3/11/2017

BERARDUCCI
TEORIA

Def Data M una $\mathcal{L}$-struttura e $X \subseteq M^n$, si dice che X è φ-definibile se esiste una $\mathcal{L}$-formula $\varphi(x_1, \dots, x_n)$ tale che $X = \{\vec{a} \in M^n \mid M \models \varphi(\vec{a})\}$

oss Cioè X è definibile se può essere caratterizzato da una formula.

Def Data M una $\mathcal{L}$-struttura e $X \subseteq M^n$, si dice che X è B-definibile se esiste una $\mathcal{L}$-formula $\varphi(\vec{x}, \vec{y}) = \varphi(x_1, \dots, x_n, y_1, \dots, y_k)$ e $\vec{b} \subseteq B$ tale che $X = \{\vec{a} \mid M \models \varphi(\vec{a}, \vec{b})\}$

Esempio Gli zeri di un polinomio sono definibili prendendo come parametri i coefficienti del polinomio

Si vedono alcuni fatti senza dimostrazione.

- I primi sono definibili in $(\mathbb{N}, +, \cdot)$ ma non in $(\mathbb{N}, +)$

Def $f: M^n \to M$ definibile se $\Gamma(f) = \{(\vec{a}, \vec{b}) \mid f(\vec{a}) = \vec{b}\}$ è definibile.

- $+: \mathbb{N}^2 \to \mathbb{N}$ non è definibile in $(\mathbb{N}, 0, S)$ (anche se lo è al II ordine)
- $\times: \mathbb{N}^2 \to \mathbb{N}$ non è definibile in $(\mathbb{N}, 0, S, +)$
- L'applicazione $(x, y) \mapsto x^y$ da $\mathbb{N}^2 \to \mathbb{N}$ è definibile $(\mathbb{N}, +, \cdot)$

oss Si considera la logica del II ordine. Allora il $+$ è definibile se è caratterizzato da una formula φ del II ordine $(x+y=z \iff \mathbb{N} \models \varphi(x,y,z))$

Si può considerare

$$\forall P \text{ ternario } [\forall a\, P(a,0,a) \wedge \forall a,b,c\, P(a,b,c) \to P(a, S(b), S(c)] \to P(x,y,z)$$

che è una formula che definisce la somma al II ordine.
In particolare il grafico della funzione somma è la più piccola P che soddisfa la proprietà sopra.

oss La dimostrazione che l'esponenziazione è definibile al I ordine non è banale. È stata fatta da Gödel e si basa su teorema cinese del resto:

Siano $a_0, \dots, a_n \in \mathbb{Z}$ coprimi e $b_0, \dots, b_n \in \mathbb{Z}$
Allora $\exists x$ t.c. $\begin{cases} x \equiv b_0 \ (a_0) \\ \vdots \\ x \equiv b_n \ (a_n) \end{cases}$

Però, come si intendono i moduli?

Lemma $\forall u, x \in \mathbb{N}\ \exists d > x$ tale che $d+1, 2d+1, \ldots, ud+1$ sono coprimi.

Esempio Se $n=3$, $x=5$

Dim

Si consideri $y > \max(u,x)$ e si consideri $d = y!$
Se p è un primo tale che $p \mid id+1$ e $p \mid jd+1$
allora $p \mid (i-j)d$, quindi $p \mid (i-j)$ o $p \mid d$
Ma, visto che $y > \max(u,x)$, allora $y!$ ha come fattori tutti i numeri minori di u, tra cui $i-j$.
perciò $(i-j) \mid d$.
Allora sicuramente $p \mid d$, assurdo in quanto visto che $p \mid id+1$, si avrebbe $p \mid 1$.

Def Si definisce $\mathrm{re}(x,y) = r$ se $\exists q\,(x = yq + r \wedge r < y)$

oss Questa è la definizione della funzione resto della divisione classica ed è definibile in $\mathbb{N}$.

oss Si noti che composizione di funzioni definibili è definibile.

Supponendo di aver definito $f(x_1, \ldots, x_k)$ e $g(x_1, \ldots, x_n)$
e si consideri $h(\vec{x}) = f(g(\vec{x}))$, cioè $h(x_1, \ldots, x_n) = f(g_1(x_1 \ldots x_n), \ldots, g_k(x_1 \ldots x_n))$

$$h(x) = y \iff \exists z\,(g(x) = z \wedge f(z) = y)$$

Questa formula, visto che $g(x) = z$ e $f(z) = y$ sono definibile, è una definizione di h.

Si definisca ora la β di Gödel

Def Si definisce $\beta(c,d,i) = \mathrm{re}(c, (i+1)d+1)$

Lemma Per ogni $u \in \mathbb{N}$ e $\forall (b_0, \ldots, b_u)\ \exists c,d$ tali che $\beta(c,d,0) = b_0$, $\beta(c,d,1) = b_1$, $\ldots$ $\beta(c,d,n)$

Dim

Dati u e $b_0, \ldots, b_u$, sia d tale che $d+1, 2d+1, \ldots, nd+1$ coprimi
e $d > \max b_i$ (che esiste per il lemma precedente).
Per il teorema cinese del resto, sia c tale che

$$\bigwedge_{i=0}^{u=1} c \equiv b_i \quad ((i+1)d+1)$$

Si noti, però, che $b_i = \mathrm{re}(c, (i+1)d+1) = \beta(c,d,i)$

oss Si osservi che la β di Gödel è definibile usando solo $+$ e $\cdot$.

