(95) Teorema cinese del resto.

$$\exists x : \begin{cases} MCD(a_i, a_j) = 1 \quad \forall i \neq j \\ x \equiv b_1 \ (a_1) \\ \vdots \\ x \equiv b_k \ (a_k) \end{cases}$$

Da x ricavo $b_1, \dots, b_k$ (se $b_i < a_i$)

Lemma $\forall n, x \ \exists d > x$ tale che $a_1 = d+1 \quad a_n = nd+1$ sono relativamente primi

Infatti $d = (\max(n, x)+1)!$

Lemma $\forall n \ \forall b_1 \dots b_n \in \mathbb{N} \ \exists c, d$
$\exists \beta : \mathbb{N}^3 \to \mathbb{N}$ definibile con $+, \cdot$
tale che $\beta(c, d, i) = b_i \quad i = 1 \dots n$.

$$\beta(c, d, i) = \text{resto } \frac{c}{(i+1)d+1}$$

23 novembre 2007

(Appunti sui calcolabilità e Gödel, 20/V/2002)

Codifica successioni finite di interi

$$\langle a_0, \dots, a_n \rangle \longmapsto \prod_{i=0}^{n} p_i^{a_i+1}$$

Codifica coppie : $\mathbb{N}^2 \to \mathbb{N}$

$$\mathbb{N} \ni \langle x, y \rangle \begin{cases} (x,y) \longmapsto \frac{(x+y)(x+y+1)}{2} + x \\ (x,y) \longmapsto 2^y(2x+1) - 1 \\ (x,y) \longmapsto 2^{x+1} 3^{y+1} \end{cases}$$

sono PR

96 Esercizio. Successione di Fibonacci è PR.

$$f(0)=1 \quad f(1)=1 \quad f(n+2)=f(n+1)+f(n)$$

$$F(n)=\langle f(n), f(n+1)\rangle \in \mathbb{N}$$

$F(0)=\langle 1,1\rangle$ codificato con una delle codifiche di sopra

$$F(n+1)=\langle f(n+1), f(n+2)\rangle = \langle f(n+1), f(n+1)+f(n)\rangle$$

$$p_0(n)=\mu x\le n\ \exists y\le n \quad n=\langle x,y\rangle$$

Indipendentemente dalle codifiche, le proiezioni sono PR.

$$=\langle p_1(F(n)), p_1(F(n))+p_0(F(n))\rangle = h(F(n))$$

$$F \text{ è } PR \Rightarrow f(n)=p_0(F(n))$$

In generale: $f(x)=h(x,\langle f(0),\dots,f(x-1)\rangle)=$

$$h:\mathbb{N}^2\to\mathbb{N}$$

$$=h(x,\prod_{i<x} p_i^{f(i)+1})$$

$f(0)=h(x,\langle\ \rangle)$ successione vuota.

$$\boxed{h \text{ PR} \Rightarrow f \text{ PR}}$$

Infatti: $f^{\#}(x)=\langle f(0),\dots,f(x-1)\rangle$

$\# =$ sharp

$$f(x)=h(x, f^{\#}(x))$$

$f^{\#}$ è PR: $f^{\#}(0)=\langle\ \rangle$

(9)

$$f^{\#}(x+1) = \langle f0, \ldots, fx \rangle =$$

$$= cat(\langle f0, \ldots, f(x-1) \rangle, \langle f(x) \rangle) =$$

$$= cat(f^{\#}(x), \langle h(x, f^{\#}(x)) \rangle) =$$

$$= H(x, f^{\#}(x))$$

Alcune ricursioni non sono PR.

Esempio. Funzione di Ackermann:

$$A(x+1, y+1) = A(x, A(x+1, y))$$

$$A(x+1, 0) = A(x, 1)$$
$$A(0, y) = S(y)$$

$A: N^2 \to N$

Per induzione su $\omega x + y$
si dimostra $A(x,y)\downarrow$, cioè
è ben definita.

$A(5,5)$ è un numero astronomico

A è μ-calcolabile totale non PR.

Per la tesi di Church dovrebbe
essere μcalcolabile.

Esercizio. A è μ-calcolabile. $G_A \subset N^3$
G_A = grafico di A

$$\langle x, y, z \rangle \in G_A \Leftrightarrow A(x,y) = z$$

$$\langle x+1, y, z \rangle \in G_A \wedge \langle x, y, z \rangle \in G_A$$
$$\Downarrow$$
$$\langle x+1, y+1, w \rangle \in G_A$$

93

$\langle x, 1, z\rangle \in G_A \Rightarrow \langle x+1, 0, z\rangle \in G_A$

$\langle 0, y, S(y)\rangle \in G_A$

$\langle \langle a, b, c\rangle, \langle u, v, z\rangle, \langle \ , \ , \ \rangle, \ldots \rangle$

Z è una computazione di $\langle x, y, z\rangle$ se è una successione finita di terne contenente $\langle x, y, z\rangle$ e tale che $\forall \langle a, b, c\rangle$ in Z
o $\langle a, b, c\rangle = \langle 0, y, Sy\rangle$ $\exists y$ (è un assioma)
o $\langle a, b, c\rangle$ si deduce da altre terne in Z

$A(2,1) = A(1, A(1,1))$
$A(1,1) = A(0, A(1,0))$
$A(1,0) = A(0,1)$
$A(0,1) = 2$

$\langle 012\rangle, \langle 102\rangle, \ldots$

$A(x,y) = z \Leftrightarrow \exists c$ (c è una computazione e $estrai(c, lh(c)) = \langle xyz\rangle$)

Teorema. Una funzione $f: N^k \to N$ parziale è μ-ricorsiva se e solo se $G(f)$ è RE.

