano le ipotesi del lemma. scegliendo c come nel th. cin. del resto β risulta def

(b_i = resto $(c/(i+1)d+1)$)

oss nella dimostrazione si usa il fattoriale ma nella def di β non compare!

Corollario 2^n è definibile, i.e. esiste $\varphi(x,y)$ $L = \{+, \cdot, 0, 1\}$

$2^a = b \iff \mathbb{N} \models \varphi(a,b)$

(dim) $2^a = b \iff \exists (b_i)_{0\le i\le a}$ t.c. $b_0 = 1$ $b_{i+1} = 2b_i$ $\forall i<a$ $\iff$

$\iff \exists e, d$ t.c. $\beta(e,d,0) = 1$ $\underbrace{\beta(e,d,i+1) = 2\beta(e,d,i)}_{\forall i<a}$

$\exists y\ \beta(e,d,i) = y \wedge \beta(e,d,i+1) = 2y$

EX n è definibile in $(\mathbb{N}, +, \cdot, 0, 1)$

OSS a partire da $(\mathbb{N}, +, \cdot, 0, 1)$ si definiscono al primo ordine 2^n, $n!$ etc. Al secondo ordine si riesce a fare anche di più con solo $(0, \sigma)$.

EX un insieme non definibile si trova per diagonalizzazione.

corollario (*) $\{n \mid \mathbb{N} \models \varphi_n(n)\}$ non è def. * alla sol. di EX.

th decidibili $\subset$ definibili

(dim) postposta (idea: tramite β di Gödel ...)

corollario non esiste algoritmo per sapere se ϑ è vero in $\mathbb{N}$.

(idea di dim) altrimenti $\{n \mid \mathbb{N} \models \varphi_n(n)\}$ è dec. quindi definibile (th) in contradd. al coroll. precedente

17-11-2006

EX $L = \{E\}$ assiomi dei grafi non orientati

$$T_{gr} = \left(\forall xy \begin{array}{l} E(x,y) \to E(y,x) \\ \neg E(x,x) \end{array} \right.$$

un grafo connesso $G \stackrel{def}{=} ((V, E) \models T_{gr}) \wedge \boxed{(E \subset V^2)}$
$\wedge \neg \exists A, B < V \quad A \cap B = \phi \wedge A \cup B = V \quad \forall x, y \quad x \in A \wedge y \in B \to \neg \exists (x,y)$. $(V, E) \models \neg \exists A, B$ predicati unari, etc.

Non esiste una L-teoria T_{gre} t.c. $Mod(T_{gre})$ = grafi connessi.

soluzione: per assurdo una tale T_{gre} esiste

fissato n $\quad \varphi_n(x,y) =$ "dist $(x,y) \leq n$".

"$\varphi_0(x,y) \leftrightarrow x = y$" $\quad \varphi_{n+1}(x,y) \leftrightarrow \varphi_n(x,y) \vee \exists z \; \varphi_n(x,z) \wedge E(z,y)$

OSS

$G \models \varphi_n(x,y)$)

$L^* = \{E, a, b\}$

sia $T^* = T_{gre} \cup \{\neg \varphi_1(a,b), \neg \varphi_2(a,b), \dots\}$

mostrando che T^* non ha modelli e che invece li ha si giunge ad un assurdo.

T^* non ha modelli "perché uno di tali modelli sarebbe un grafo sconnesso e connesso". D'altra parte un sottoinsieme finito S di assiomi di T^* è contenuto in $T_{gre} \cup \{\neg\varphi_1(a,b), \neg\varphi_2(a,b), \dots \neg\varphi_N(a,b)\}$ che ha modello (a — · — · — · — · — b)

EX sia $\mathbb{K} = \{G = (V, E) \mid G$ è connesso$\}$ (classe propria)

(def una classe $\mathbb{K}$ di L-strutture è elementare se esiste T : $\mathbb{K} = Mod(T)$.)

e sia $Th(\mathbb{K}) = \{\varphi \; L\text{-enunciati} \mid \forall G \in K \quad G \models \varphi\}$

grafi connessi $\subsetneq Mod(Th(\mathbb{K}))$

(!) trovare un modello di $Th(\mathbb{K})$ ma non connesso.

EX se ogni sottografo finito di $G = (V, E)$ è 3-colorabile anche G è 3-colorabile

(dim) dato $G = (V^G, E^G)$ $\quad L' = \{E, c_v \mid v \in V\}$

$T' = D(G) = \{E(c_v, c_{v'}) \mid (v, v') \in E^G\} \cup \{\neg E(c_v, c_{v'}) \mid (v, v') \notin E^G\}$
(diagramma di G). $\quad \cup \{\neg(c_v = c_{v'}) \mid v \neq v'\}$

$M \models D(G)$ sse $M \mid_{L - \{E\}} \supset G = (V, E)$.

sia T = "th delle tre-colorazioni di G"

$L = \{E, c_v, G, R, B \mid v \in V^G$ e G, R e B sono pred. unari$\}$

assiomi di T:

$\forall xy\ (E(x,y) \wedge G(x)) \to \neg G(x)$ ...

ogni 3-colorazione $f: V^G \to \{g, r, b\}$ di G, induce un modello M di T, dove M è il grafo G con i predicati G, R, B interpretati in M. Viceversa dato $M \models T$ si ottiene una colorazione di G ($v \in V^G$ $f(v) = r \Leftrightarrow M \models R(c_v)$). Per cui esiste una 3-colorazione di G sse $\exists M$ $M \models T$ sse T coerente sse $\forall S \subseteq_{\text{finito}} T$ è coerente. Ora ogni S vive se $S \subseteq_{\text{finito}} D(H)$ dove $H \subseteq_{\text{finito}} G$, con "vertici di H" $= \{v \mid c_v$ appare in $S\}$. Per cui se si assume la 3-colorabilità di ogni sottografo finito ~~segue~~ (da cui la coerenza di ogni $S \subseteq_{\text{finito}} T$) segue la 3-colorabilità di tutto G.

EX ogni ordine parziale può essere reso totale

$$T = \forall xy \begin{cases} x \leq y \wedge y \leq z \to x \leq z \\ x \leq x \\ x \leq y \wedge y \leq x \to x = y \end{cases}$$

per essere totale deve verificare $\forall xy$ $x \leq y \vee y \leq x$.
(si vuole far vedere che $(A, \leq_A)$ parziale può essere immerso in $(B, \leq_B)$ totale), diciamo anche che "B totalizza A")

A è finito) $\exists$ el massimale infatti la successione $a_0 < a_1 < \dots$ è finita altrimenti si avrebbero $i \neq j$ t.c. $a_i = a_j \wedge a_i < a_j$.
$A \setminus \{$el. massimale$\}$ per induzione è totalizzabile ed aggiungendo el massimale in fondo A è totale.

A infinito) ci si riduce al caso finito usando la completezza; per questo è sufficiente trovare che un modello che soddisfa gli assiomi dell'ordine totale ed inoltre che $c_a \leq c_{a'}$ se $a \leq_A a'$ e $a \neq a'$ implica $c_a \neq c_{a'}$.
(Ogni modello $B \models T$ contiene una totalizzazione di A) Resta da dimostrare che T è coerente ...

def (funzioni ricorsive primitive)
$f: \mathbb{N}^k \to \mathbb{N}$ per vari k. Sono ricorsive primitive: $z(x) = 0$ $\sigma(x) = x+1$ $U_i^n(x_1, \dots x_n) = x_i$.
Sono ricorsive primitive composizione di ric. prim. e def. per ric. prim. Si dice che f è definita per ricorsione primitiva da h e da g se: $f(0, \vec{y}) = g(\vec{y})$, $f(x+1, \vec{y}) = h(x, \vec{y}, f(x, \vec{y}))$.
Le funzioni ricorsive primit. sono le più piccole classe contenente z, σ, U_i^n chiusa per compos. e ric. prim.

OSS se $g: \mathbb{N}^3 \to \mathbb{N}$ è ric. prim. allora $f(x,y) = g(y,x,y)$ è ric. prim. $(f(x,y) = g(U_2^2(x,y), U_1^2(x,y), U_2^2(x,y))$.

ESEMPIO: + è prim ric
$(x + 0 = x \qquad x + \sigma(y) = \sigma(x+y))$
$+(x,0) = x = U_1^1(x) \qquad +(x, \sigma(y)) = \sigma(U_3^3(\dots))$

ESEMPIO: $\cdot$ è prim ric.
$\cdot(x,0) = 0 = U_2^2(x) \quad \cdot(x, \sigma(y)) = +(\cdot(x,y), x)$

ALTRI: x^y è prim. ric. ed anche il predecessore.

$\mu: \mathbb{N} \to \mathbb{N}$ $\quad \mu: \begin{cases} x \to x-1 & \text{se } x>0 \\ 0 \to 0 \end{cases}$

$\mu(0)=0 \qquad \mu(x+1) = U_1^2(x, \mu(x))$

def $P \subset \mathbb{N}^k$ è pr. ric. sse $\mathbb{1}_P: \mathbb{N}^k \to \{0,1\}$ è prim. ric.

$\dot{-}: \mathbb{N}^2 \to \mathbb{N}$ $\qquad x \dot{-} 0 = x$
$\qquad x \dot{-} \sigma(y) = \mu(x \dot{-} y)$

l'uguaglianza è prim. ric., infatti l'uguaglianza a zero lo è ed il $\leq$ lo è.

$\mathbb{1}_=(x,y) = \mathbb{1}_\leq(x,y) \cdot \mathbb{1}_\leq(y,x)$

EX $P(x) \leftrightarrow x$ è primo $\qquad P(x)$ è prim. ric.

th I predicati primitivi ricorsivi sono chiusi per $\wedge$, $\vee$, $\neg$, $\to$, $\forall x \leq y$, $\exists x \leq y$. (gli insiemi prim. ric. sono chiusi per $\cap$, $\cup$, compl., ...

$\mathbb{1}_{P \cap Q} = \mathbb{1}_P \cdot \mathbb{1}_Q \qquad \mathbb{1}_{\neg P}(x) = 1 \dot{-} \mathbb{1}_P(x)$

th siano g, h prim. ric. e P pred. prim. ric. e sia $f(x) = \begin{cases} g(x) & \text{se } P(x) \\ h(x) & \text{se } \neg P(x) \end{cases}$ allora

$f(x)$ è prim. ric.

(dim) $f(x) = g(x)\, \mathbb{1}_P(x) + h(x)\, \mathbb{1}_{\neg P}(x)$

ESEMPIO la produttoria $f(n) = \prod_{i=0}^{n} h(i)$ con h pr. ric. è prim. ric.

(dim) $f(0) = h(0)$
$f(n+1) = f(n)\, h(n+1)$

analogo per sommatoria.

th

26

th sia $P(x) \leftrightarrow \forall y \leq x\ Q(y)$

Q prim. ric $\to$ P prim ric.