Adesso è possibile dimostrare che $x,y \mapsto x^y$ è definibile in $(\mathbb{N}, +, \cdot, 0, S)$ (anche se $0, S$ sarebbero superflui)

$$x^y = z \iff \exists (b_0, \dots, b_y) \left[b_0 = 1 \wedge b_y = z \wedge \forall i<y \; b_{i+1} = x \cdot b_i \right]$$

Questa definizione però è del secondo ordine, ma può essere ridotta al primo ordine tramite la β di Gödel

$$x^y = z \iff \exists c,d \left[\beta(c,d,0) = 1 \wedge \beta(c,d,y) = z \wedge \forall i<y \; \beta(c,d,i+1) = x \cdot \beta(c,d,i) \right]$$

Questa invece è una formula $\varphi(x,y,z)$ del primo ordine che definisce l'esponenziazione (le varie somme e prodotti sono espandibili con le loro definizioni).

oss Le due definizioni, grazie alla definizione di β, sono equivalenti.

Def Si definisce ricorsione primitiva una funzione f tale che

$$f(\vec{x}, 0) = g(\vec{x}) \quad \text{e} \quad f(\vec{x}, i+1) = h(\vec{x}, i, f(\vec{x}, i))$$

Prop Se g e h sono definibili, allora anche la ricorsione primitiva f lo è

Dim
$$f(\vec{x}, y) = z \iff \exists (b_0, \dots b_y) \text{ tali che } b_0 = g(\vec{x}),\ b_y = z \text{ e } \forall i<y \; b_{i+1} = h(\vec{x}, i, b_i)$$

È possibile trasformare questa formula in una del primo ordine:

$$f(\vec{x}, y) = z \iff \exists c,d \left[\beta(c,d,0) = g(\vec{x}) \wedge \beta(c,d,y) = z \wedge \forall i<y \; \beta(c,d,i+1) = h(\vec{x}, i, \beta(c,d,i)) \right.$$

Visto che g e h sono definibili, allora questa è una definizione di f.

Def $f : \mathbb{N}^n \to \mathbb{N}$ è primitiva ricorsiva se si ottiene da $0, S, \prod_i^n$ ($\prod_i^n$ è la proiezione: $\prod_i^n(x_1, \dots, x_n) = x_i$) con composizione e ricorsione primitiva.

Esempio $+$ è primitiva ricorsiva.

Infatti $+(x,y)$ dovrebbe essere definita in modo che
$+(x,0) = g(x)$ e $+(x, y+1) = h(x, y, +(x,y))$
Questo è possibile scegliendo:

- $g(x) = x = \prod_1^1(x)$
- $h(x,y,z) = z+1 = S\left(\prod_1^3(x,y,z)\right)$

oss Allo stesso modo si vede che anche $\cdot$ è primitiva ricorsiva.

Esempio Si consideri la funzione predecessore definita in modo che $P(0)=0$ e $P(x+1)=x$.

Anche questa, vedendo $P(x+1) = x = h(x, p(x))$, con $h = \Pi_1^2$, è primitiva ricorsiva.

Esempio Si consideri la funzione sottrazione definita in modo che

- $x \dot{-} 0 = x$
- $x \dot{-} s(y) = p(x \dot{-} y)$

Quindi anche questa è ~~definita~~ primitiva ricorsiva.

Esercizio Vedere che la funzione $x \mapsto P_x$ (cioè il più piccolo primo maggiore di x) è primitiva ricorsiva.

oss A livello di programmazione, le funzioni primitive ricorsive sono quelle calcolabili usando solo cicli 'for'.

Def $X \subseteq \mathbb{N}^k$ è primitivo ricorsivo se la sua funzione caratteristica è primitiva ricorsiva.

Esercizio L'insieme dei primi è primitivo ricorsivo.

oss $x=y$, cioè $\{(x,y) \mid x=y\} \subseteq \mathbb{N}^2$ è primitivo ricorsivo.

Cioè $\chi_= : \mathbb{N}^2 \to \{0,1\}$ è primitiva ricorsiva

$$x=y \iff x \dot{-} y = 0 \wedge y \dot{-} x = 0$$

oss La funzione $A : \mathbb{N}^3 \to \mathbb{N}$ tale che $A(x,0) = x+1$, $A(0,y) = y+1$, $A(x+1, y+1) = A(x, A(x+1, y))$ (funzione di Ackermann)
Questa è una funzione ricorsiva che non è primitiva ricorsiva, però è comunque definibile, in quanto esiste comunque una successione finita di passi che la calcola e procedere con la β di Gödel analogamente a prima.

oss Si ottengono esistono funzioni non definibili, infatti $|\mathbb{N}^{\mathbb{N}}| = 2^{\aleph_0}$ mentre le formule possibili che possono definire una funzione sono solo $\aleph_0$.
È difficile però trovarne una.

oss Le funzioni definibili però non sono sempre calcolabili

Esempio La funzione $f(n)$ = n-esima cifra del π è primitiva ricorsiva.