$(f\vec{x} = y) \Leftrightarrow (\vec{x}, y) \in G(f) \Leftrightarrow \exists c\ R(c, \vec{x}, y)$

$f(\vec{x}) = p_0(\mu \langle y, e\rangle : R(e, \vec{x}, y)) =$

$= \underbrace{p_0}_{PR}(\mu n \underbrace{R(p_1(n), x, p_0(n))}_{PR})$

β di Gödel. $\beta(c,d,i) = \frac{c}{(i+1)d+1}$

$$\beta(c,d,i)=r \iff \exists q\le c\,[c=q[(i+1)d+1]+r \wedge r<(i+1)d+1]$$

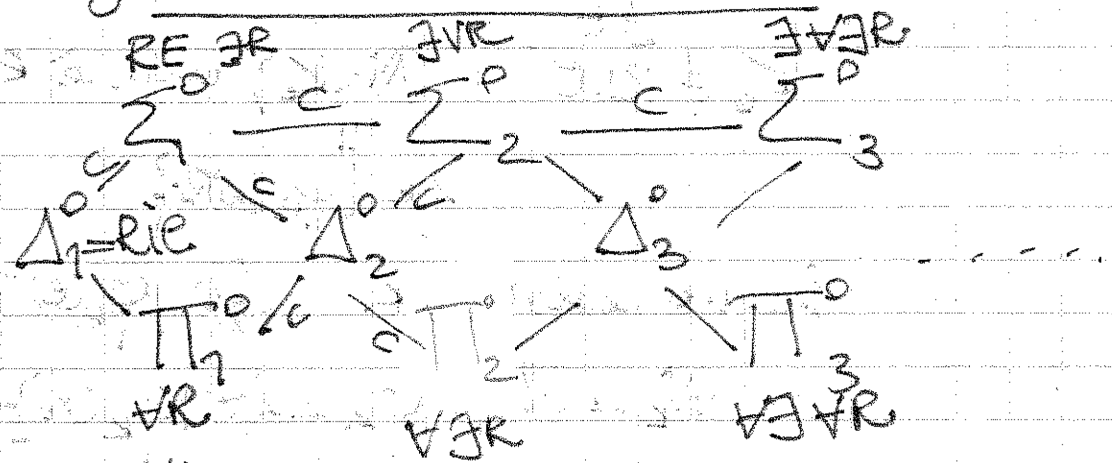
Δ^0 è PR

$\forall n\ \forall b_1,\dots,b_n\ \exists c,d$

$\beta(c,d,0)=b_0,\dots,\beta(c,d,n)=b_n$

Infatti: dati $b_0,\dots,b_n$ scelgo d tale che $d+1, 2d+1, \dots, nd+1$ sono relativamente primi. Scelgo $c \equiv b_i\ ((i+1)d+1)$

Gerarchie aritmetiche



$A\subseteq \mathbb{N}^k$

$A=\{\vec{x} \mid \exists y_1\ \forall y_2\ \exists y_3\ \forall y_4 \dots R(\vec{x},\vec{y})\}$

$Q_1y_1 \dots Q_ny_n$.

$\Sigma^0_n=\exists\Pi^0_{n-1}$

$\Pi^0_n=\forall\Sigma^0_{n-1}$

Un insieme $A\subseteq\mathbb{N}$ è aritmetico se $\exists n\,(A\in\Sigma^0_n)$

(100) $\bigcup_n \Sigma^0_n = \bigcup_n \Pi^0_n$ = aritmetici

$\shortparallel$

insiemi definibili in $(\mathbb{N}, +, \cdot; S, 0)$ } Teorema

$\shortparallel$

$\bigcup_n \Sigma^0_n = \bigcup_n \Pi^0_n$ }

Barda direzione: ricorsivo finito

Esempio $\{e \mid \varphi_e$ è totale$\}$ cioè $\forall x \exists t \; \underbrace{\varphi_e(x)\downarrow t}$

$K_0 = \{e \mid \varphi_e(e)\downarrow\} \in \Sigma^0_1$; RE

$\exists t \, \varphi_e(e)\downarrow t$

Problema della fermata

$K_0 \notin$ RIC $\quad (\mathbb{N} \setminus K_0)$ non è RIC

$\shortparallel$

$\{e \mid \varphi_e(e)\uparrow\}$

Se no esiste K $\{e \mid \varphi_e(e)\uparrow\} = W_K$

$W_K = \mathrm{dom}\,\varphi_K = \{x \mid \varphi_K(x)\downarrow\}$

$x \in K_0 \Leftrightarrow x \in W_K \quad \forall x$

$x \notin K_0 \Leftrightarrow x \in W_K$ Assurdo.

TOT $= \{e \mid \varphi_e$ è totale$\} \in \Pi^0_2 \setminus \Sigma^0_1$

Infatti: se fosse RE allora TOT $=$ Im(h) con h totale ric.

$\Rightarrow \{\varphi_{h(n)} \mid n \in \mathbb{N}\}$ = funzioni ricorsive totali.

$e \in$ TOT $\Rightarrow \exists n \quad e = h(n) \to \varphi_e = \varphi_{h(n)}$

(10) $D(x) = \varphi_{h(x)}(x)+1$ (diagonale) è totale

e ricorsiva $D = \varphi_{h(a)}$

$D(a) = \varphi_{h(a)}(a)$

$= \varphi_{h(a)}(a)+1$ Assurdo.

Possiamo codificare i poliedri.

$\{\ulcorner p \urcorner \mid p \underset{T}{\simeq} \text{sfera}\}$ non è un insieme aritmetico.

omeomorfo

$A \subset \mathbb{N}^2$ e RE se i poliedri sono tridimensionali

$\{(\ulcorner p_1 \urcorner, \ulcorner p_2 \urcorner) \mid p_1 \simeq p_2\}$

Gli insiemi che appartengono alla gerarchia aritmetica sono numerabili.

Tutti gli insiemi della gerarchia aritmetica sono definibili.

$f(\vec{x}, 0) = g(\vec{x})$

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

g, h definibili in $(\mathbb{N}, +, \cdot) \Rightarrow$ anche f lo è.