(dim) $\mathbb{1}_{P(x)} = \prod_{y \leq x} \mathbb{1}_{Q(y)}$

anche $P(x) \leftrightarrow \forall y \leq x\ Q(x,y)$ allora ...

(dim) $R(x,z) \leftrightarrow \forall y \leq x\ Q(y,z) \wedge P(x) \leftrightarrow R(x,x)$ e segue dalla prec.

corollario se $P(x) \leftrightarrow \exists x \leq y\ Q(x,y)$ allora
Q è prim. ric. $\Rightarrow$ P prim. ric.

(dim) ovvia perché $\exists x \leq y\ Q(x,y) \leftrightarrow \neg \forall x \leq y\ \neg Q(x)$.

(Soluzione) EX: $P(x) \leftrightarrow x$ è primo è prim. ric.

$P(x) \leftrightarrow \forall y \leq x\ \forall z \leq x\ y \cdot z = x \to y=1 \vee z=1$ la soluzione segue da quanto fatto finora.

corollario (di discorsi fatti finora) tutti gli insiemi definibili in $(\mathbb{N}, +, \cdot)$ usando $=$, $\wedge$, $\vee$, $\to$ $\forall x \leq y$, $\exists x \leq y$ (insiemi Δ_0 limitati) sono prim. ric.
(si vedrà che vale $\Delta_0 \subset PR \subset$ definibili)

"def" ~~ricorsive~~ {funzioni μ-ricorsive} $\supset$ {f. prim. ric}

$f(\vec{y}) = \mu(x)\ P(x, \vec{y})$ $\begin{cases} \min x \text{ t.c. } P(x,y) & \text{se esiste} \\ \uparrow \text{ (indefinita)} & \text{altrimenti} \end{cases}$

le funzioni μ calcolabili sono la più piccola classe contenente $z(x)$, $\sigma(x)$, $U_i^n(\vec{x})$ e chiusa per comp., ric. prim. e per μ (con le notazioni fin qui introdotte) / Occorre ridefinire composizione e ric. prim. in maniera che possano avere come variabili valori indefiniti. È conveniente esprimere:

ordine parziale

def $f(y) = \mu_x\, th(x,y)=0) = \begin{cases} z & \text{se } \forall u<z\ h(u,y)\downarrow \neq 0 \wedge h(z,y)\downarrow = 0 \\ \uparrow & \text{altrimenti} \end{cases}$

def $f: \mathbb{N}^k \rightharpoonup \mathbb{N}$ è una funzione parziale sse è un sottoinsieme di $\mathbb{N}^{k+1}$ t.c. $(\vec{x},y) \in f \wedge (x,\vec{z}) \in f \to y = z$

def (comp. di funz. parz.)

$(x,z) \in (f \circ g) \leftrightarrow \exists z\ (x,z) \in g \wedge (z,y) \in f$

~~$(f \circ g)(x) \neq y$~~ $f \circ g\,(x)$ def.$(\downarrow) \Rightarrow g$ def.$(\downarrow)$.

def (ricors. prim. per funz. parz.)

$f(x+1) = h(x, f(x))$

$f(n)\downarrow \leftrightarrow \forall i \leq n\ f(i)\downarrow$ e $h(i, f(i))\downarrow$

"th" μ-ric. = calcolabili con un algoritmo } tesi di Church

(si vedrà che $\Delta_0 \subset RP \subset RIC \subset$ definibili e che RIC coincide con decidibili)

14-11-2006

programma per $\mu y\ h(x,\vec{y})=0$

① input $\vec{x}$

② $z = 0$

③ $u = h(\vec{x}, z)$

④ se $u = 0$ output z

⑤ se $u \neq 0$ $z = z+1$ e si ricomincia da ③.

una macchina a registri è "una lista di comandi del tipo:

$x = 0$; $x = x+1$; $x = y$; se $x = y$ vai al punto

oss μ-ric. e comp non fanno uscire fuori dalle funzioni calcolabili con macchina a registri e facilmente si dimostra che le funzioni μ-ricorsive sono calcolabili con mac. a reg. L'altra inclusione è difficile.

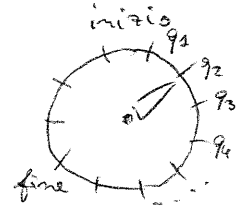
(idea)

μ-ricorsione $\overset{\text{theorema}}{=}$ calcolabili a registri

~~tesi~~ ‖ ‖ theorema

Algoritmicamente calcolabili $\overset{\text{tesi}}{=}$ Turing calcolabili

Turing



"Hardware"

software

stato	simbolo	stato	simbolo	spost.

$\delta: \{\text{stati}\} \times \{\text{simboli}\} \longrightarrow \{\text{stati}\} \times \{\text{simboli}\} \times \{D, S\}$

EX addizione tra naturali per macchine di T.

NOTA la macchina di Turing è non programmabile

th esiste una macchina di Turing universale U (i.e. $\forall M \in MT$ $U(e, x) = M(x)$ $e = \ulcorner M \urcorner$)

def $A \subset \mathbb{N}^k$ è decidibile (o ricorsivo) se la funzione caratteristica $\chi_A: \mathbb{N}^k \to \{0,1\}$ è calcolabile.

$A \subset \mathbb{R}^k$ è semidecidibile se $A = \{x \mid \exists y\ R(\vec{x}, y)\}$
con $R \subset \mathbb{N}^{k+1}$ decidibile $(A$ è $\Sigma^0_1)$

codifiche di D

$\alpha: D \to \mathbb{N}$ biunivoca

(o 1-1 con immagine decidibile)

$f: D \to D$ è calcolabile rispetto ad α se
$\tilde{f}$ ~~sched~~ ~~che~~ $\mathbb{N}$ ~~che f computatore~~

$$\text{t.e.}\quad \begin{array}{ccc} D & \xrightarrow{f} & D \\ \alpha\downarrow & & \downarrow\alpha \\ \mathbb{N} & \xrightarrow[\tilde{f}]{} & \mathbb{N} \end{array}$$

è calcolabile.

codifiche varie ...

th (Post)

$A \subset \mathbb{N}$ è decidibile sse A ed $\mathbb{N} \setminus A$ sono semidecidibili

(dim) $\Rightarrow$ ovvie

$\Leftarrow$ se A e $A^c = \mathbb{N} \setminus A$ sono decidibili allora

$A = \{y \mid \exists x\ P(x,y)\}$ $A^c = \{y \mid \exists x\ Q(x,y)\}$ con
P e Q decidibili. (sia $f(y) = \mu x\, [P(x,y) \vee Q(x,y)]$
$x \in A \leftrightarrow P(x, f(x))$ ruol di x e y invert.)

th A semidecidibile $\Leftrightarrow$ $\exists f$ calcolabile t.c. $A = dom(f)$

(dim) $A = \{x \mid \exists y\ R(x,y)\}$ $f(x) = \mu y\ R(x,y)$

(Matiasevic 1970 ?) $\sim$

ESEMPIO $\{\varphi \mid PA \vdash \varphi\}$ è semidecidibile, ma non dec.
$\{\varphi \mid \mathbb{N} \vdash \varphi\}$ non è neanche semidecidibile

$\{(w_1, w_2) \mid G \models w_1 = w_2\}$, dove w_1 e w_2 sono parole della th dei gruppi, è semidec. ma non dec.

prop gli insiemi decidibili sono stabili per:
$\wedge$, $\vee$, $\neg$, $\forall x \le y$, $\exists x \le y$.
gli insiemi semidecidibili sono stabili per:
$\wedge$, $\vee$, $\forall x \le y$, $\exists x$.

riassunto: $\Delta \subset$ prim. ric. $\subset$ decid. $\subset$ semidecid.
(NOTA: tali diseguaglianze sono tutte strette)

(EX $f(0) = 1$ $f(n) = h(f(\left[\frac{x}{2}\right]))$ h primitiva ricorsiva
① f è μ-ricorsiva ② f è prim. ric.)

def $\langle (a_i)_{0 \le i \le n} \rangle = \prod_{i=0}^{n} p_i^{a_i+1}$

EX esiste estrai: $(\langle (a_i)_{0\le i\le n}\rangle, i) \mapsto a_i$ (se $i \le n$)
esiste cat: $(\langle (a_i)_{0\le i\le n}\rangle, i) \mapsto \langle (a_i)_{0\le i\le n}\, (b_i)_{0\le i\le m} \rangle$
esiste lungh.: $(\langle (a_i)_{0\le i\le n}\rangle) \mapsto n+1$
~~$\leftarrow$ tesi~~ (primitive ricorsive)
Im $(\langle\cdot\rangle)$ è primitiva ricorsiva.
$i \mapsto p_i$ è primitiva ricorsiva.

$g(t) = \mu y < t\ f(y) = \begin{cases} \min(y)\ f(y) & \text{se } y < t \\ t & \text{altrimenti} \end{cases}$ è prim. ric.

$g(0) = 0$ $g(t+1) = \begin{cases} g(t) & \text{se } g(t) < t \\ t+1 & \text{se } g(t) \dots \end{cases}$

th (di ricorsione sul decorso dei valori)
sia $h: \mathbb{N}^2 \to \mathbb{N}$ prim. ricorsiva allora
$f(n) = h(n, \langle (f(i))_{0 \le i < n} \rangle)$ è prim. ric.

$f^\#(0) = \langle f_0 \rangle$

$f^\#(x+1) = cat(\langle (f_i)_{0\le i\le x}\rangle, \langle f_{x+1}\rangle) = cat(f^\#(x), \langle h(x, f^\#(x))\rangle)$

Ora $f(x) = estrai(x, f^\#(x))$ è prim. ric.

Gödel $L = \{0, \sigma, +, \cdot\}$

codifica termini

$$\begin{cases} + \longmapsto \#(+) \\ \cdot \longmapsto \#(\cdot) \\ \sigma \longmapsto \#(\sigma) \\ 0 \longmapsto \#(0) \\ v \longmapsto \#(v) \end{cases}$$

$\ulcorner v_i \urcorner = \langle \# v, i \rangle$

$\ulcorner t_1 + t_2 \urcorner = \langle \#(+), \ulcorner t_1 \urcorner, \ulcorner t_2 \urcorner \rangle$

$\ulcorner t_1 t_2 \urcorner = \langle \#(\cdot), \ulcorner t_1 \urcorner, \ulcorner t_2 \urcorner \rangle$

$\ulcorner \sigma(t) \urcorner = \langle \#(\sigma), \ulcorner t \urcorner \rangle$

$\ulcorner 0 \urcorner = \langle \# 0 \rangle.$

ESEMPIO $\ulcorner (0+0)+0 \urcorner = \langle \#(+), \langle \#(+), \#(0), \#(0)\rangle, \#(0)\rangle = 2^{\#(+)} 3^{2^{\#(+)} \cdot 3^{\#(0)} \cdot 5^{\#(0)}} 5^{\#(0)}$

(tale codifica è detta codifica ad albero, un'altra possibilità è la codifica a stringa.

th $\{\ulcorner t \urcorner \mid t \text{ termine}\}$ è prim. ricorsivo.

sia chiamo Ter l'insieme sopra definito.