In conclusione

$$\{\text{f primitiva ricorsiva}\} \subsetneq \{\text{f calcolabile}\} \subsetneq \{\text{f definibile in } (\mathbb{N}, +, \cdot)\}$$

16/11/2017

BERARDUCCI
TEORIA

L'altra volta si è dimostrato che $a^b = c \Leftrightarrow \mathbb{N} \models \varphi(a,b,c)$, cioè che l'esponenziazione è definibile in $\mathbb{N}$.
In realtà è possibile dimostrare che $a^b = c \Leftrightarrow PA \vdash \dots$
$\Leftrightarrow Q \vdash \dots$
In PA, inoltre, oltre qualcosa in più, si può dimostrare infatti che
$PA \vdash \forall x,y \; \exists! z \, "(x^y = z)"$

Def di minimalizzazione

Def Data una funzione la
minimalizzazione
$f : \mathbb{N}^k \to \mathbb{N} \qquad f(\bar{x}) = \mu y [h(\bar{x},y) = 0]$

Si vede una possibile definizione di funzione calcolabile

calcolabilità e registri

$\begin{cases} X := Y \\ X := X+1 \\ \text{if } X = 0 \text{ go to} \\ X := 0 \end{cases}$

Programma a registri per f

1) Input X
2) $Z := 0$
3) $U := h(X,Z)$
4) if $U = 0$ output Z
5) else $Z := Z+1$ go to (3)

Può capitare che 1) non funzioni mai, ossia la f è indefinita per quello argomento
Quindi anche se si trovasse z non è detto che sia il minimo

Esempio se $h(3,0) = 2$
$h(3,1)$ non termina
$h(3,2) = 0$
Quanto è $f(3)$? $(f(3)\uparrow)$
$f(3)$ non termina con questo algoritmo perché si blocca al passaggio 2)

μ fa questo

$$f(\bar{x}) = y \Leftrightarrow u(\bar{x},y) = 0 \wedge \forall y' < y \; u(\bar{x},y') \downarrow \neq 0 \Leftrightarrow$$

($f(\bar{x}) = y$: termina e mi dà come output y; $u(\bar{x},y') \downarrow$: termina e $\neq 0$)

$$\Leftrightarrow h(\bar{x},y) = 0 \wedge \forall \bar{y}' < y \; (\exists u \neq 0)[h(\bar{x},y') = u]$$

oss Questa def, se la vedi bene, non usa quantificatori universali

Esercizio La ricorsione primitiva è calcolabile a registri

La ric. prim era $f(\vec{x},0)=g(\vec{x})$
$f(\vec{x},y+1)=h(\vec{x},y,f(\vec{x},y))$
supponiamo che h, g calcolabili a registri

1) input $\vec{x}, y$
2) $z := g(\vec{x})$
3) $k := 0$
4) se $k=y$ output z
5) se no $z := h(x,k,z)$ [se la vecchia z valeva $f(x,k)$ la nuova z vale $f(x,k+1)$
$k = k+1$
goto 4)

Def $f: \mathbb{N}^k \to \mathbb{N}$ è parziale è una funzione definita solo su un sottoinsieme di $\mathbb{N}^k$
cioè $f: \mathbb{N}^k \longrightarrow \mathbb{N} \cup \{\uparrow\}$

Def $\text{dom } f = \{x \mid f(x) \neq \uparrow\}$

oss Dato un programma a registri
input $x_1, \dots, x_n$ output y
gli associo $f: \mathbb{N}^k \to \mathbb{N} \cup \{\uparrow\}$ t.c. $f(\vec{a}) = b \in \mathbb{N}$
Se $P(\vec{a})$ si ferma output b, se non si ferma $f(\vec{a}) = \uparrow$

Def ~~Una~~ funzione è μ-calcolabile sono la più piccola classe di funzioni che hanno le funzioni 0, S, ricorsione primitiva, μ (minimalizzazione)

oss Queste in realtà sarebbero μ-programmi, a cui vengono associati delle funzioni

Si deve definire il dominio della funzione calcolata con un μ-programma

$\text{dom } 0 = \mathbb{N}^k$
$\text{dom } S = \mathbb{N}^k$
$\text{dom } (f \circ g) = ?$

$$f(g(x))\downarrow \iff \exists z\ g(x)\downarrow = z \wedge f(z)\downarrow$$

Esempio Sup. $f(\vec{x}) = \mu y [h(\vec{x},y)=0]$

$\text{dom } f = ?$

$$f(\vec{x})\downarrow \iff \exists y\ h(\vec{x},y)\downarrow = 0 \wedge \forall y'<y\ h(\vec{x},y')\downarrow \neq 0$$

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

$$f(\vec{x},y)\downarrow \iff \forall y'<y\ \exists u\ [f(\vec{x},y)\downarrow = u \wedge g(\vec{x})\downarrow \wedge h(\vec{x},y,u)\downarrow]$$