$f(\vec{x}, y) = z \iff \exists \langle a_0, \ldots, a_y \rangle$ tale che

$a_0 = g(\vec{x})$
$a_y = z$
$a_{i+1} = h(\vec{x}, i, a_i) \quad \forall i < y$

(102) In maniera equivalente

$\exists c, d$ tali che $\beta(c,d,0) = g(\vec{x})$

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

$\beta(c,d,i+1) = h(\vec{x}, i, \beta(c,d,i))$

$\forall i < y$

28 novembre 2007

Teoria Q di Robinson.

(Peano = Q + induzione)(schema)

$Sx = Sy \Rightarrow x = y$

$y \neq 0 \Rightarrow \exists x \; Sx = y$

$Sx \neq 0$

$x + 0 = x$

$x + Sy = S(x+y)$

$x \cdot 0 = 0$

$x \cdot Sy = xy + x$

$2^x \quad \varphi(x,y) \qquad \mathbb{N} \models \varphi(a,b) \Leftrightarrow 2^a = b$

$PA \vdash \varphi(a,b) \Leftrightarrow 2^a = b$

$Q \vdash \varphi(a,b) \Leftrightarrow 2^a = b$

$2^a = b \Rightarrow Q \vdash \varphi(a,b) \Rightarrow PA \vdash \varphi(a,b) \Rightarrow \mathbb{N} \models \varphi(a,b)$

$f : \mathbb{N} \to \mathbb{N}$ è binumerabile in Q

se esiste $\varphi(x_1 \ldots x_n, y)$ tale che

$fa = b \Rightarrow Q \vdash \varphi(S^a 0, S^b 0)$

e

$fa \neq b \Rightarrow Q \vdash \neg\varphi(S^a 0, S^b 0)$

f binumerabile in Q

$\Downarrow$

in PA

$\Downarrow$

$Th(\mathbb{N})$

$\varphi(x,y) \quad 2^x = y$

$Q \vdash \varphi(S^3 0, S^8 0)$

$PA \vdash \forall x \; \underbrace{2^{x+1}}_{y} = \underbrace{2^x}_{z} \cdot 2$

$PA \vdash \forall x \; \varphi(x,z) \to \varphi(x+1, z+z)$

$Q \nvdash$

Teorema Se $f : \mathbb{N}^k \to \mathbb{N}$ è ricorsiva totale allora f è rappresentabile funzionalmente in Q:
c'è $\varphi(\vec{x}, y)$ tale che $\quad (\underline{a} = S^a 0)$
$fa = b \Rightarrow Q \vdash \varphi(\underline{a}, \underline{b}) \quad (k=1)$
$fa \neq b \Rightarrow Q \vdash \neg\varphi(\underline{a}, \underline{b})$
$\forall a \in \mathbb{N} \; Q \vdash \exists! y \, \varphi(\underline{a}, y)$

$fa = b \Rightarrow Q \vdash \forall x (\varphi(\underline{a}, x) \leftrightarrow x = \underline{b})$

$M \models Q \quad \{(a,b) \in M^2 \mid M \models \varphi(a,b)\}$

$f : M \to M$

Osservazione Le funzioni rappresentabili funzionalmente sono chiuse per composizione (e per ricorsione primitiva).
Infatti: $h = f \circ g$ unarie

$\varphi_f(x,y) \quad \varphi_g(x,y)$

$hx = y \leftrightarrow \exists z (gx = z \wedge fz = y)$

$\varphi_h(x,y) = \exists z (\varphi_g(x,z) \wedge \varphi_f(z,y))$

$ha = b \leftrightarrow Q \vdash \forall x [\varphi_h(\underline{a}, x) \leftrightarrow x = \underline{b}]$

Siamo interessati ad insiemi particolari

(104) $n \in \mathbb{N}$ $\quad \underline{n} = S^n 0 = SSS\ldots S0$

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

$$Q \vdash x+0=x$$

$$Q \vdash x+Sy = S(x+y)$$

$$\underline{a}+\underline{b+1} = \underline{a}+S\underline{b} = S(\underline{a}+\underline{b}) =$$

$$\underset{\uparrow}{=} S(\underline{a+b}) = \underline{a+b+1}$$

ipotesi induttiva

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

$$Q \vdash S^a 0 \cdot S^b 0 = S^{a\cdot b}(0)$$

Vogliamo dimostrare $\varphi \in \Delta_0$ chiuse

$$\Downarrow$$

$$Q \vdash \varphi \text{ o } Q \vdash \neg\varphi$$

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

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

$$a = k+n \quad b = k$$

$$\underbrace{S^k S^n 0}_{\underline{a}} = \underbrace{S^k 0}_{\underline{b}}$$

$$\downarrow Q$$

$$S^n 0 = 0$$

Assurdo

(105) t termine chiuso allora $\exists\, n \in \mathbb{N}$
tale che $Q \vdash t = S^n(0)$

Esempio $t = (SSO + SO)\, SSO$
$t = t_1 + t_2$

$$Q \vdash t_1 = \underline{n}_1 \quad Q_2 \vdash t_2 = \underline{n}_2$$

$$Q \vdash \underline{n}_1 + \underline{n}_2 = \underline{n_1 + n_2}$$

Se t_1, t_2 sono termini chiusi

$$\mathbb{N} \models t_1 = t_2 \Rightarrow Q \vdash t_1 = t_2$$

$$t_1 \neq t_2 \Rightarrow Q \vdash \neg(t_1 = t_2)$$

Teorema: $\varphi \in \Delta_0$ chiusa $\Rightarrow Q \vdash \varphi$ o $Q \vdash \neg\varphi$

Δ_0 = Atomiche (definite per induzione)

oppure
$\Delta_0 \wedge \Delta_0$
oppure
$\Delta_0 \vee \Delta_0$

$\neg \Delta_0$

$\forall x \leq y\, \Delta_0 \quad \exists x \leq y\, \Delta_0$

Se $\alpha \vee \beta$ abbiamo quattro casi da controllare:

$$\begin{cases} Q \vdash \alpha \text{ e } Q \vdash \beta \\ Q \vdash \neg\alpha \text{ e } Q \vdash \beta \\ Q \vdash \alpha \text{ e } Q \vdash \neg\beta \\ Q \vdash \neg\alpha \text{ e } Q \vdash \neg\beta \end{cases}$$