$n \in Ter \leftrightarrow (n = \ulcorner 0 \urcorner) \vee (\exists k\ \ n = \langle \#(\sigma), k \rangle \wedge k \in Ter) \vee$
$\vee (\exists k_1 k_2\ \ n = \langle \#(+), k_1, k_2 \rangle \wedge k_1, k_2 \in Ter)$
$\vee (\exists k_1 k_2\ \ n = \langle \#(\cdot), \ldots \rangle)$
$\vee (\exists i\ \ n = \langle \#(v), i \rangle.)$

$1_{Ter}(n) \leftrightarrow H(n, \langle 1_{Ter}(0), \ldots, 1_{Ter}(n-1) \rangle$

$H(n, \sigma) \overset{=1}{\leftrightarrow} (n = \ulcorner 0 \urcorner) \vee (\exists k < n\ \ n = \langle \#(\sigma), k \rangle \wedge \text{Estrai}(k, s) = 1)$

$\vee \ldots$

$\ulcorner\ \urcorner$: formule $\to \mathbb{N}$ $\quad \ulcorner t_1 = t_2 \urcorner \mapsto \langle \#(=), \ulcorner t_1 \urcorner, \ulcorner t_2 \urcorner \rangle$

$\ulcorner \forall v_i\, \varphi \urcorner = \langle \#(\forall), i, \ulcorner \varphi \urcorner \rangle$

analogamente a quanto visto in precedenza $\{\ulcorner \varphi \urcorner \mid \varphi \text{ formula}\}$ è prim. ric.

se $\varphi, i, t \longmapsto \varphi(t/v_i)$ allora $sub: (\ulcorner \varphi \urcorner, i, \ulcorner t \urcorner) \longmapsto \ulcorner \varphi(t/v_i) \urcorner$

altrimenti è una costante arbitraria (per es. se vale 0 sub è prim. ric.). inoltre

$sub: (\ulcorner t_1 \urcorner, i, \ulcorner t_2 \urcorner) \mapsto \ulcorner t_1(t_2/v_i) \urcorner$

def
TERMINI
$v_i(t/v_i) = t \qquad v_j(t/v_i) = v_j \quad i \neq j.$
$t_1 + t_2(t/v_i) = t_1(t/v_i) + t_2(t/v_i)$
$t_1 t_2 (t/v_i) = \ldots$
$\sigma(t_1)(t/v_i) = \sigma(t_1(t/v_i))$

FORMULE
$(t_1 = t_2)(t/v_i) = (t_1(t/v_i) = t_2(t/v_i))$
$(\varphi \vee \psi)(t/v_i) \ldots \psi(t/v_i)$
$\neg\varphi(t/v_i) \ldots$
$(\forall v_i\, \varphi)(t/v_i) = \forall v_i\, \varphi$
$(\forall v_i \varphi)(t/v_j) = \forall v_i (\varphi(t/v_j))$

$sub: \mathbb{N}^3 \to \mathbb{N}$ definita per casi ed induzione (pg 24 dispense)

$sub: (\ulcorner \neg\varphi \urcorner, i, n) \mapsto \langle \#(\neg), sub(\ulcorner \varphi \urcorner, i, n) \rangle$

$sub: (\ulcorner \forall v_i\, \varphi \urcorner, i, n) \longmapsto \ulcorner \forall v_i\, \varphi \urcorner$

$sub: (\ulcorner \forall v_i\, \varphi \urcorner, j, n) \longmapsto \langle \#(\forall), i, sub(\ulcorner \varphi \urcorner, j, n) \rangle$

$sub: (\ulcorner t_1 = t_2 \urcorner, i, t) \longmapsto \langle \#(=), sub(\ulcorner t_1 \urcorner, i, \ulcorner t \urcorner), sub(\ldots) \rangle$

...

(dove $sub(k, i, n) = H(k, i, n, \langle sub(0, i, n) \ldots sub(k-1, i, n) \ldots$ vedere cos'è H!).

th oss $\{\ulcorner \varphi \urcorner \mid \varphi \in PA\}$ è prim. ricors. $\subsetneq$ funzioni μ-ricors. totali $\subsetneq$ funzioni μ-ricors. parz. = calcolabili

$A: (x,y) \longmapsto A(x-1, A(x, y-1))$ se $x>0 \wedge y>0$
$(x, y) \longmapsto A(x-1, 1)$ se $x>0$
$(0, y) \longmapsto y+1$ altrimenti

è μ-ricors. totale ma non prim. ric.

EX $A(2,2) = \dots$

$m \in Ax_{PA} \iff (m \in Ax_Q) \vee (m \in Ax_{indu z.})$

$m \in Ax_{Induz.} \iff m = \ulcorner \forall \vec{y} \{(\varphi(0,\vec{y}) \wedge \forall x\, \varphi(x,\vec{y}) \to \varphi(\sigma(x),\vec{y})) \to \forall z\, \varphi(z,\vec{y})\}\urcorner$

che nel caso senza $\forall \vec{y}$ si semplifica:

$m \in Ax_{Ind.} \iff \exists k\, (k \in \text{Formula} \wedge m = \langle \#(\to), \langle \#(\wedge), sub(k, 0, \ulcorner 0 \urcorner), \langle \#\forall, 0, \langle \#(\to), k, sub(k, 0, \langle \#\sigma, 0\rangle)\rangle\rangle\rangle, \langle \#\forall, 0, k\rangle\rangle)$

$\{(\ulcorner d \urcorner, \ulcorner \varphi \urcorner) \mid \ulcorner d \urcorner$ codifica una dimostrazione d di φ in PA$\}$ è prim. ric.

$PA \vdash^{d} \varphi$ se $\exists T \subset_{finito} PA$ $T \vdash^{d} \varphi$

$prov_{PA} = \{(x,y) \in \mathbb{N}^2 \mid x$ cod. una dim di y in PA$\}$ è prim. ric.

$teo_{PA} = \{y \mid y$ codif. un th di PA$\} = \{y \mid \exists x\, (x,y) \in prov_{PA}\}$ è semidecidibile.

riassunto: $L = \{0, \sigma, +, \cdot\}$

$\mathbb{N} \supset \{\ulcorner \varphi \urcorner \mid \varphi$ L-formula$\}$ $\mathbb{N} \supset \{\ulcorner t \urcorner \mid t$ L-termine$\}$

$\mathbb{N} \supset \{\ulcorner \varphi \urcorner \mid$ assioma di PA$\}$ (primitivi ricorsivi)

$\mathbb{N}^2 \supset \{(\ulcorner d \urcorner, \ulcorner \varphi \urcorner) \mid PA \vdash^{d} \varphi\}$ è prim. ricors.

def $P \subset \mathbb{N}^k$ è binumerabile in T ~~una~~ (L-teoria) se esiste $\varphi(x_1, \dots x_k)$ L-formula e

① $(a_1, \dots a_k) \in P \Rightarrow T \vdash \varphi(\sigma^{a_1}(0) \dots \sigma^{a_k}(0)) = \varphi(\underline{a_1}, \dots \underline{a_k})$

② $(a_1, \dots a_k) \notin P \Rightarrow T \vdash \neg\varphi(\underline{a_1}, \dots \underline{a_k})$

$\mathbb{N}^{k+1}$

def una funzione è binumerabile se il suo grafico lo è.

def $P \subset \mathbb{N}$ è numerabile (nelle stesse notaz. prec.) sse

$(a_1, \dots a_k) \in P \iff T \vdash \varphi(\underline{a_1} \dots \underline{a_k})$

OSS se $\mathbb{N} \models T$ φ definisce P in $\mathbb{N}$ $P = \{(a_1, \dots a_k) \mid \mathbb{N} \models \varphi(a_1, \dots a_k)\}$.

OSS se $T = Th(\mathbb{N})$ definibile in $\mathbb{N}$ = binumerabile in T

se $T \neq Th(\mathbb{N})$ definibile in $\mathbb{N} \not\Rightarrow$ binumerabile in T

OSS P binumerabile in PA $\Rightarrow$ P decidibile (ma ci sono insiemi definibili in $\mathbb{N}$ non decidibili).

(vale anche P decidibile $\Rightarrow$ P binumerabile)

def $f: \mathbb{N}^k$ —

NOTA sia Q che PA binumerano tutti gli insiemi primitivi ricorsivi (decidibili) però PA lo fa meglio

ESEMPIO: $n!$ $G = \{(a,b) \mid b = a!\} \subset \mathbb{N}^2$

esiste $\varphi(x,y)$ L-formula che binumera G in Q.

$b = a! \Rightarrow Q \vdash \varphi(\underline{a}, \underline{b})$

$b \neq a! \Rightarrow Q \vdash \neg\varphi(\underline{a}, \underline{b})$

in più PA dimostra:

$PA \vdash \forall x\ \ (x+1)! = (x+1)\, x!$

$PA \vdash \forall x, y\ \ \varphi(x,y) \to \varphi(x+1, y \cdot (x+1))$

In Q:

- la somma è binumerabile da $(x+y=z)$

infatti in ZF per induzione su b si dimostra

$a+b=c \Rightarrow Q \vdash \underline{a} + \underline{b} = \underline{c}$

~~$a+b \neq c \Rightarrow Q \vdash \neg(\underline{a}+\underline{b} = \underline{c})$~~

$b = 0 \dots$

$b = k+1$ $(a+k \overset{\text{ip. ind}}{=} c-1) \Rightarrow a + (k+1) = c$ e

$Q \vdash \sigma(\underline{a} + \underline{k}) = \sigma(\underline{c-1}) = \underline{c}$

il prodotto è ~~d~~ianumerabile ...

$a \cdot b = c \Rightarrow Q \vdash \underline{a} \cdot \underline{b} = \underline{c}$

per induzione su b ...

<u>corollario</u> se t è un L-termine chiuso allora esiste

$n \in \mathbb{N}$ t.c. $Q \vdash t = \underline{n}$

(dim) ~~per induz~~ se $t = t_1 + t_2$ per induzione $Q \vdash t_1 = \underline{n_1} \wedge t_2 = \underline{n_2}$ e dunque $Q \vdash t_1 + t_2 = \underline{n_1} + \underline{n_2} = \underline{n_1 + n_2}$

analogam. se $t = t_1 t_2$, $t = 0$ e $t = \sigma(t_1)$.