Abbiamo visto quindi che
μ-calcolabili $\subseteq$ calcolabili $\rightarrow$ registri

(in realtà $\supseteq$ è vero ma è più difficile

Quindi si ha la TESI DI TURING, cioè

intuitivamente calcolabile = calc. a registri
(Turing-calcolabile)

Funzioni calcolabili totali (quelle che terminano sempre)

UIH

primitive ricorsive

Dimostriamo che l'inclusione è propria

Enumero in modo intuitivamente calcolabile: programmi primitivi ricorsivi

$P_0 \rightarrow f_0$
$P_1 \rightarrow f_1$ potrebbe essere anche che $f_i = f_j$ con $i \neq j$
$P_2 \rightarrow f_2$

e considero la funzione $n \mapsto P_n$ (è una funz. da $\mathbb{N} \rightarrow \{\text{Programmi}\}$

Faccio un proc. ohegoniale e definisco $D(n) = f_n(n) + 1$

Sicuramente $D(n)$ è calcolabile totale però non è primitiva ricorsiva.
se lo fosse $\exists k$ $D = f_k$ ma $D(k) \neq f_k(k)$ assurdo

oss Siamo al limite del paradosso infatti

sia P_n = n-esimo programma che calcola

$f_n : \mathbb{N} \rightarrow \mathbb{N} \cup \{\uparrow\}$

$D(n) = f_n(n) + 1$
$D \neq f_k \ \forall k$ assurdo (contraddice la tesi di Turing)

Il problema sta nel fatto che in realtà
D e f_k calcolate in k potrebbero divergere entrambe

Abbiamo visto quindi che

Teorema μ-calcolabili $\subseteq$ calcolabili $\Rightarrow$ registri

(in realtà $\supseteq$ è vero ma è più difficile

Quindi si ha la TESI DI TURING, cioè

intuitivamente calcolabile = calc. a registri

(Turing-calcolabile)

Funzioni calcolabili totali (quelle che terminano sempre)

UNIT

primitive ricorsive

Dimostriamo che l'inclusione è propria

Enumero in modo intuitivamente calcolabile i programmi primitivi ricorsivi

$P_0 \to f_0$

$P_1 \to f_1$ potrebbe essere anche che $f_i = f_j$ con $i \neq j$

$P_2 \to f_2$

e considero la funzione $n \mapsto P_n$ (è una funz. da $\mathbb{N} \to$ {programmi})

Faccio un proc. diagonale e definisco $D(n) = f_n(n) + 1$

Sicuramente $D(n)$ è calcolabile totale però non è primitiva ricorsiva.

Se lo fosse $\exists k$ $D = f_k$ ma $D(k) \neq f_k(k)$ assurdo

oss Siamo al limite del paradosso infatti

sia P_n = n-esimo programma che calcola

$f_n : \mathbb{N} \to \mathbb{N} \cup \{\uparrow\}$

$D(n) = f_n(n) + 1$

$D \neq f_k \ \forall k$ assurdo (contraddice la tesi di Turing)

Il problema sta nel fatto che in realtà

D e f_k calcolate in k potrebbero divergere entrambe

Def Decidibile = ricorsivo (RIC)
semidecidibile = ricorsivamente numerabile (RE)

Def $A \subseteq \mathbb{N}^k$ è decidibile se $\chi_A : \mathbb{N}^k \to \{0,1\}$ è μ-calcolabile totale

$A \subseteq \mathbb{N}^k$ è RE se esiste $B \subseteq \mathbb{N}^k \times \mathbb{N}^e$ decidibile tale che

$x \in A \iff \exists y$ t.c. $(x,y) \in B$

oss Intuitivamente RE = $\exists$ RIC

Esempio Quando $\mathbb{Q} \to \mathbb{Q}$ è calcolabile?

Fissiamo una codifica con i naturali

$$\begin{array}{ccc} q/p & \mathbb{Q} & \xrightarrow{f} & \mathbb{Q} \\ \uparrow & \uparrow cod & & \uparrow cod \\ (a,b) & \mathbb{N}^2 & \xrightarrow{\hat{f}} & \mathbb{N}^2 \end{array}$$

Qui si parla di calcolabilità rispetto a una codifica
Se le codifiche però sono fatte "senza barare" sono tutte equivalenti.

oss Le codifiche si fanno o con codifiche surgettive o con codifiche biunivoche
(una quella serve basterà)

oss Supponiamo ci sia $\exists$. $\{\text{formule}\} \to \mathbb{N}$ una codifica iniettiva

(cod: Dominio $\to \mathbb{N}$ iniettiva e $Im(cod) \subseteq \mathbb{N}$ decidibile)

Def
$$\begin{array}{ccc} Dominio_1 & \xrightarrow{cod_1} & \mathbb{N} \\ f \downarrow & & \downarrow \hat{f} \\ Dominio_2 & \xrightarrow{cod_2} & \mathbb{N} \end{array}$$
f calc $\Leftrightarrow \hat{f}$ calc.