$x \leq y \Leftrightarrow \exists z\,(z+x = y)$

(Q non dimostra che $\leq$ è un ordine: la dimostra solo rispetto agli elementi standard)

$\forall x \leq y\ \varphi \equiv \forall x\,(x \leq y \to \varphi)$

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

$n = 0$, ovvero $x \leq \underline{0}$ $\exists z$ $z + x = 0$

se $x \neq 0$ allora $x = Sy$

$z + Sy = 0 \Rightarrow S(z+y)$ Assurdo

$n+1$: in Q $x \leq \underline{n+1} = S(\underline{n})$

$z + x = \underline{n+1}$

se $x = 0$ ok

se no $x = Sy$ $\underset{\shortparallel}{z+Sy} = n+1$

$S(z+y) \Rightarrow z + y = n$

$\Rightarrow y < n$

$y = \underline{0} \vee \ldots \vee y = \underline{n}$

$x = \underline{1} \vee \ldots \vee x = \underline{n+1}$

$Q \vdash \forall x \leq \underline{n}\ \varphi(x) \leftrightarrow \varphi(\underline{0}) \wedge \ldots \wedge \varphi(\underline{n})$

$\exists x \leq \underline{n}\ \varphi(x) \leftrightarrow \varphi(\underline{0}) \vee \ldots \vee \varphi(\underline{n})$

cioè i quantificatori limitati si possono eliminare.

Corollario. Ogni $\varphi \in \Delta_0$ equivale in Q a una ψ senza quantificatori.

corollario. $\forall\varphi\in\Delta_0$ $Q\vdash\varphi$ o $Q\vdash\neg\varphi$. $\square$

$\beta : \mathbb{N}^3 \to \mathbb{N}$ $\quad \beta(c,d,i) = \text{Resto}\ \dfrac{c}{d(i+1)+1}$

β è Δ_0 $\quad$ Resto$(x,y) = z$ vuol dire che
$\exists q \leq x\ (x = yq + z \wedge 0 \leq z < y)$

β è rappresentata in Q funzionalmente
cioè $\forall a,b \in \mathbb{N}$
$Q \vdash \exists! z\ \text{Resto}(\underline{a},\underline{b}) = z$
(il resto è forzato ad essere standard).

$\forall a_0 \ldots a_n\ \exists c,d\ \ \beta(c,d,0)=a_0 \wedge \ldots \wedge \beta(c,d,n)=a_n$

$Q \vdash \varphi_\beta(\underline{c},\underline{d},\underline{0},\underline{a_0}) \vee \ldots$

PA oltre a dimostrare le cose che dimostra Q dimostra anche

$$\forall c,d,i,a\ \exists c',d'\ \ \forall j \neq i$$
$$\beta(c',d',j) = \beta(c,d,j)$$
$$\beta(c,d,i) = a$$

Questo implica che si possono codificare successioni di lunghezze non standard.

Le successioni codificate sono chiuse per aggiunta di un elemento (in pratica si può codificare tutto)

(108) 30 novembre 2007

Teorema $f: \mathbb{N}^k \to \mathbb{N}$ μ-ricorsiva (= calcolabili) totali ⇒ f è rappresentabile in Q — funzionalmente

cioè esiste una formula $\varphi_f(x_1 \dots x_k, y)$ tale che

1) $f(a_1 \dots a_k) = b \Rightarrow Q \vdash \varphi_f(\underline{a_1} \dots \underline{a_k}, \underline{b})$

2) $\Rightarrow Q \vdash \neg \dots$

3) $f(\vec{a}) = b \qquad \Rightarrow Q \vdash \forall y [\varphi_f(\underline{a_1} \dots \underline{a_k}, y) \leftrightarrow y = \underline{b}]$

Ricorsione primitiva

$$f(x,0) = g(x)$$
$$f(x,n+1) = h(x,n,f(x,n))$$
$$x = (x_1 \dots x_k)$$

β di Gödel $\forall a_0 \dots a_n \exists c,d \ \beta(c,d,0) = a_0$

$\beta(c,d,n) = a_n$

β è rappresentabile funzionalmente in Q.

$f(x,y) = z \Leftrightarrow \exists c,d$ tali che $\beta(c,d,0) = g(x)$ e

$\forall i < y, \ \beta(c,d,i+1) = h(x,i,\beta(c,d,i))$

L'idea è che $\beta(c,d,i) = f(x,i)$

$\beta(c,d,0) = g(x) \rightarrow \varphi_g(x, \beta(c,d,0))$

$\exists z [\varphi_g(c,d,0,z) \wedge \varphi_g(x,z)]$

Siano $\varphi_g, \varphi_h \in \exists\Delta_0$ per ipotesi induttiva

(109) ($\exists\Delta_0$ → chiuse per $\exists$, $\forall i<y$, $\wedge$, $\vee$)

φ_f è $\exists\Delta_0$ nel senso esteso

Teorema (Matijasevič):
$$f(x)=y \Leftrightarrow \exists \vec{z}\ p(x,y,\vec{z})=0$$
(Robinson, Davis, Putnam).

$$(p_1=0 \wedge p_2=0) \longleftrightarrow p_1^2+p_2^2=0$$

$$(p_1=0 \vee p_2=0) \longleftrightarrow p_1 p_2=0$$

$$p_1\neq 0 \leftrightarrow \exists w \quad p_1 w=1$$

Problema delle fermate
(10 problema di Hilbert:

$$K=\{(x,y)\mid \varphi_x(y)\downarrow\}=$$

$$=\{(x,y)\mid \exists t\ \underbrace{\varphi_x(y)\downarrow_t}_{\text{è ricorsivo}}\}=$$

$$=\{(x,y)\mid \exists t\ \exists \vec{z}\ p(x,y,t,\vec{z})=0\}$$

(*) $f(a)=b \Rightarrow Q\vdash \varphi_f(\underline{a},\underline{b})$

(**) $\qquad Q\vdash \forall y[\varphi_f(\underline{a},y)\leftrightarrow y=\underline{b}]$