~~somma~~ <u>lemma</u> $a \neq b \Rightarrow Q \vdash \underline{a} \neq \underline{b}$

(dim) wlog $a < b$ per induzione su a

$a = 0 \Rightarrow Q \vdash \forall x\ (0 \neq \sigma(x))$

$0 < a < b \Rightarrow a-1 < b-1 \overset{\text{ip. ind.}}{\Rightarrow} Q \vdash \underline{a-1} \neq \underline{b-1} \rightarrow$

$\rightarrow Q \vdash \overset{a=}{\sigma(\underline{a-1})} \neq \sigma(\underline{b-1}) = \underline{b}$.

<u>lemma</u> t_1, t_2 termini chiusi. $Q \vdash t_1 = t_2$ o $Q \vdash t_1 \neq t_2$.

(dim) $Q \vdash t_1 = \underline{a_1}$ $Q \vdash t_2 = \underline{a_2}$ e la tesi segue dal lemma prec.

def $x \leq y \leftrightarrow \exists z\ (z + x = y)$

ES $\forall n \in \mathbb{N}$, $Q \vdash \forall x\ (x \leq \underline{n} \leftrightarrow x = \underline{0} \vee x = \underline{1} \vee \dots \vee x = \underline{n})$

per ind su n.

$n = 0$ in Q $x \leq \underline{0}$ se $\exists z$ $z + x = 0$

se $x \neq \underline{0}$ $\overset{\exists y}{\vee}$ $x = \sigma(y)$ $z + x = z + \sigma(y) = \sigma(z+y) \neq 0$ assurdo.

$n > 0$ in Q $x \leq \underline{n}$ $z + x = \underline{n}$ se $x = \underline{0}$ ok

se $x \neq \underline{0}$ $n = z + x = z + \sigma(y) = \sigma(z+y) \rightarrow \underline{n-1} = z + y \rightarrow$

$y \leq \underline{n-1} \rightarrow y = 0 \dots y = n-1 \rightarrow y = 1 \dots y = n$.

(i numeri standard sono isomorfi a $\mathbb{N}$)

sia $M \models Q$ se $x \in M$ $x \leq \underline{n} \rightarrow x$ standard.

per cui M: 0 $\sigma(0)$ $\sigma^{(2)}(0) \dots$ altro

<u>EX</u> trovare $L = \{0, \sigma, \dots\}$ e una L-teoria T t.c.

$\forall n \in \mathbb{N}$ $T \vdash \varphi(\underline{n})$ ma $T \nvdash \forall x\ \varphi(x)$

φ = "x è pari o dispari" in Q

sol. più semplice: $L = \{0, \sigma, P\}$ P predicato unario

$T: \{P(0), P(1) \dots\}$ (o più sofisticato $T = \{P(0), \forall x\ [P(x) \rightarrow P(\sigma(x))]$)

th $\overset{\forall k \in \mathbb{N}}{\forall n \leq k}$ $Q \vdash \varphi(\underline{n}) \longleftrightarrow Q \vdash \forall x \leq \underline{k}\ \varphi(x)$.

$Q \vdash \forall x \leq \underline{k}\ \varphi(x) \leftrightarrow Q \vdash \forall x\ (x = \underline{0} \vee \dots\ x = \underline{k}) \rightarrow \varphi(x) \leftrightarrow Q \vdash \varphi(\underline{0}) \wedge \varphi(\underline{1}) \dots \varphi(\underline{k}) \leftrightarrow Q \vdash \varphi(\underline{0}), \dots \varphi(\underline{k})$ ...

riassunto:

th $n \in \mathbb{N}$ $Q \vdash \forall x\ (x \leq \underline{n} \leftrightarrow x = \underline{0} \vee \dots \vee x = \underline{n})$

th $n \in \mathbb{N}$ tfae:

1. $\forall a \leq n$ $Q \vdash \varphi(\underline{a})$
2. $Q \vdash \forall x \leq \underline{n}\ \varphi(x)$
3. $Q \vdash \varphi(\underline{0}) \wedge \varphi(\underline{1}) \wedge \dots \varphi(\underline{n})$

$Q \nvdash$ ($\leq$ è un ordine), ma

th $a, b \in \mathbb{N}$ $(Q \vdash \underline{a} \leq \underline{b})$ o $(Q \vdash \neg(\underline{a} \leq \underline{b}))$

(dim) $a \leq b$ $Q \vdash (\underline{a} = \underline{a} \rightarrow)\ \underline{a} = \underline{0} \vee \dots\ \underline{a} = \underline{b}$

$Q \vdash \underline{a} \leq \underline{b}$

$a > b$ $Q \vdash \forall x\ (x = \underline{0} \vee x = \underline{1} \vee \dots \vee x = \underline{b}) \rightarrow x \neq \underline{a}$

$m \neq n$ $Q \vdash \underline{m} \neq \underline{n}$

$Q \vdash \forall x\ (x = 0 \rightarrow x \neq \underline{a},\ x = \underline{1} \rightarrow x \neq \underline{a} \dots$

$x = \underline{b} \rightarrow x \neq \underline{a})$

$Q \vdash \neg(\underline{a} \leq \underline{b})$

(INDOVINELLO: $\int_a^z (a-x)(b-x) \dots (z-x)\, dx = 0$.)

th $b \in \mathbb{N}$ $Q \vdash \forall x\, (x \leq \underline{b} \vee \underline{b} \leq x)$

(dim) per ind. su b

$b = 0$ $\quad Q \vdash \underline{0} \leq x \quad (x + \underline{0} = x)$

$b > 0$ in Q per ip. ind. $x \leq \underline{b-1}$ o $\underline{b-1} \leq x$

nel primo caso $x \leq \underline{b}$

nel secondo $\exists z \;\; z + \underline{b-1} = x$ ora

se $z = \underline{0}$ $\quad x = \underline{b-1} \leq \underline{b}$.

se $z \neq \underline{0}$ $\quad \exists y \; z = \sigma(y)$?

$Q^* = Q + \{\forall x (x \leq \underline{b} \vee \cancel{\underline{b} \leq x} \mid b\}$ $\forall xy (x \leq y \vee y \leq x)$

Lemma $M \models Q$ $\quad A \subset M$ se A contiene uno standard

allora A ha un minimo m

$\forall a \in A \quad M \models m \leq a$.

$A' = \{x \in M \mid M \models x \leq k'\} \subset \mathbb{N} \subset M$

il minimo di A' è il minimo di A.

$\Delta_0 = \quad t_1 = t_2 \mid \Delta_0 \wedge \Delta_0 \mid \Delta_0 \vee \Delta_0 \mid \neg \Delta_0 \mid \forall x \leq t\, \Delta_0$

formule con quantif. limitati

def φ chiusa. φ è decisa da Q se $Q \vdash \varphi$ o $Q \vdash \neg\varphi$.

th tutte le Δ_0 sono decise in Q

(dim) se Q decide sia φ che ψ allora Q decide

$\varphi \wedge \psi \quad \varphi \wedge \psi \quad \neg\varphi$ (si vede per casi)

Q decide $\varphi(\underline{0}), \varphi(\underline{1}), \dots \varphi(\underline{n}) \Rightarrow$

Q decide $\forall x \leq \underline{n}\; \varphi(x)$ infatti

$\forall x \leq \underline{n}\; \varphi(x) \overset{Q}{\Longleftrightarrow} \varphi(\underline{0}) \wedge \dots \wedge \varphi(\underline{n})$

$\varphi \in \Delta_0$ chiusa $\quad \mathbb{N} \models \varphi \Leftrightarrow Q \vdash \varphi$

$\mathbb{N} \not\models \varphi \Leftrightarrow Q \vdash \neg\varphi$

EX $Q \vdash \forall xy \leq 10^{10}\; (x + y = y + x)$

def $A, B \models Q^-$ $\quad (Q^- = Q + (\leq$ è un ord tot$)$ ...

$A \subseteq_e B \Leftrightarrow (\overset{\forall a,b}{a \in A \wedge b \in B \setminus A \rightarrow a \leq_B b})$ (e = "end extension") (e a A sottostr. di B)

EX $A \subseteq_e B$ $\quad \varphi(x_1, \dots x_n) \in \Delta_0 \quad a_1, \dots a_n \in A$

$A \models \varphi(a_1, \dots a_n) \Leftrightarrow B \models \varphi(a_1, \dots a_n)$

EX trovare 3 ord. lin. $A \subseteq_e B \subseteq_e C$ e φ t.c.

$\varphi \restriction A \quad \neg\varphi \restriction B \quad \varphi \restriction C$. $\quad ([0,1] < [0,2) < [0,2])$

OSS $\forall B \models Q \quad \mathbb{N} \subseteq_e B$ (per cui $\mathbb{N} \models \varphi \Rightarrow Q \vdash \varphi$

e $\mathbb{N} \models \neg\varphi \Rightarrow Q \vdash \neg\varphi$)

$\exists \vec{x}\, \Delta_0$ (talvolta dette $\Sigma^0_1(Q)$).

th $\mathbb{N} \models \exists x\, \varphi(x) \quad \varphi \in \Delta_0 \Rightarrow Q \vdash \exists x\, \varphi(x)$

(dim) $\mathbb{N} \models \exists x\, \varphi(x) \Rightarrow \exists a \in \mathbb{N} \models \varphi(\underline{a}) \Rightarrow \exists a \in \mathbb{N}\; Q \vdash \varphi(\underline{a})$

$\Rightarrow Q \vdash \exists x\, \varphi(x)$.

SEMPIO la cong. di Goldbach

$\forall n\, \exists p, q$ primi $p + q = 2n$ è del tipo $\forall \Delta_0$

Ora se PA $\nvdash$ cong. G. $\overset{\text{metateoria}}{\Rightarrow}$ $\mathbb{N} \models$ G. cong.

PA $\nvdash$ $\neg$ cong. G.

infatti $\mathbb{N} \not\models$ cong. G. $\Rightarrow$ $\quad Q \vdash \dots$

la minima classe di prop. non dim. in PA è $\forall \Delta_0$.

dimostrazione avanzata delle scorse volte:

$b \in \mathbb{N} \quad Q \vdash \forall x\, (x \leq \underline{b} \vee \underline{b} \leq x)$

per induzione su b

$b = 0$ ...

$\sigma(y) + \underline{b-1} = x$

$\sigma^{b-1}(\sigma(y) + 0) = \sigma^b(y) = \sigma^b(y) = \sigma^b(y + 0) = y + \sigma^b(0) = y + \underline{b}$

corollario se un enunciato $\psi \in \forall \Delta_0$ è indip. da ...

th ($\exists\Delta_0 = \exists$ prim. ric.$^{(*)}$) $A \subset \mathbb{N}$ si può definire nella forma $\exists\Delta_0 \iff$ si può def. nella forma $\exists PR$.