TEORETTA DI POST

Teorema $A \subseteq \mathbb{N}^k$ RE, $\mathbb{N}^k \setminus A$ RE $\Rightarrow A$ RIC

Prop $A \subseteq \mathbb{N}$ RE $(\neq \emptyset) \iff \exists f : \mathbb{N} \to \mathbb{N}$ calcolabile totale t.c.
$A = Im f = \{ f(n) \mid n \in \mathbb{N} \}$

Intanto fissiamo una codifica delle coppie $\langle , \rangle : \mathbb{N}^2 \to \mathbb{N}$
t.c.

$$\langle x,y \rangle = n \iff n = \frac{(x+y)(x+y+1)}{2} + x \iff 2n = (x+y)(x+y+1) + 2x$$

20/11/2017 BERARDUCCI

Prop Se $A \subseteq \mathbb{N}$ ($A \neq \emptyset$) è semidecidibile, allora esiste $f: \mathbb{N} \to \mathbb{N}$ tale che $A = \mathrm{Im} f = \{f(n) \mid n \in \mathbb{N}\}$ e f calcolabile totale.

Dim

Sia $a \in A = \{x \mid \exists \vec{y}\, Q(x, \vec{y})\}$ con Q ricorsiva.

Si definisca $f: \mathbb{N}^2 \to \mathbb{N}$ tale che $f(x,y) = \begin{cases} x & \text{se } \exists y\, Q(x,y) \\ a & \text{altrimenti} \end{cases}$

Si osservi che $\mathrm{Im} f = A$. Per avere una funzione con dominio $\mathbb{N}$ è possibile comporla con una biiezione da $\mathbb{N}$ a $\mathbb{N}^2$.
In questo modo si ottiene una f' con le proprietà richieste.
Ad esempio la funzione $2^x(2y+1) - 1 \longleftrightarrow (x,y)$, che è anche primitiva ricorsiva (esercizio).

Prop Se $A = \mathrm{Im} f$, con f calcolabile totale, allora A è semidecidibile

Dim

Ovvia in quanto $x \in A \iff \exists y\, x = f(y)$ che è decidibile in quanto l'$=$ è decidibile (si è visto che $\chi_=$ è primitiva ricorsiva).

TEOREMA DI POST

Teorema Sia $A \subseteq \mathbb{N}$. Se A e $A^c = \mathbb{N} \setminus A$ sono ricorsivamente enumerabili, allora A è ricorsivo.

Dim

Si ha che $x \in A \iff \exists y\, Q(x,y)$, con Q decidibile e $x \notin A \iff \exists y\, R(x,y)$, con R decidibile.
Si definisca ora $T(x) = \mu y\, [Q(x,y) \vee R(x,y)]$, che termina sempre in quanto $x \in A \vee x \notin A$, ed è μ-calcolabile. (← in pratica voglio il minimo tempo per cui ho Q o R)
Dunque $x \in A \iff Q(x, T(x))$ e $x \notin A \iff \neg Q(x, T(x)) \iff R(x, T(x))$.
Quindi A è decidibile

oss Facciamo un piccolo cenno su ciò che si vedrà in seguito

Sia T una teoria ricorsivamente assiomatizzata

$\{\varphi \mid T \vdash \varphi\} = \{\varphi \mid \exists d\, \underbrace{T \vdash_d \varphi}_{\text{ricorsivo}}\}$ è ricorsivamente enumerabile

Se però la teoria è completa, allora $\{\varphi \mid T \vdash \varphi\}$ è ricorsivo.

oss Riguardo al teorema di Post, vale anche il viceversa.

Teorema $A \subseteq \mathbb{N}$ ricorsivamente enumerabile $\Leftrightarrow \exists f$ ricorsiva (parziale) tale che $A = \text{dom } f$.

Dim

$\Rightarrow$

$A = \{x \mid \exists y\ Q(x,y)\}$, con Q decidibile.
Definendo f in modo che $f(x) = \mu y\, Q(x,y)$, si ha che questa è la funzione richiesta (in quanto si ferma proprio su A).

$\Leftarrow$

Si considera $\mathcal{Q}$ l'aritmetica di Robinson

Def $A \subseteq \mathbb{N}^k$ si dice binumerabile in $\mathcal{Q}$ se esiste $\varphi(x_1, \dots, x_n)$ formula in $\mathcal{L} = \{0, S, +, \cdot\}$ tale che

- $\langle a_1, \dots, a_k \rangle \in A \Rightarrow \mathcal{Q} \vdash \varphi(a_1, \dots, a_k)$
- $(a_1, \dots, a_k) \notin A \rightarrow \mathcal{Q} \vdash \neg\varphi(a_1, \dots, a_k)$

~~Teorema~~ ~~Sia $A \subseteq \mathbb{N}^k$ ricorsiva allora~~

Lemma Se t_1 e t_2 sono termini chiusi, allora $\mathcal{Q} \vdash t_1 = t_2$ o $\mathcal{Q} \vdash \neg(t_1 = t_2)$

~~Lemma~~

Prop Siano $a, b, c \in \mathbb{N}$ tale che $a + b = c$. Allora $\mathcal{Q} \vdash \underline{a} + \underline{b} = \underline{c}$