Lemma. $\exists\Delta_0$ chiuse ϑ, $\mathbb{N}\models\vartheta \Rightarrow Q\vdash\vartheta$

$$\mathbb{N}\models\vartheta=\exists x\underbrace{\varphi(x)}_{\Delta_0} \Rightarrow \exists k\ \mathbb{N}\models\underbrace{\varphi(\underline{k})}_{\Delta_0}$$

$$\Rightarrow Q\vdash\varphi(\underline{k})$$
$$Q\vdash\exists x\,\varphi(x)$$

Questo lemma dimostra (*)
$$f(a)=b \Leftrightarrow \mathbb{N}\models\varphi_f(a,b)$$
$$\Rightarrow Q\vdash\varphi_f(a,b)$$

110

$f(a) \neq b \Rightarrow \exists c \neq b \quad f(a) = c$

$\Rightarrow \exists N \vdash \underline{c} \neq \underline{b} \quad \varphi_f(\underline{a}, \underline{c}) \Rightarrow Q \vdash \varphi_f(\underline{a}, \underline{c})$

$a \in N \quad Q \vdash \exists ! y \; \varphi_f(\underline{a}, y)$

Minimalizzazione:

$f(x) = \mu y [g(x,y) = 0]$

g rinumerabile funzionalmente in Q e $\exists \Delta_0$ allora f è rinumerabile funzionalmente in Q $\Rightarrow$ da $\exists \Delta_0$

Dimostrazione $f(x) = z \Leftrightarrow g(x,z) = 0 \wedge$

$\wedge (z' < z) \; \neg(N, x z') \; , g(x,z) = \Delta_0$

Queste formule sono vere in Q.

Teorema $R \subseteq \mathbb{R}^2 \Rightarrow \exists$ Rc relativamente calcolabili $f \subset R$ allora sse f_R dove R_R, dove $f = \{x \mid Rxy\}$

[illegible]

(111)

$\ulcorner \; \urcorner$ formule $\to \mathbb{N}$

$\ulcorner \; \urcorner$ termini $\to \mathbb{N}$

($\ulcorner \; \urcorner$ = codifica iniettiva)

$v_0, \ldots, v_n, \ldots$ variabili

$$\langle a_0, \ldots, a_n \rangle = \prod_{i=0}^{n} p_i^{a_i+1}$$

$$\#(v) \in \mathbb{N}, \#(0), \#(S), \#(+), \#(\cdot), \#(\exists)$$

$$\#(\forall), \#(\vee), \#(\wedge), \#(=) \in \mathbb{N}$$

$$\ulcorner v_i \urcorner = \langle \#(v), i \rangle = 2^{\#v+1} \cdot 3^{i+1}$$

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

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

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

$$\ulcorner 0 \urcorner = \langle \#(0) \rangle$$

Esempio. $SS0 = \langle \#S, \langle \#S, \langle \#0 \rangle \rangle \rangle = $

$$= 2^{\#} \cdot 3^{\left(2^{\#S+1} \cdot 3^{2^{\#(0)+1}}\right)}$$

Questa è una codifica ad albero.

$$\ulcorner \varphi \wedge \psi \urcorner = \langle \#(\wedge), \ulcorner \varphi \urcorner, \ulcorner \psi \urcorner \rangle$$

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

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

Teorema $\{\ulcorner \varphi \urcorner \mid \varphi \text{ formula}\}$ è PR

$\{\ulcorner \; \urcorner \mid$ " termini $\}$ 4

112

Dimostrazione: sia $\mathcal{Y} = \{\ulcorner\varphi\urcorner \mid \varphi \text{ formula}\}$

$n \in \mathcal{Y} \iff n = \langle \#(=), a, b \rangle \ \exists a, b \leq n$ e $a, b \in T$

$T = \{\ulcorner t \urcorner \mid t \text{ termini}\}$

oppure

$\exists n_1$ e $n_2 < n$ tale che

$n = \langle \#(\wedge), n_1, n_2 \rangle \quad n_1, n_2 \in \mathcal{Y}$

oppure

$\exists n' \leq n \ \exists i \leq n \quad n = \langle \#\forall, \ulcorner v_i \urcorner, n' \rangle$ e $n' \in \mathcal{Y}$

- - - -

Questa non è ancora una definizione in quanto appare a entrambi i membri. Passiamo alle funzioni caratteristiche: $n \in \mathcal{Y} \iff \chi_{\mathcal{Y}}(n) = 1$

$\chi_{\mathcal{Y}}$ è primitiva ricorsiva.

Esercizio $\{\ulcorner\varphi\urcorner \mid \varphi \in Ax(PA)\}$ PR

Basta dimostrare che

$\ulcorner \varphi(0) \wedge \forall x \{\varphi(x) \to \varphi(sx)\} \to \forall z \, \varphi(z) \urcorner$ è PR

v_0 variabile : $sub : N^2 \to N$ (sostituzione)

$sub(\ulcorner\varphi\urcorner, \ulcorner t \urcorner) = \ulcorner \varphi(t, v_0) \urcorner$ è PR.

(113)

$sub(\ulcorner \varphi \wedge \psi \urcorner, \ulcorner t \urcorner) = \langle \#(\wedge), sub(\ulcorner\varphi\urcorner, \ulcorner t\urcorner), sub(\ulcorner\psi\urcorner, \ulcorner t \urcorner)\rangle$

$sub(\ulcorner \forall v_0 \varphi \urcorner, \ulcorner t \urcorner) = \ulcorner \forall v_0 \varphi \urcorner$

$sub(\ulcorner \forall v_i \varphi \urcorner, \ulcorner t \urcorner) = \langle \#(\forall), \langle \# v, i\rangle, sub(\ulcorner\varphi\urcorner, \ulcorner t\urcorner)\rangle$ altrimenti.

etc.