($^{(*)}$ ma $\Delta_0 \neq PR$)

dim) è suff. per vedere che $PR \subset \exists\Delta_0 \Rightarrow \exists PR \subset \exists\exists\Delta_0 = \exists\Delta_0$

def $f: \mathbb{N}^k \to \mathbb{N}$ è binumerabile in Q se esiste $\varphi(x_1, \dots x_k, x_{k+1})$ $\forall (a_1, \dots a_k) \in \mathbb{N}$ se $f(a_1, \dots a_k) = b \Rightarrow$

$Q \vdash \varphi(\underline{a_1}, \dots \underline{a_k}, \underline{b})$ se — $\neq b \Rightarrow Q \vdash \neg\varphi(- -)$

si dice binumerabile funzionalmente se

$f(a_1 \dots a_k) = b \Rightarrow Q \vdash \exists!_y\ \varphi(a_1, \dots a_k) = b$.

OSS se $f: \mathbb{N} \to \mathbb{N}$, $g: \mathbb{N} \to \mathbb{N}$ sono binumerabili funzionalmente anche $f \circ g$ lo è.

$(f \circ g)(x) = y \iff \exists z [g(x) = z \wedge f(z) = y]$ $\quad [\varphi_g(x,z) \wedge \varphi_f(y,z)]$

$x = n \in \mathbb{N}$

$Q \vdash \exists! z\ \varphi_g(n, z)$ $\qquad Q \vdash \varphi_g(\underline{n}, \underline{k})$ $\qquad (k = g(n))$

$\left.\begin{array}{l} Q \vdash \forall y\ \ \varphi_g(n, y) \iff y = k \\ Q \vdash \forall z\ \ \varphi_f(k, z) \iff z = l \end{array}\right\} \Rightarrow Q \vdash \forall w\ \theta(\underline{n}, w) \iff w = \underline{l}$

la formula Σ_1^0

th le funzioni binumerabili funzionalmente in Q sono chiuse per ricorsione primitiva.

Corollario Prim. Ric. $\subset$ binumerabili in Q.

(**def** Σ_1^0 è il più piccolo insieme t.c. $\Delta_0 \subset \Sigma_1^0$ e stabile per $\wedge, \vee, \forall x < t, \exists x$

(predicati $\Sigma_1^0 = \exists PR$)

def (beta di Goedel) $\beta(c, d, i) = \text{resto}\ (c, (i+1)d + 1)$ ($\in \Delta_0^{\mathbb{N}}$)

($\beta \in \Delta_0^{\mathbb{N}}$ infatti $(\exists q \leq x\ \ yq + z = x \wedge z < y)$ è Δ_0 e ...)

già visto: $\forall n\ \forall b_0, \dots b_n \in \mathbb{N}\ \exists c, d\ \ \beta(c, d, i) = b_i \quad 0 \leq i \leq n$.

β è definibile in $\mathbb{N}$ (ovvio) e binumerabile funz. in Q dalla formula $\beta(c, d, i) = z \iff \exists q \leq c\ (c = q((i+1)d + 1) + z$ $\wedge\ 0 \leq z < (i+1)d + 1]$ che è Δ_0. Inoltre z è unico perché è standard in quanto minore di $(i+1)d + 1$ con d standard.

(dim th) $f(\vec{x}, 0) = g(\vec{x})$ $\qquad f(\vec{x}, y+1) = h(\vec{x}, y, f(\vec{x}, y))$

con g, h binumerate funzionalmente da φ_g, φ_h $\in \Sigma_1^0$. ~~la formula φ_f è~~ Ora fissati $\vec{x}, y \in \mathbb{N}$

$f(\vec{x}, y) = z \iff \exists (a_i \mid i \leq y)$ $a_0 = g(\vec{x})$ e $\forall i \leq y$

$a_{i+1} = h(\vec{x}, i, a_i)$ $\qquad a_y = z$. $\qquad f(\vec{x}, y) = z \iff \exists c, d$

$\beta(c, d, 0) = g(\vec{x}) \wedge \forall i \leq y\ \ \beta(c, d, i+1) = h(\vec{x}, i, \beta(c, d, i))$

$\beta(c, d, y) = z$.

dettagli: piuttosto che scrivere $\beta(c, d, i+1) = h(\vec{x}, i, \beta(\dots$

è meglio scrivere $\exists u, v\ \ u = \beta(c, d, i+1)$

$v = \beta(c, d, i)$ $\quad \varphi_h(x, i, v, u)$ e da questo si vede che la formula non $\exists\Delta_0$ bensì Σ_1^0.

$\varphi_f(\vec{x}, y, z)$ binumera funzionalmente f in Q. Siano

$\vec{a}, b \in \mathbb{N}$ $\qquad Q \vdash \exists! z\ \varphi(\underline{a}, \underline{b}, z)$.

(cenno di unicità in Q: presi $\underline{a}$ e $\underline{b}$ c ed d potrebbero non essere unici, ma $\beta(c, d, 0) \dots \beta(c, d, i)$ lo sono.

OSS f prim. ric. ~~posson~~ può essere definita in modi diversi e dunque avere diverse formule Σ_1^0 associate. Non è chiaro se Q (e forse lo stesso PA) ~~siano~~ in grado di dimostrarne l'eq.

ESEMPIO $\begin{cases} 2^0 = 1 \\ 2^{x+1} = 2^x 2 \end{cases}$ $\qquad \begin{cases} 2^0 = 1 \\ 2^{2x} = (2^x)^2 \\ 2^{2x+1} = (2^x)^2 \cdot 2 \end{cases}$ $\qquad$ PA dimostra l'eq. delle due def. Q no.

anticipazione:

th f.o. $\varphi(x)$ esiste γ t.c. $Q \vdash \gamma \iff \varphi(\ulcorner\gamma\urcorner)$

(dal quale segue $\mathbb{N} \models \gamma \iff \varphi(\ulcorner\gamma\urcorner)$

th (lemma di diagonalizzazione)

$L = \{0, \sigma, +, \cdot\}$. sia $\alpha(x)$ una L-formula. esiste un L-enunciato β t.c.

$Q \vdash \beta \leftrightarrow \alpha(\underline{\ulcorner\beta\urcorner})$

($\ulcorner\beta\urcorner$ è il numero di Gödel di β. $\underline{\ulcorner\beta\urcorner}$ è il termine associato a tale numero)

(dim) idea: sia $f_n^{(x)}$ la formula ~~chiusa~~ con numero di Gödel n (in realtà la codifica non è suriettiva). si cerca ~~cerca~~ β della forma $f_n(\underline{n})$, ~~infine~~ cioè si cerca ~~A~~ un n t.c. $Q \vdash f_n(\underline{n}) \leftrightarrow \alpha(\underline{\ulcorner f_n(\underline{n})\urcorner})$. l'idea è di scegliere n in maniera tale che

$n = \ulcorner \alpha(f_n(\underline{n}))\urcorner$. ~~infatt~~

(si è già dimostrato che $sub : \mathbb{N}^3 \to \mathbb{N}$ è prim. ric.

$sub : (\ulcorner\varphi\urcorner, i, \ulcorner t\urcorner) \longmapsto \ulcorner\varphi(t/v_i)\urcorner$.

sia $sub_0 : (\ulcorner\varphi\urcorner, \ulcorner t\urcorner) \longmapsto \ulcorner\varphi(t/v_0)\urcorner = \ulcorner\varphi(t/x)\urcorner$ e

sia $NUM : \mathbb{N} \to \mathbb{N}$ $\quad NUM : n \mapsto \ulcorner\sigma^n(0)\urcorner$.

NUM è prim. ric. (infatti $\ulcorner\sigma^{n+1}(0)\urcorner = \langle \#(\sigma), \ulcorner\sigma^n(0)\urcorner\rangle$ e quindi $NUM(n+1) = \langle\#(\sigma), NUM(n)\rangle$)

$D : \mathbb{N} \to \mathbb{N}$ $\quad D(n) = sub_0(n, NUM(n))$ è PRIM. ric. poiché composizione di prim. ric.

"def" $f(x) = \alpha(D(x)) = \alpha(sub(x, NUM(x)))$

Ora $\alpha(D(x)) \leftrightarrow \forall y\,(y = D(x) \to \alpha(y)) \leftrightarrow \forall y\,(\delta(x,y) \to \alpha(y))$

dove δ binumera ~~f~~ funzionalmente D. per cui

def $f(x) = \forall y\,(\delta(x,y) \to \alpha(y))$.

scelto $\beta = f(\underline{\ulcorner f\urcorner})$ esso soddisfa la tesi.

(VERIFICA) $f(\underline{\ulcorner f\urcorner}) = \forall y\,(\delta(\underline{\ulcorner f\urcorner}, y) \to \alpha(y))$ ①

$Q \vdash \delta(\underline{\ulcorner f\urcorner}, y) \leftrightarrow y = \underline{b}$ ②

[illegible]

$= \ulcorner f(\underline{\ulcorner f\urcorner})\urcorner$) da ① e ② segue $Q \vdash \alpha(\underline{b}) \overset{\leftrightarrow \beta}{\scriptstyle e}$

quindi $Q \vdash \alpha(\underline{\ulcorner f(\underline{\ulcorner f\urcorner})\urcorner}) \leftrightarrow \beta$ e infine

$Q \vdash \beta \leftrightarrow \alpha(\underline{\ulcorner\beta\urcorner})$.

(i passaggi fatti sono riassunti da:

① si cerca un punto fisso x per un operatore A $(x = Ax)$

② si pone $ff = x$ per cui $A(ff) = ff$

③ si risolve rispetto a ~~d~~ ~~f~~ $fx = A(xx)$).

th PA è incompleta.

si usa: assiomi di PA sono un insieme ricorsivo (in realtà anche primitivo, ~~ma~~ basterebbe addirittura ricorsivamente numerabile), PA è coerente, PA è ω-coerente (usata da Gödel ed eliminata da ~~Rosser~~ Rosser nel 1936).

def $L = \{0, \sigma, +, \cdot\}$ $\quad T$ L-Teoria

($\mathbb{N} \models T \Rightarrow T$ è ω-coerente $\Rightarrow T$ è coerente)

T è ω-coerente se non esiste una formula $\varphi(x)$ t.c. $T \vdash \exists x\, \varphi(x)$ e $\forall n \in \mathbb{N}$ $T \vdash \neg\varphi(\underline{n})$.