Dim

Applico l'induzione su b

- $b = 0$, quindi $a = c$

  $\mathcal{Q} \vdash \underline{a} = \underline{c}$ in quanto $\mathcal{Q} \vdash t = t$

- $b > 0$ $\quad a + b = c \Rightarrow a + (b-1) = (c-1)$

  Per ip induttiva $\mathcal{Q} \vdash \underline{a} + \underline{b-1} = \underline{c-1} \Rightarrow$

  $\Rightarrow \mathcal{Q} \vdash S(\underline{a} + \underline{b-1}) = S(\underline{c-1})$ (in quanto ogni teorema $\vdash x = y \rightarrow f(x) = f(y)$
  $\Rightarrow \mathcal{Q} \vdash \underline{a} + S(\underline{b-1}) = \underline{c} \Rightarrow$
  $\Rightarrow \mathcal{Q} \vdash \underline{a} + \underline{b} = \underline{c}$

Prop Siano $a, b, c \in \mathbb{N}$ tali che $a \cdot b = c$. Allora $\mathcal{Q} \vdash \underline{a} \cdot \underline{b} = \underline{c}$

Dim

Induzione su b.

- $b = 0$, quindi $c = 0$

  $\mathcal{Q} \vdash \underline{a} \cdot \underline{0} = \underline{0}$

- $b > 0$ ~~enumerazione~~ (si sfrutta $\mathcal{Q} \vdash x \cdot 0 = 0$, $\mathcal{Q} \vdash x \cdot Sy = xy + x$ e la prop precedente) (esercizio).

Prop Per ogni termine t, $\exists u$ t.c. $Q \vdash t = \underline{u}$ vedi dispense

Prop $a \neq b \Rightarrow Q \vdash \underline{a} \neq \underline{b}$

Dim

- $a < b$
  - $a = 0$ $\quad Q \vdash \underline{0} \neq S(x) \Rightarrow Q \vdash \underline{0} \neq \underline{b}$
  - $a > 0$ $\quad a-1 \neq b-1$

    $Q \vdash \underline{a-1} \neq \underline{b-1} \Rightarrow Q \vdash \underline{a} = \underline{b}$

Dim lemma vedi dispense

Def $x \leq y \iff \exists z\ (z + x = y)$ e $x < y \iff x \leq y \wedge x \neq y$

oss Sicuramente $Q \vdash \forall xy\ (x \leq y \vee y \leq x)$

oss Se $M \models Q$, $(\mathbb{N}, 0, S, +, \cdot)$ è isomorfo a una sottostruttura di M.
(quindi c'è una funzione iniettiva da $\mathbb{N}$ in M)

Prop $u \in \mathbb{N}$ $\quad Q \vdash \forall x\ (x \leq u \iff x = \underline{0} \vee \dots \vee x = \underline{u})$

Dim

Induzione su u.

Sia x in $M \models Q$. Si suppone $x \leq \underline{u}$

- $u = 0$ quindi $x \leq \underline{0}$

  $\exists z\ z + x = \underline{0}$ se per assurdo $x \neq \underline{0}$ allora $\exists y\ x = S(y)$
  Quindi $z + S(y) = \underline{0} \Rightarrow S(z+y) = \underline{0}$, assurdo.

- $u > 0$

  Sia $x < \underline{u} \Rightarrow \exists z\ z + x = \underline{u}$

  - se $x = \underline{0}$ ho finito
  - se $x \neq \underline{0}$ allora $\exists y\ x = S(y)$

    $z + S(y) = \underline{u} \Rightarrow S(z+y) = \underline{u} \Rightarrow z + y = \underline{u-1} \Rightarrow$
    $\Rightarrow y \leq \underline{u-1} \underset{\text{ind}}{\Rightarrow} y = \underline{0} \vee \dots \vee y = \underline{u-1} \Rightarrow x = \underline{1} \vee \dots \vee x = \underline{u}$

Prop $n \in \mathbb{N}$. Sono equivalenti:

1. $\forall a \leq n$ $\quad Q \vdash \varphi(\underline{a})$
2. $Q \vdash \forall x \leq \underline{n}\ \varphi(x)$

21/11/2017

BERARDUCCI
TEORIA

Si ricordi che l'altra volta si è dimostrato che

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

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

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

oss Il secondo corollario implica il primo e non viceversa.

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

Dim
Si applichi l'induzione su b (in metateoria)
vedere dispense

Prop $\forall x \leq n\ Q \vdash \varphi(x) \iff Q \vdash \forall x \leq \underline{n}\ \varphi(x)$

oss La proposizione vale analogamente per '$\exists x \leq n$'

Dim
È un corollario del teorema ricordato all'inizio

Corollario
$Q \vdash [\forall x \leq \underline{n}\ \varphi(x)] \iff [\varphi(0) \wedge \dots \wedge \varphi(n)]$
$Q \vdash [\exists x \leq \underline{n}\ \varphi(x)] \iff [\varphi(0) \vee \dots \vee \varphi(n)]$