$sub(n, k) = z$ se $\exists a, b < n = \langle \#(\wedge), a, b \rangle \wedge$
$z = \langle \#(\wedge), sub(a,k), sub(b,k) \rangle$

$n = \ulcorner \psi(0) \wedge \forall x (\psi(x) \to \psi(x+1)) \to \forall y\, \psi(y) \urcorner \in Ind$

$n \in$ Induzione $\leftrightarrow \exists a < n \;\; a \in \mathcal{F} \wedge$
$n = \langle \#(\to), \langle \#(\wedge), sub(a, \ulcorner 0 \urcorner),$
$\langle \#\forall, \ulcorner v_0 \urcorner, \langle \#(\to), a, \langle \#S, \ulcorner v_0 \urcorner \rangle \rangle \rangle$
$\langle \#\forall, \ulcorner v_0 \urcorner, a \rangle \rangle$

$\Rightarrow$ PA sono PR

5 dicembre 2007

Formule x termini $\to$ Formule

$\downarrow \qquad\qquad\qquad \downarrow$

$\mathbb{N} \times \mathbb{N} \xrightarrow[sub]{} \mathbb{N}$

Numerale : $NUM : \mathbb{N} \to \mathbb{N}$
$n \mapsto \ulcorner S^n 0 \urcorner$

$NUM(0) = \ulcorner 0 \urcorner = \langle \#0 \rangle = 2^{\#0}$

$NUM(n+1) = \langle \#S, NUM(n) \rangle = 2^{\#S} \cdot 3^{NUM(n)}$

(114) $D : \mathbb{N} \longrightarrow \mathbb{N}$ (diagonale)

$D(x) = sub(x, NUM(x))$

D è PR perché composizione di PR.

$D(\ulcorner\varphi\urcorner) = sub(\ulcorner\varphi\urcorner, NUM(\ulcorner\varphi\urcorner)) =$

$= sub(\ulcorner\varphi\urcorner, \ulcorner S^n(0)\urcorner)$, $n = \ulcorner\varphi\urcorner$

$= \ulcorner\varphi(S^n 0 / v_0)\urcorner =$

$= \ulcorner\varphi(\ulcorner\underline{\varphi}\urcorner)\urcorner$ $\qquad \underline{k} = S^k 0$

Ogni funzione ricorsiva totale è rappresentabile funzionalmente in Q. In particolare lo è $D : \mathbb{N} \to \mathbb{N}$, cioè esiste $\varphi_D(x,y)$ tale che

$D(n) = k \Rightarrow Q \vdash \varphi_D(\underline{n}, \underline{k})$

$D(n) \neq k \Rightarrow Q \vdash \neg\varphi_D(\underline{n}, \underline{k})$

$Q \vdash \exists! y\, \varphi_D(\underline{n}, y)$

Notazione: Data una formula $P(x)$ ha senso parlare di $P(D(x))$

$P(\underline{D}(x)) \underset{def}{\equiv} \forall y [\varphi_D(x,y) \to P(y)]$

Lemma: $D(n) = k$ $\quad Q \vdash P(\underline{D}(\underline{n})) \leftrightarrow P(\underline{k})$

$P(\underline{D}(\underline{n})) \leftrightarrow P(\underline{D(n)})$

Dimostrazione. $Q \vdash P(\underline{D}(\underline{n}))$

$$\left[\begin{array}{l} Q \vdash \forall y [\varphi_D(\underline{n}, y) \to P(y)] \\ Q \vdash \forall y [\varphi(\underline{n}, y) \leftrightarrow y = \underline{D(n)}] \\ Q \vdash P(\underline{D(n)}) \end{array}\right.$$

La stessa cosa vale per ogni funzione ricorsiva totale.

(115) Teorema di diagonalizzazione o del punto fisso

Data $\alpha = \alpha(v_0)$ esiste β chiusa tale che $Q \vdash \alpha(\ulcorner \underline{\beta} \urcorner) \leftrightarrow \beta$

$$\left(\begin{array}{ccccc} \text{Formule} & \to & \mathbb{N} & \to & \text{termini} \\ \beta & \to & \ulcorner \beta \urcorner & \to & \ulcorner \underline{\beta} \urcorner = S^{3} \end{array} \right)$$

Dimostrazione

(Idea: β dice "io godo della proprietà $\alpha(x)$")

(Idea per la costruzione di β: $\beta = \varphi\varphi \qquad \alpha(\varphi\varphi) \leftrightarrow \varphi\varphi$, $\varphi(x) = \alpha(xx)$)

$$\beta = \varphi(\ulcorner \underline{\varphi} \urcorner)$$

Voglio che $Q \vdash \alpha(\ulcorner \varphi(\ulcorner \underline{\varphi} \urcorner) \urcorner) \leftrightarrow \varphi(\ulcorner \underline{\varphi} \urcorner)$

$$\alpha(\ulcorner \underline{\varphi(\ulcorner \varphi \urcorner)} \urcorner) = \alpha(\underline{D}(\ulcorner \varphi \urcorner)) \leftrightarrow$$

$$\underset{Q}{\leftrightarrow} \alpha(\underline{D}(\ulcorner \underline{\varphi} \urcorner))$$

$$\varphi(x) \doteq \alpha(\underline{D}(x)) = \forall y[\varphi_D(x,y) \to \alpha(y)]$$

$$\beta \doteq \varphi(\ulcorner \underline{\varphi} \urcorner)$$

$$\alpha(\ulcorner \underline{\beta} \urcorner) = \alpha(\ulcorner \underline{\varphi(\ulcorner \varphi \urcorner)} \urcorner) \underset{Q}{\leftrightarrow} \alpha(\underline{D}(\ulcorner \varphi \urcorner))$$

$$\| $$

$$\alpha(\ulcorner \underline{\varphi} \urcorner) = \beta$$

Non si può sperare che $\beta = \alpha(\beta)$ ma soltanto che siano equivalenti perché il numero di Gödel non è lo stesso.