(si dice se non è ω-incoerente).

th T coerente, ric. assiomatizz., ω-coer. $\overset{(T \supseteq Q)}{\Rightarrow}$ T incompl.

si è già visto $\varphi \in \Sigma_1^0$ $\mathbb{N} \models \varphi \Rightarrow Q \vdash \varphi \Rightarrow T \vdash \varphi$.

se T è ω-coerente $\overset{e\ T \supseteq Q}{}$ valgono anche le frecce opposte, cioè e oltre una teoria ω-coerente contenente Q dimostra cose false in $\mathbb{N}$ solo se esse sono di complessità maggiore di Σ_1^0. per semplicità si suppone $\exists\Delta_0$ piuttosto che Σ_1^0.

sia $\varphi = \exists x\, \theta(x)$ $\quad \theta \in \Delta_0$ se $T \vdash \exists x\, \theta x$ e $\mathbb{N} \not\models \exists x\, \theta(x)$ allora $\mathbb{N} \models \neg\theta(\underline{n})$ per cui

$Q \vdash \neg(\theta(\underline{n}))$ $\quad T \vdash \neg(\theta(\underline{n}))$ ...

[illegible]

(dim (1° Gödel)). esiste un ~~predicato~~ relazione (prim.) ricorsivo $\mathrm{Prov}_T \subset \mathbb{N}^2$ t.c. $(n, \ulcorner\varphi\urcorner) \in \mathrm{Prov}_T \leftrightarrow n$ codifica una dimostr. di φ in T. In particolare Prov_T è binumerabile da $P_T(x,y) \in \Sigma^0_1$ in Q.

$(n, \ulcorner\varphi\urcorner) \in \mathrm{Prov}_T \Rightarrow (T \vdash^n \varphi) \Rightarrow Q \vdash P_T(\underline{n}, \ulcorner\varphi\urcorner)$ e

$(n, \ulcorner\varphi\urcorner) \notin \mathrm{Prov}_T \Rightarrow Q \vdash \neg P_T(\underline{n}, \ulcorner\varphi\urcorner)$.

Abbiamo visto:

th $L = \{0, \sigma, +, \cdot\}$ se $\alpha(x)$ è una L-formula allora esiste un L-enunciato β t.c.

$Q \vdash \beta \leftrightarrow \alpha(\ulcorner\underline{\beta}\urcorner)$ (dove $\underline{n} = \sigma^n(0)$)

(fatto chiave dim) $(n, \ulcorner\varphi\urcorner) \longmapsto \ulcorner\varphi(\sigma^n(0)/x)\urcorner$ è prim. ric.

(in realtà è suff. che sia ric.).

th (1° di Gödel: caso PA) PA è incompleta.

(dim) $\{\ulcorner\varphi\urcorner \mid \varphi$ assioma di PA$\}$ è (primitivo) ricorsivo, pertanto è binumerabile da una Σ^0_1 $Ax_{PA}(x)$.

$(\varphi \in Ax(PA) \Rightarrow Q \vdash Ax_{PA}(\ulcorner\varphi\urcorner)$ e

$\varphi \notin Ax(PA) \Rightarrow Q \vdash \neg Ax_{PA}(\ulcorner\varphi\urcorner)$.

def $(PA \vdash^n \varphi) \Leftrightarrow n$ codifica una dimostrazione di φ in PA.

$\{(n, \ulcorner\varphi\urcorner) \mid PA \vdash^n \varphi\}$ è prim. ric., per cui è binumerabile in Q da una formula $\mathrm{Dim}_{PA}(x,y)$

$(PA \vdash^n \varphi \Rightarrow Q \vdash \mathrm{Dim}_{PA}(\underline{n}, \ulcorner\varphi\urcorner)$ e

$PA \nvdash^n \varphi \Rightarrow Q \vdash \neg \mathrm{Dim}_{PA}(\underline{n}, \ulcorner\varphi\urcorner)$.)

oss Dim_{PA} oltre che da PA dipende anche da Ax_{PA}

~~Per il th precedente esiste una formula~~

Sia $\mathrm{Teo}_{PA}(x) \overset{def}{\equiv} \exists y\, \mathrm{Dim}_{PA}(y, x) \in \Sigma^0_1$.

per il th. precedente esiste una G t.c.

$Q \vdash G \leftrightarrow \neg \mathrm{Teo}_{PA}(\ulcorner\underline{G}\urcorner)$.

$PA \nvdash G$ se per assurdo $PA \vdash G \Rightarrow \exists n$

$(PA \vdash^n G) \Rightarrow \exists n (Q \vdash \mathrm{Dim}(\underline{n}, \ulcorner G\urcorner)) \Rightarrow Q \vdash \mathrm{Teo}(\ulcorner G\urcorner) \Rightarrow$

$\Rightarrow Q \Rightarrow \neg G \Rightarrow PA \vdash \neg G$ il che contraddice la coerenza di PA

$PA \nvdash \neg G$. $PA \vdash \neg G \Rightarrow \mathbb{N} \vDash \neg G \Rightarrow \mathbb{N} \vDash \mathrm{Teo}_{PA}(\ulcorner\underline{G}\urcorner) \overset{(*)}{\Rightarrow} PA \vdash G$

(tale dim usa $\mathbb{N} \vDash PA$, per cui si preferisce) ...

th $\mathbb{N} \vDash G$

(dim) $PA \nvdash G \Rightarrow \mathbb{N} \vDash \neg \mathrm{Teo}_{PA}(\ulcorner G\urcorner) \Rightarrow \mathbb{N} \vDash G$. (si veda anche (*))

In generale (1° th. di Gödel)

th $T \supset Q$, T ricors. assiomatizz., T coerente, T ω-coerente $\Rightarrow T$ è incompleta.

(oss T ω-coerente $\Rightarrow T$ non dimostra enunciati Σ^0_1 falsi in $\mathbb{N}$.)

(dim) $Q \vdash G \leftrightarrow \neg \mathrm{Teo}_T(\ulcorner\underline{G}\urcorner)$. $T \nvdash G$ (analogo a $PA \nvdash G$ del 1° th di Gödel: caso PA).

$T \nvdash \neg G \Rightarrow T \vdash \mathrm{Teo}_T(\ulcorner\underline{G}\urcorner) \rightarrow T \vdash \exists x\, \mathrm{Dim}_T(x, \ulcorner\underline{G}\urcorner)$, ma

$T \nvdash G \Rightarrow \forall n\ T \nvdash^n G \Rightarrow \forall n\ Q \vdash \neg \mathrm{Dim}_T(\underline{n}, \ulcorner\underline{G}\urcorner) \Rightarrow$

$\forall n\ T \vdash \neg \mathrm{Dim}_T(\underline{n}, \ulcorner\underline{G}\urcorner)$

NOTA: esiste una 3ª versione che sfrutta solo la coerenza di T (Rosser 1936).

(*) $(\mathbb{N} \vDash \mathrm{Teo}_{PA}(\ulcorner\underline{G}\urcorner)) \Rightarrow (\mathbb{N} \vDash \exists x\, \mathrm{Dim}_{PA}(x, \ulcorner\underline{G}\urcorner)) \Rightarrow (\exists n \in \mathbb{N}$

$\mathbb{N} \vDash \mathrm{Dim}_{PA}(\underline{n}, \ulcorner\underline{G}\urcorner)) \Leftrightarrow (\exists n \in \mathbb{N}\ PA \vdash^n G) \Rightarrow (PA \vdash G)$.

per cui $PA \nvdash^n G \Leftrightarrow Q \vdash \neg \mathrm{Dim}_{PA}(\underline{n}, \ulcorner\underline{G}\urcorner) \Rightarrow$

$\Rightarrow \mathbb{N} \vDash \neg \mathrm{Dim}_{PA}(\underline{n}, \ulcorner\underline{G}\urcorner)$.

th (2° di Gödel)
$PA \nvdash Con(PA)$ $\quad (Con(PA) = \neg Teo_{PA}(\ulcorner \bot \urcorner)$ è Π^0_1).

(dim) basta far vedere che $PA \vdash G \leftrightarrow Con(PA)$.
(in realtà basta far vedere $PA \vdash Con(PA) \to G$)

idea: nella dim $PA \nvdash G$ si usa solo la coerenza di PA, vale a dire:
$PA \vdash Con(PA) \to \neg Teo_{PA}(\ulcorner G \urcorner) \to G$. Ma $PA \nvdash G$. Quindi $PA \nvdash Con(PA)$.

un po' di dettagli: sia $\Box_T \varphi = Teo_T(\ulcorner \varphi \urcorner)$. ($T$ ricors. assiomatiz.)

Lemma D1 $(T \vdash \varphi) \Rightarrow (Q \vdash \Box_T \varphi)$
D2 $PA \vdash \Box_T \varphi \to \Box_Q \Box_T \varphi$
(① generalizzato: $\psi \in \Sigma^0_1$ $\mathbb{N} \models \psi \Rightarrow Q \vdash \psi$)
D3 $PA \vdash (\Box_T \varphi \wedge \Box_T(\varphi \to \psi)) \to \Box_T \psi$.

OSS per dim ② e ③ serve PA, Q non basta.

def $\Box^n_T \varphi = Dim(\underline{n}, \ulcorner \varphi \urcorner)$ $\qquad (\Box = \Box_{PA})$

NOTA: D1, D2, D3 si dicono 'condizioni di derivabilità'

formalmente: $PA \vdash G \overset{def\, G}{\underset{D1}{\longleftrightarrow}} \neg \Box G \to \neg \Box \bot$
$(PA \vdash \bot \to G) \Rightarrow (PA \vdash \Box_T(\bot \to G)) \overset{D3}{\Rightarrow} (PA \vdash \Box\bot \to \Box G)$
$\Rightarrow (PA \vdash \neg \Box G \to \neg \Box \bot)$ (questo dà $G \to Con(PA)$)

in PA: $\Box G \overset{D2}{\to} \Box\Box G$, ma anche $\Box G \leftrightarrow \neg G$ che per ① equivale a $\Box(\Box G \leftrightarrow \neg G)$ e per ③ $\Box\Box G$
$\leftrightarrow \Box \neg G$, ma $G \to (\neg G \to \bot)$ e dunque
$\Box(G \to (\neg G \to \bot))$ da cui $\Box G \to \Box(\neg G \to \bot)$ ed
infine $\Box G \to (\Box \neg G \to \Box \bot)$.

OSS (Feferman 1963) $\quad PA_n \overset{def}{=} \{\varphi \in PA \mid \ulcorner \varphi \urcorner \leq n\}$
th $\forall n$ $PA \vdash Con(PA_n)$
inoltre $PA \vdash (Con\, PA \leftrightarrow \forall n\, Con(PA_n))$
$PA^* \overset{def}{=} \bigcup \{PA_n \mid PA_n \text{ coerente}\}$ $(= PA)$
$PA \vdash Con(PA^*) = Con(PA)$ (il [illegible])

(nota: $PA \vdash Con(PA) \leftrightarrow PA = PA^*$)

th (della funz. univ.) esiste $\varphi : \mathbb{N}^{n+1} \to \mathbb{N}$ calc. parz. t.c. p.o. $f : \mathbb{N}^n \to \mathbb{N}$ calc. parz. esiste $e \in \mathbb{N}$ e p.o. x $\varphi(e, \bar{x}) = f(\bar{x})$.