È dunque possibile definire una nuova classe di formule Δ_0 in maniera induttiva nel modo seguente

$$\Delta_0 = \text{Atomiche} \mid \neg\Delta_0 \mid \Delta_0 \wedge \Delta_0 \mid \Delta_0 \vee \Delta_0 \mid \forall x \leq t\ \Delta_0 \mid \exists x \leq t\ \Delta_0$$

Teorema Se $\varphi \in \Delta_0$ è chiusa, allora esiste φ^* senza quantificatori $\forall, \exists$ tale che $Q \vdash \varphi \iff \varphi^*$

oss Intuitivamente, quindi per formule chiuse, è possibile, grazie ai corollari, togliere i quantificatori

Esempio Nella formula $\forall x \leq y\ \varphi(x)$ non è possibile togliere i quantificatori in quanto non è una formula chiusa (y è libera)

Esempio $\forall x \leq 3+3\ \underbrace{\exists y \leq x\ \varphi(x,y)}_{\theta(x)} = \phi$

È possibile scrivere, partendo dall'esterno

$$\phi(x,y) \equiv \bigwedge_{a=0}^{6} \theta(\underline{a}) \equiv \bigwedge_{a=0}^{6} \bigvee_{b=0}^{a} \varphi(\underline{a},\underline{b})$$

Alternativamente, era possibile dimostrarlo formalmente per induzione su φ

- $\varphi = \alpha \wedge \beta$, allora si considera $\varphi^* = \alpha^* \wedge \beta^*$
- $\varphi = \exists x \leq t\ \theta(x)$, allora $\varphi^* \equiv \bigvee_{a \leq n} \theta^*(\underline{a})$ (per ip induttiva $\theta(\underline{a}) \iff \theta^*(\underline{a})$)

Esempio x è primo $\leftrightarrow (\forall a,b \leq x)[a \cdot b = x \wedge x \neq 1] \rightarrow a=1 \vee b=1 \quad \in \Delta_0$

Def Dato $A \subseteq \mathbb{N}$, si pone $A \in \Delta_0^{\mathbb{N}}$ se $A = \{a \mid \mathbb{N} \models \varphi(a)\}$

oss Si vedrà che $\Delta_0^{\mathbb{N}} \subseteq RIC$

Prop $\varphi \in \Delta_0$ chiusa $\Rightarrow Q \vdash \varphi$ o $Q \vdash \neg\varphi$

Dim
$Q \vdash \varphi \leftrightarrow \varphi^*$, con φ^* chiusa senza quantificatori
Ma allora φ^* è formata da formule atomiche unite con connettivi booleani.
Inoltre se una formula è decidibile in Q allora le decide anche in combinazioni tramite connettivi booleani
Ma visto che Q decide le atomiche (in quanto solo solo del tipo $t_1 = t_2$ poiché non ci sono simboli di predicato), per induzione si ha che φ^* è decidibile in Q e dunque lo è φ.

Ricordando che $\mathcal{L} = \{0, 1, +, \cdot\}$ e $x \leq y \equiv \exists z\,(z + x = y)$ e $\exists x \leq t\ \varphi \equiv \exists x (x \leq t \wedge \varphi)$
si definisce una nuova classe di funzioni in modo induttivo:

$$\Sigma_1^0 = \Delta_0 \mid \Sigma_1^0 \wedge \Sigma_1^0 \mid \Sigma_1^0 \vee \Sigma_1^0 \mid (\forall x \leq t)\,\Sigma_1^0 \mid \exists x\,(\Sigma_1^0)$$

oss Quindi si considerano solo le combinazioni positive di Σ_1^0
(le negazioni si accettano solo se erano già in partenza in Δ_0)

Teorema A è Σ_1^0-definibile in $\mathbb{N}$ (cioè $A = \{a \mid \mathbb{N} \models \varphi(a)\}$, con $\varphi \in \Sigma_1^0$) $\Leftrightarrow$ A è ricorsivamente enum.

Dim

oss Si ha $\Delta_0^{\mathbb{N}} \subsetneq$ Prim ric $\subsetneq RIC$, mentre se si mette $\forall$ esiste si ha

$$\forall \Sigma_1^{0\,\mathbb{N}} = \exists \Delta_0^{\mathbb{N}} = \exists \text{ Prim ric} = \exists RIC = RE$$

Per il teorema di Post si ha $RIC = \underbrace{\Sigma_1^{0\,\mathbb{N}}}_{\text{RE}} \cap \underbrace{\neg\Sigma_1^{0\,\mathbb{N}}}_{\text{co RE}}$

Prop Se $\varphi \in \Sigma_1^0$ chiusa, $\mathbb{N} \models \varphi \Rightarrow Q \vdash \varphi$

Gödel ha dimostrato che esiste φ vera in $\mathbb{N}$, ma non dimostrabile in PA né in ZF.

oss ~~Dimostrare la congettura di Goldbach~~.