(116) Teorema (PA è incompleta)
$\exists$ formula G tale che $PA \nvdash G$ e
$PA \nvdash \neg G$

$\{ \ulcorner \varphi \urcorner \mid \varphi \in$ assiomi di $PA \}$ è PR

$PROV_{PA} = \{ (n, \ulcorner \varphi \urcorner) \mid n$ codifica una dimostrazione di φ in $PA \}$

$(n, \ulcorner \varphi \urcorner)$ è PR (non dimostrato)

$$TEO_{PA} = \{ \ulcorner \varphi \urcorner \mid PA \vdash \varphi \} = \underbrace{\{ \ulcorner \varphi \urcorner \mid \exists n \underbrace{(n, \ulcorner \varphi \urcorner) \in PROV_{PA}}_{\text{Ric}} \}}_{RE}$$

TEO_{PA} sono RE ma non PR.

In generale: se T è una L-teoria e L un linguaggio finito

Assiomi (T) Ricorsivi
$\Rightarrow \{ (n, \ulcorner \varphi \urcorner) \mid T \vdash_n \varphi \}$ Ric
$\{ \ulcorner \varphi \urcorner \mid T \vdash \varphi \}$ RE

$PROV_{PA} \subset \mathbb{N}^2$ ed esiste una formula che lo trinumera in Q, cioè

$(a, b) \in PROV_{PA} \Rightarrow Q \vdash P(\underline{a}, \underline{b})$
$(a, b) \notin PROV_{PA} \Rightarrow Q \vdash \neg P(\underline{a}, \underline{b})$

$T_{PA}(y) = \exists x\, P(x, y)$ non è PR

$$\left(\begin{array}{ccccc} (PA \vdash_n \varphi) & \Rightarrow & (n, \ulcorner \varphi \urcorner) \in PROV_{PA} & \Rightarrow & Q \vdash P(\underline{n}, \underline{\ulcorner \varphi \urcorner}) \\ \nvdash_n & & \notin & & \neg \end{array} \right)$$

$PA \vdash \varphi \Rightarrow \exists n\ PA \vdash_n \varphi$
$\Rightarrow Q \vdash P(\underline{n}, \underline{\ulcorner \varphi \urcorner})$.

$\Rightarrow Q \vdash T_{PA}(\underline{\ulcorner \varphi \urcorner})$

 Se $PA \nvdash \varphi$ non c'è niente da fare.

$$PA \nvdash \varphi \Rightarrow \nexists n\ PA \vdash_n \varphi$$

$$\nexists n\ Q \vdash P(\underline{n}, \ulcorner\underline{\varphi}\urcorner)$$, ma da qui

non possiamo dedurre:

$$Q \vdash \neg\exists x\, P(x, \ulcorner\varphi\urcorner)$$
$$\neg T(\ulcorner\varphi\urcorner)$$

In generale: $\exists t \quad T \vdash P(t)$
$$\Downarrow \quad \Uparrow$$
$$T \vdash \exists x\, P(x)$$

(*) $PA \vdash \varphi \overset{\Leftarrow}{\Rightarrow} Q \vdash T_{PA}(\ulcorner\varphi\urcorner) \Rightarrow \mathbb{N} \models T_{PA}(\ulcorner\varphi\urcorner)$

$$\Rightarrow \mathbb{N} \models \exists x\, P(x, \ulcorner\varphi\urcorner)$$

$$\Rightarrow \exists n \in N \quad \mathbb{N} \models P(n, \ulcorner\varphi\urcorner)$$

$$\Rightarrow \exists n \in N\ (n, \ulcorner\varphi\urcorner) \in PROV_{PA}$$

$$\Rightarrow PA \vdash_n \varphi \Rightarrow PA \vdash \varphi$$

(*) non è equivalente a dire che φ è enumerabile.
Questa proprietà si dice numerabilità.

Primo teorema di Goedel
$\exists G \quad PA \nvdash G$ e $PA \nvdash \neg G$

Dimostrazione. Scelgo G tale che
$$Q \vdash G \leftrightarrow \neg T_{PA}(\ulcorner\underline{G}\urcorner)$$

G dice "io non sono dimostrabile",
però G risulterà vera

(118) Supponiamo per assurdo che $PA \vdash G$

$\Rightarrow \exists n\ (PA \vdash_n G)$

$\Rightarrow (n, \ulcorner G \urcorner) \in PROV_{PA}$

$\Rightarrow Q \vdash P(\underline{n}, \ulcorner \underline{G} \urcorner)$

$\Rightarrow Q \vdash \exists x\, P(x, \ulcorner \underline{G} \urcorner)$

$\Rightarrow Q \vdash T_{PA}(\ulcorner \underline{G} \urcorner)$

$\Rightarrow Q \vdash \neg G$ (usando la def. di G)

$\Rightarrow PA \vdash \neg G$

$\Rightarrow PA \vdash G \wedge \neg G$

$\Rightarrow PA \vdash \bot$. Assurdo perché PA è coerente.

(In generale: $PA \rightsquigarrow T \supseteq Q$, T r.e. Ax + coerente)

Supponiamo per assurdo che $PA \vdash \neg G$.

$PA \vdash \neg G$

$\Rightarrow PA \vdash T_{PA}(\ulcorner G \urcorner)$

$\Rightarrow \mathbb{N} \models T_{PA}(\ulcorner G \urcorner)$ $(\mathbb{N} \models PA)$

$\Leftrightarrow \mathbb{N} \models \exists x\, P(x, \ulcorner \underline{G} \urcorner)$

$\Leftrightarrow \exists n \in \mathbb{N}\ \ \mathbb{N} \models P(\underline{n}, \ulcorner \underline{G} \urcorner)$

$\Leftrightarrow (n, \ulcorner G \urcorner) \in PROV_{PA}$

$\Leftrightarrow PA \vdash_n G$

$\Leftrightarrow PA \vdash G$

$\Rightarrow PA \vdash G \wedge \neg G$ Assurdo.