('dim') Codifico (intuit. calcol.) le macchine di Turing con numeri naturali. Sia $\varphi_e : \mathbb{N}^n \to \mathbb{N}$ la funzione calcolata dalla macchina di Turing codificata da e. Infine $\varphi(e, \bar{x}) = \varphi_e(\bar{x})$.

EX esiste $f : \mathbb{N}^2 \to \mathbb{N}$ t.c. p.o. $e \in \mathbb{N}$ $x \mapsto f(e, x)$ calc.
p.o. $x \in \mathbb{N}$ $y \mapsto f(y, x')$ calc.

ma f non è calc.

th (~~forma normale di Kleene~~)

def si indica con $\varphi_e(x) \downarrow_t = y$ che la macchina di Turing di indice e si ferma dopo al più t passi con input x e dà in output y.

th (forma normale di Kleene)
$\{(e, \bar{x}, t, y) \mid \varphi_e(\bar{x}) \downarrow_t = y\}$ è (prim.) ric.

(dim) intuit. dec. ovvio (per cui utilizzando la tesi di Church si può ottenere una dimostrazione intuitiva).

th $f : \mathbb{N} \to \mathbb{N}$ $\quad f : n \longmapsto \begin{cases} \varphi_n(n) + 1 & \text{se } \varphi_n(n)\downarrow \\ 0 & \text{se } \varphi_n(n)\uparrow \end{cases}$

non è calc.

(dim) altrimenti per qualche e $f = \varphi_e$, ma allora
$f(e) = \varphi_e(e) + 1 = f(e) + 1$ (essendo f totale si deve applicare il primo caso).

OSS $g(n) = \varphi_n(n) + 1$ è calc. (parziale).

Cor $K_0 = \{x \mid \varphi_x(x)\downarrow\}$ non è ricorsivo, ma è ric. enumerabile.

(dim) con le ~~f~~ not. prec. $f(n) = \begin{cases} \varphi_n(n)+1 & \text{se } n \in K_0 \\ 0 & \text{se } n \notin K_0 \end{cases}$

$(f_n(n) = \varphi_n(n)\, \mathbb{1}_{K_0})$

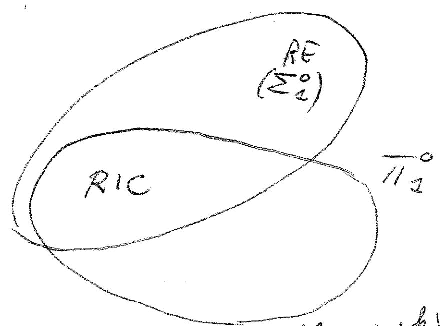
Cor $K = \{(x,y) \in \mathbb{N}^2 \mid \varphi_x(y)\downarrow\}$ non è ricorsivo. problema della fermata

(dim) $x \in K_0 \longleftrightarrow (x,x) \in K$

$\mathbb{1}_{K_0}(x) = \mathbb{1}_K(x,x)$

$\varphi_x(y)\downarrow \longleftrightarrow \exists\, t, u \quad \varphi_x(y)\downarrow_t = u$. (esist. + ricors.)

NOTA



per il th. di Post: RIC $= \Sigma_1^0 \cap \Pi_1^0$.

th tfae: $(A \subset \mathbb{N}^k)$

(1) A è della forma $\exists$ ric (ricors. enum.)

(2) $A = \mathrm{dom}(f)$ dove è calc. (parz.)

(3) $A = \mathrm{Im}(g) \vee (A = \emptyset)$, con g calc. tot. (prim. ric.).

(dim) (1) $\Rightarrow$ (2) $A = \{x \mid \exists y\, R(x,y)\}$ R ricorsivo. $f(x) = \mu y\, R(x,y)$.

(2) $\to$ (1) $A = \mathrm{dom}(f)$ $f = \varphi_e$ $x \in A \leftrightarrow f(x)\downarrow \longleftrightarrow \exists t, u$ $\varphi_e(x)\downarrow_t = u$.

(1) $\to$ (3) $A = \{x \mid \exists y\, R(x,y)\}$

se $A = \emptyset$ fatto

se $A \neq \emptyset$ sia $a \in A$ sia $h(x,y) = \begin{cases} x & \text{se } R(x,y) \\ a & \text{se } \neg R(x,y) \end{cases}$

$\mathrm{Im}(h) = A$. Ora per ottenere una ~~biezione~~ funzione g tra $\mathbb{N}$ ed A è suff. ~~una~~ comporre h con una bijezione tra $\mathbb{N} \to \mathbb{N}^2$.

EX l'inv. di una funz. calc. totale f è a sua volta calc. $(f^{-1}(y) = \mu x\, (f(x) = y))$.

Cor $\exists$ ric $= \exists$ prim ric. $(\varphi_e(x)\downarrow_t = u$ è prim. ric.$)$

OSS $\exists$ prim ric $= \exists \Delta_0$

~~th $\{x \mid \varphi_x$ è totale$\}$~~

EX $\exists A \subset \mathbb{N}$ non ric. enum.

$A = (\mathbb{N} \setminus K_0) = \{x \mid \varphi_x(x)\uparrow\}$ per il th. di Post

th $\{x \mid \varphi_x$ è totale$\}$ non è ric., né ric. enum., (né il suo compl. è...)

(dim) l'insieme è ~~Π_2^0~~ al più Π_2^0 (φ_x è totale sse $\forall y\, \exists t u\, [\varphi_x(y)\downarrow_t = u]$).

(ESEMPIO $\{\ulcorner\varphi\urcorner \in \mathbb{N} \mid Q \models \varphi\} = \{\ulcorner\varphi\urcorner \mid Q \vdash \varphi\}$
molto grosso RE.)

OSS esiste $h : \mathbb{N} \to \mathbb{N}$ calc. totale t.c. $\{\varphi_{h(i)}\}_{i \in \mathbb{N}} = \{$prim. ricors.$\}$. dove $h(e)$ è l'e-simo μ-programma senza μ.

Oss $g(n) = \varphi_{h(n)}(n)+1$ è calc. tot., ma non pr. ric.

(Libro di riferimento "theory of recursion function" - Rogers (o Odifreddi))

l'insieme di sopra viene (in genere) denominato TOT. La dim. si ottiene utilizzando la g seguente all'oss.

def $A, B \subset \mathbb{N}$ disg. sono ric. inseparabili (RI) se

ESEMPIO $A = \{ \ulcorner\varphi\urcorner \mid Q \vdash \varphi \}$ $B = \{ \ulcorner\varphi\urcorner \mid Q \vdash \neg\varphi \}$

sono RI (per cui in part. non sono ricors.)

(dim) posposta.

th esistono A, B RI e RE.

(dim) $A = \{ x \mid \varphi_x(x)\downarrow = 0 \}$ $B = \{ x \mid \varphi_x(x)\downarrow = 1 \}$

per il th Kleene sono entrambi ric. en.

Se per assurdo esistesse R ricorsivo che li separa allora 1_R (è calcolabile) è uguale a φ_e per qualche e. Ora se $e \in R$ $\varphi_e(e) = 1$ e dunque $R \cap B \neq \phi$. Se $e \notin R$ $\varphi_e(e) = 0$ e dunque $A \cap R \neq \phi$.

def una teoria T è indecidibile sse l'insieme dei suoi teoremi $\{\varphi \mid T \vdash \varphi\}$ non è ricorsivo. (1)

th se T è ric. assiomatizzata ($\{\varphi \mid T \vdash \varphi\}$ è RE e $\{\varphi \mid T \vdash \varphi\}$ è ric. en.) e se T è completa (T si assume sempre coerente) ~~$\{\varphi \mid T \vdash \varphi\}$ ed il~~ allora T è decidibile.

oss basta anche T ric. enum.

def T_1 è equivalente a T_2 $\iff \forall \varphi (T_1 \vdash \varphi \iff T_2 \vdash \varphi)$ $\iff Mod(T_1) = Mod(T_2)$.

ESEMPI

T	decidibile	indecidibile	completa	non completa	assiomatizzabile
PA & ZF	no	sì	no	sì	sì
Q	no	sì	no	sì	sì
$Th(\mathbb{N},+,\cdot)$	no	sì	sì	no	no
$Th(\mathbb{Z},+,\cdot)$	no	sì	sì	no	no
$Th(\mathbb{N},+,0,\sigma)$	sì	no	sì	no	sì
$Th(\mathbb{C},+,\cdot,0,1)$	sì	no	sì*	no	sì
$Th(\mathbb{R},+,\cdot,0,1,<)$	sì	no	sì	no	sì
$Th(\mathbb{Q},+,\cdot)$	no	sì	sì	no	no

~~th (Rosser, Gödel)~~

def T è essenzialmente indecidibile sse ogni $T' \supseteq T$ ($L(T) = L(T')$) è indecidibile.

ESEMPIO la teoria dei campi è indecidibile, ma non lo è essenzialmente.

infatti ~~perché~~ $(\mathbb{C}, \dots)$ è decidibile ed è un'estensione della teoria dei campi.

* assiomi dei campi alg. chiusi e di caratt. 0.

$ACF_0 \equiv Th(\mathbb{C}, +, \cdot, 0, 1)$

campi
$x+y = y+x$
$xy = yx$
$\forall x \neq 0 \; \exists y \; xy = 1$
$x(y+z) = xy + xz$
$x0 = 0 \quad x1 = x \quad x+0 = x$
$(x+y)+z = x+(y+z)$
$(xy)z = x(yz)$.

char = 0 $\forall n \; \underbrace{1+1+\dots+1}_{n \text{ volte}} \neq 0$.

AC p.o. n ~~...~~ $\forall (a_i)_{0 \le i \le n} \; \exists x \; \sum_{0}^{n} a_i x^i = 0$.

th Q è essenzialmente indecidibile. (da sapere!)

(dim) siano $A, B \subset \mathbb{N}$ ~~due insiemi~~ RE e ~~non~~ RI

in Q = Q*

(p.es. $A = \{x \mid \varphi_x(x)\downarrow = 0\}$ $B = \{x \mid \varphi_x(x)\downarrow = 1\}$.)

$\varphi_x(x)\downarrow = 0 \iff \exists t \; \varphi_x(x)\downarrow_t = 0 = \exists t \, R_A(x,t)$ con R_A PR

$A = \{x \mid \exists t \; R_A(x,t)\}$ $\quad B = \{x \mid \exists t \; R_B(x,t)\}$ con R_B PR

$A \cap B = \emptyset$. siano $\alpha(x,t)$ e $\beta(x,t)$ formule che binumerano rispettivamente R_A ed R_B (in Q).