Def φ è indecidibile in T se $T \nvdash \varphi$ e $T \nvdash \neg\varphi$.

oss Se Goldbach fosse indecidibile in PA allora sarebbe vera (in $\mathbb{N}$) (esercizio)

Infatti se fosse falso, sarebbe vera la negazione, cioè

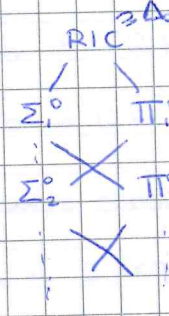
$$\neg(\forall x\ (x \text{ pari} > 2 \rightarrow \underbrace{\exists a,b \leq x \text{ primi } x = a+b}_{\Delta_0}) =$$

$$= \underbrace{\exists x}_{\Sigma_1^0}\ (x \text{ pari} > 2 \wedge \underbrace{(\forall a,b \leq x \text{ primi } x \neq a+b}_{\Delta_0})$$

Quindi $\neg$ Gold $\in \Sigma_1^0$, quindi sarebbe decidibile in Q.

oss Quindi Goldbach non può essere la φ ~~dell~~ di Gödel, ma servirebbe qualcosa di complessità superiore

oss È possibile ampliare la gerarchia della complessità



$\Pi_1^0 = \neg\Sigma_1^0$ $\quad (\Delta_0 \mid \vee \mid \wedge \mid \forall \mid \exists x \leq t)$

$\Pi_2^0 = \forall\Sigma_1^0 = \forall\exists$ RIC

$\Sigma_2^0 = \exists\Pi_1^0 = \exists\forall$ RIC

Esempio La congettura ~~che~~ per cui esistono infiniti primi gemelli, cioè

$$(\forall n)(\exists a \geq n)\ \underbrace{(a \text{ è primo} \wedge a+2 \text{ è primo})}_{\Delta_0}$$

è di complessità Π_2^0.

Si è visto che se f, g sono primitive ricorsive, allora $f \circ g$ è primitiva ricorsiva.
Non è vero però che se $f, g \in \Delta_0^{\mathbb{N}}$, allora $f \circ g \in \Delta_0^{\mathbb{N}}$.

Ad esempio, della $h = f \circ g$, $h(x) = y \Leftrightarrow \exists z\ (\underbrace{g(x) = z}_{\Delta_0} \wedge \underbrace{f(z) = y}_{\Delta_0})$
dove c'è $\exists z$ che non la rende Δ_0.

Teorema Una funzione f è μ-ricorsiva $\Leftrightarrow$ f è Σ_1^0-definibile in $\mathbb{N}$.

Dim
Le funzioni μ-ricorsive sono quelle ottenibili dalle funzioni base $0, S$, la proiezione Π dalla composizione, ricorsione primitiva e minimalizzazione.
Si deve vedere, quindi, che il grafico di queste funzioni sta in Σ_1^0.

$\Gamma(0) = \{y \mid \overbrace{y = 0}^{\Sigma_1^0}\}$ $\qquad$ $\Gamma(S) = \{(x,y) \mid \overbrace{y = S(x)}^{\text{Atomica}}\}$

$\Gamma(\Pi_i^n) = \{(x_1, \dots, x_n) \mid y = x_i\}$
$\varphi(x_1, \dots, x_n, y) \equiv y = x_i$

La composizione di ~~formule~~ Σ_1^0, inoltre, è Σ_1^0

Rimangono quindi la ricorsione primitiva e la minimalizzazione.

- Supponiamo che g, h Σ_1^0-definibili in $\mathbb{N}$ da φ_g e φ_h e sia f tale che

$$f(\bar{x}, 0) = g(\bar{x})$$
$$f(\bar{x}, y+1) = h(\bar{x}, y, f(\bar{x}, y))$$

$$f(\bar{x}, y) = z \Leftrightarrow \exists c,d\ \beta(c,d,0) = g(x) \wedge \beta(c,d,y) = z \Leftrightarrow$$
$$\Leftrightarrow \exists c,d\ [\exists u\ \overbrace{\underbrace{u = \beta(c,d,0)}_{\varphi_g(x,u)} \wedge u \neq g(x)}^{\Delta_0}\ \text{etc.}\ ]$$

Quindi alla fine f è Σ_1^0-definibile.

- Supponiamo che $f(\bar{x}) = \mu y\, h(\bar{x}, y) = 0$, con $\varphi_h(\bar{x}, y, z) \in \Sigma_1^0$
(cioè $h(a,b)=c \Leftrightarrow \mathbb{N} \models \varphi(a,b,c)$)

$f(x) = y \Leftrightarrow h(x,y) = 0 \wedge \forall i < y\ \exists u\ (u \neq 0 \wedge h(x,i) = u) \Leftrightarrow$

$\Leftrightarrow \mathbb{N} \models \varphi_h(x,y,0) \wedge \forall i \underset{\mathbb{N}}{<} y\ \exists u \underset{\mathbb{N}}{\in} \mathbb{N}\ (u \neq 0 \wedge \mathbb{N} \models \varphi_h(x,i,u)) \Leftrightarrow$

$\Leftrightarrow \mathbb{N} \models [\varphi_h(x,y,0) \wedge \forall i < y\ \exists u\ (u \neq 0 \wedge \varphi_h(x,i,u))] \in \Sigma_1^0$

↑ per semantica di Tarski, la $\mathbb{N}$ bonariamente esce fuori