$M \models Q$ $\quad \{x \in M \mid M \models \exists t \; \alpha(x,t)\} = A_M$ $\quad (= A$ se $M = \mathbb{N})$

$\{x \in M \mid M \models \exists t \; \beta(x,t)\} = B_M$ $\quad (= B$ se $M = \mathbb{N})$

siano $A'(x) = \exists t (\alpha(x,t) \wedge \forall t' < t \; \neg \beta(x,t'))$ $\quad \begin{pmatrix} A(x) = \exists t \, \alpha(x,t) \\ B(x) = \exists t \, \beta(x,t) \end{pmatrix}$

e $B'(x) = \exists t (\beta(x,t) \wedge \forall t' < t \; \neg \alpha(x,t'))$

$\forall n \in \mathbb{N} \quad Q \vdash n \notin (A' \cap B')$

$n \in A \Rightarrow Q \vdash \underline{n} \in A'$

$n \in A \Rightarrow \exists t \in \mathbb{N} \; R_A(n,t) \Rightarrow \exists t \in \mathbb{N} \; Q \vdash \alpha(\underline{n}, \underline{t})$

p.o. $t' \le t$ $\; R_B(n,t') \Rightarrow Q \vdash \forall t' < \underline{t} \; \neg \beta(\underline{n}, t') \Rightarrow Q \vdash \underline{n} \in A'$

analogamente $n \in B \Rightarrow Q \vdash \underline{n} \in B'$

se Q fosse decidibile R sarebbe ricorsivo. 54

Cor sia $T \supseteq Q^*$ coerente, ric. assiomat., $L(T)=L(Q^*)$ allora T è incompl.

(dim) se fosse completa (per il th. di Post) sarebbe decidibile.

ESEMPIO $T = PA + \neg Con(PA)$ è coerente, ric. assiomat. $L(T)=L(Q^*)$ per cui è incompleta.

th (Church) il calcolo dei predicati è indecidibile. ($\{\varphi \mid \models \varphi\}$ è indecid.) se il linguaggio contiene almeno una relazione binaria.

(dim) sia $L=\{0, \sigma, +, \cdot\}$ (non importa perché non si usano assiomi su tali 'simboli').

$Q^* \vdash \varphi \iff \vdash \bigwedge Q^* \to \varphi$

se esistesse un algoritmo per verificare la validità di $\vdash \bigwedge Q \to \varphi$ un tale algoritmo risolverebbe anche il problema se φ fosse un teorema di Q.

th (generalizzazione del precedente)
se T è decidibile $L=L(T)$ $\varphi = L$-enunciato allora $T+\theta$ è decidibile.

(dim) $T+\theta \vdash \varphi \iff T \vdash \theta \to \varphi$.

th (di Rosser) $L=\{0, \sigma, +, \cdot\}$
sia T L-teoria $\supseteq Q$, ricors. assiomat., coerente allora T è incompleta.

(dim) (senza th. della calcolabilità) (quella originale di Rosser)
$\Box\varphi \overset{def}{=} \exists x\, Dim_T(x, \ulcorner\varphi\urcorner)$, $\Box\varphi_t = \exists x \leq t\, Dim(x, \ulcorner\varphi\urcorner)$.
$\Box\varphi \leq \Box\psi \overset{def}{\iff} \forall t\, (\Box_t\psi \to \Box_t\varphi)$.

per il lemma di diagonalizzazione esiste 55 un enunciato R t.c. $Q \vdash R \leftrightarrow (\Box\neg R \leq \Box R)$

- se $T \vdash R$ allora $\exists m \in \mathbb{N}$ $T \vdash^m R$ allora $Q \vdash \Box_m R$
Ora la precedente assunzione su R insieme a $T \vdash^m R$ dà $T \vdash \Box\neg R \leq \Box R$ e quindi $T \vdash \Box_m R$
se $T \nvdash^m \neg R$ allora $Q \vdash \neg\Box_m \neg R$ e ancora $T \vdash \neg\Box_m \neg R$ assurdo. se $T \vdash^m \neg R$ ancora assurdo.

(oss il lemma di diag. è molto forte; p. es. si può definire tramite esso una costante che sia uguale ad ogni numero.)

- se $T \vdash \neg R$ allora $\exists m$ $T \vdash^m \neg R$, e dunque $Q \vdash \Box_m \neg R$ e di conseguenza $T \vdash \Box_m R$.
Per l'assunzione su R $T \vdash \neg(\Box\neg R \leq \Box R)$ e quindi $T \vdash \Box_m R$ ... allora $T \vdash^m R$.

prop $Th(\mathbb{N}, 0, \sigma, +, \cdot)$ e $Th(\mathbb{N}, 0, 1, +, \cdot)$ sono indecidibili. (le due teorie sono perfett. equivalenti)

corollario $Th(\mathbb{Z}, 0, 1, +, \cdot)$ è indecidibile
se esistesse un algoritmo che decide se $Th(\mathbb{Z}) \vdash \varphi$ allora $(\mathbb{Z} \models \varphi)$ allora se ne potrebbe costruire un altro per sapere se $\mathbb{N} \models \psi$.
l'unico ostacolo è definire ≥ 0 in $\mathbb{Z}$.
idea di definiz.: $x \geq 0 \leftrightarrow \exists abcd\ x = a^2+b^2+c^2+d^2$.
th. Lagrange

si ottiene così una traduzione L-form $\to$ L-form $\varphi \mapsto \varphi^{\geq 0}$ definita per induzione:
$(x+y=z)^{\geq 0} = (x \geq 0, y \geq 0, z \geq 0 \wedge x+y=z)$
$(xy=z)^{\geq 0} = \dots$
$(\varphi \wedge \psi)^{\geq 0} = \varphi^{\geq 0} \wedge \psi^{\geq 0}$

$(\neg\varphi)^{\geq 0} = \dots$

$(\forall x\, \varphi)^{\geq 0} = \forall x \geq 0\ (\varphi)^{\geq 0} = \forall x\ (x \geq 0 \rightarrow (\varphi)^{\geq 0})$

$(\exists x\, \varphi)^{\geq 0} = \exists x \geq 0\ (\varphi)^{\geq 0} = \exists x\ (x \geq 0 \wedge (\varphi)^{\geq 0})$

si dice $Th(\mathbb{N}, +, \cdot, 0, 1) \underset{I}{\lhd} Th(\mathbb{Z}, +, \cdot, 0, 1)$

dove I è la traduzione.

in generale $T_1 \underset{I}{\lhd} T_2 \leftrightarrow (T_1 \vdash \varphi \Leftrightarrow T_2 \vdash \varphi^I)$

con $\varphi \mapsto \varphi^I$ calcolabile.

~~in questo caso~~

th $T_1 \underset{I}{\lhd} T_2 \Rightarrow T_2$ decid. $\rightarrow T_1$ decid.

($\Rightarrow T_1$ indecid. $\rightarrow T_2$ indecid.)

def L_1, L_2 una interpretazione $I : L_1 \rightarrow L_2$ è una traduzione t.c.

$(\varphi \wedge \psi)^I = \varphi^I \wedge \psi^I$ e $(\neg\varphi)^I = \neg(\varphi)^I$

(*) $(\forall x\ \varphi(x))^I = \forall x\ (\Delta(x) \rightarrow (\varphi(x))^I)$ (dove Δ è un parametro da cui I dipende)

def sia $I : L_1 \rightarrow L_2$

$T_1 \lhd_I T_2 \Leftrightarrow \forall\varphi\ (T_1 \vdash \varphi \Leftrightarrow T_2 \vdash \varphi^I)$.

ESEMPIO int. di PA in ZF

$\Delta(x) = \forall N\ (0 \in N \wedge \forall v\ (v \in N \rightarrow \text{'}\sigma(v)\text{'} \in N) \rightarrow x \in N]$

$0^I = x$ ~~...~~ $\xrightarrow{I} \forall u\ \ u \notin x$

$\sigma(x) = y \longrightarrow \forall u\ (u \in y \Leftrightarrow u \in x \vee u = x)$.

NOTA: PA : $\lhd$ ZF $\setminus$ {infinito} $\cup$ {$\neg$ infinito}.

$Q \lhd Th(\mathbb{N}, +, \cdot, 0, 1) \lhd Th(\mathbb{Z}, 0, 1, +, \cdot)$

(*) φ atomica $\mapsto \varphi^I$ arbitraria

$\varphi(x_1, \dots x_n) \longmapsto \Delta x_1 \wedge \dots \wedge \Delta x_n \wedge \varphi^I(x_1, \dots x_n)$.

~~prop QA φ ...~~ ~~anelli commutativi $\vdash \varphi^I$~~ dim

th $Q \lhd S \Rightarrow S$ indecidibile (la prec. è sbagliata)

(dim) sia $Q \subset T = \{\varphi \mid S \vdash \varphi^I\}$

$T \vdash \varphi \Leftrightarrow S \vdash \varphi^I$ (ci sarebbe da verif. che T è chiusa)

T indecid. $\Rightarrow S$ indecid.

th $Q \underset{I}{\lhd} S \qquad S = T + \Theta \Rightarrow T$ è indecid. (S, T coerenti)

(dim) $T + \theta \vdash \varphi \Leftrightarrow T \vdash \theta \rightarrow \varphi$.

th $Q \underset{I}{\lhd} S \qquad S \supset T \qquad L(T) = L(S) \Rightarrow T$ è indecid.

(dim) $\exists\ S' \subset S$ finita $\quad Q \underset{I}{\lhd} S' \qquad Q \vdash \varphi \Rightarrow S \vdash \varphi^I$

$S' \subset T + \{\theta_1, \dots \theta_n\} \qquad Q \underset{I}{\lhd} T + \theta_1, \dots \theta_n \Rightarrow T$ è indecid.

corollario Th (anelli commutativi) è indecidibile.

$L = \{0, 1, +, \cdot\} \qquad Ax = \{$ soliti assiomi $\}$.

dim $Q \lhd Th(\mathbb{Z}, 0, 1, +, \cdot) \supset Th(\dots)$, da cui la tesi.

oss è sempre possibile espandere un linguaggio per trovarsi nelle ipotesi del th ultimo. Ciò non dà indicazioni sulla teoria iniziale.

th (J. Robinson) $\mathbb{N}$ è definib. in $(\mathbb{Q}, +, \cdot, 0, 1)$

(oss non def. in $\mathbb{R}$) $\quad a \in \mathbb{N} \Leftrightarrow \mathbb{Q} \models \Delta(a)$.

oss ciò fornisce una interpr. di $\mathbb{N}$ in $\mathbb{Q}$

dove $+^I = + \quad \dots \quad$ e ~~...~~ $\Delta \dots$

da cui l'indecidibilità di $\mathbb{Q}$ e di seguito anche ~~quell~~ della teoria dei campi.