Complessità: $G \underset{Q}{\leftrightarrow} \neg T_{PA}(\ulcorner G \urcorner)$

$\leftrightarrow \neg \underbrace{\exists x\, P(x, \ulcorner \underline{G} \urcorner)}_{\exists \Delta_0}$

$\leftrightarrow \forall \Delta_0$

$\leftrightarrow \forall \vec{x}\ \ p(\vec{x}) \neq 0$

Esiste un polinomio che non ha soluzioni in Δ_0.

(119) G è indecidibile ma vera su N

$PA \nvdash G \iff N \models \neg T_{PA}(\ulcorner G \urcorner)$

$\underset{def}{\iff} N \models G$

Quindi G è vera pur non avendola dimostrata in PA. Questo discende dal fatto che PA è coerente: tutti i passaggi della dimostrazione avrebbe potuto farli PA tranne il fatto che PA è coerente.

7 dicembre 2007

Formule $\overset{N}{\longmapsto}$ Termini

$\varphi \longmapsto \ulcorner \varphi \urcorner \longmapsto \ulcorner \varphi \urcorner$

ξ dice "io godo della proprietà $\alpha(x)$"

Sia T una teoria SQ coerente, ricorsivamente assiomatizzata che non ha PA come modello.

Una teoria nel linguaggio dell'aritmetica è ω-coerente se
$[\forall n \in N \;\; T \vdash \neg\varphi(n)] \Rightarrow (T \nvdash \exists x \varphi(x))$

Una teoria ω incoerente è infinita e quindi le sue incoerenze le si dimostra all'infinito quindi è come se fosse coerente.

$N \models T \Rightarrow T$ ω-coerente $\Rightarrow T$ coerente

T è coerente perché non dimostra qualcosa.

(129) PA+G ha come modello $\mathbb{N}$

(∗) PA+¬G è ω-incoerente

$PA \nvdash G \Rightarrow PA+\neg G$ è coerente
$PA \nvdash \neg G \Rightarrow PA+G$ è coerente

Poiché (∗) non è la stessa cosa che aggiungere all'insieme degli assiomi della geometria euclidea oppure no.

$\neg G \leftrightarrow_{G} \exists x\, P(x, \ulcorner \underline{G} \urcorner)$

$PA \nvdash G$
$\forall n\ PA \nvdash_n G$
$\forall n\ (n, \ulcorner G \urcorner) \notin Prov_{PA}$
$\forall n\ PA \vdash \neg P(\underline{n}, \ulcorner \underline{G} \urcorner)$

$T = PA + \neg G$
$\forall n\ T \vdash \neg P(\underline{n}, \ulcorner G \urcorner)$
ma $T \vdash \exists x (P(x, \ulcorner G \urcorner))$

Lemma. $\varphi \in \Delta_0\ \ \mathbb{N} \models \varphi \Rightarrow Q \vdash \varphi$
$\varphi \in \Delta_0\ \ \mathbb{N} \models \varphi \Rightarrow Q \vdash \varphi \Rightarrow T \vdash \varphi\ ,\ T \supseteq Q$

Se T è ω-coerente,
$\varphi \in \Delta_0\ \ \mathbb{N} \models \varphi \Leftarrow T \vdash \varphi$

Dimostrazione. $\Leftarrow$ $\varphi = \exists x\, \vartheta(x) = \exists x \Delta x$

$\mathbb{N} \not\models \exists x \vartheta(x) \ldots$

$\mathbb{N} \models \neg\vartheta(0), \neg\vartheta(1), \neg\vartheta(2), \ldots$

$T \vdash \neg\vartheta(0), \neg\vartheta(1), \ldots, \neg\vartheta(n)$

ω-incoerenza

(121) Teorema. $T \supseteq Q$ T re Ax ω-coerente $\Rightarrow \exists G$ $T \nvdash G$ $T \nvdash \neg G$.

Dimostrazione. $PROV_T = \{(n, \ulcorner\varphi\urcorner) \mid T \vdash_n \varphi\}$ ricorsivamente binumerabile in Q : che $P(x,y)$ Δ_0

$T(y) = \exists x\, P(x,y)$

$Q \vdash G \leftrightarrow \neg T(\ulcorner\varphi\urcorner)$

se $T \vdash \neg G$

$T \vdash T(\ulcorner G \urcorner)$ $\qquad T(\ulcorner G\urcorner) \in \exists\Delta_0$

$\Updownarrow$ ω-coerente $\qquad P \in \exists\Delta_0$

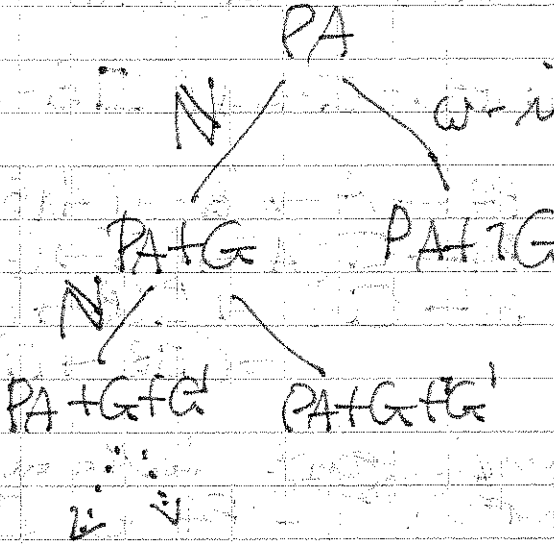
$\mathbb{N} \models T(\ulcorner G\urcorner)$

$\exists n\ \mathbb{N} \models P(n, \ulcorner G\urcorner)$

$(n, \ulcorner G\urcorner) \in PROV_T$

$T \vdash_n G$

$T \vdash G \wedge \neg G$



Non sappiamo se possiamo biforcare da queste parte perché c'è ω-incoerenza. In realtà è possibile.

Secondo teorema di Gödel: $PA \nvdash Cons(PA)$
$(\neg\Box\bot)$

$\Box\varphi = \text{box}\,\varphi = T_{PA}(\ulcorner\varphi\urcorner)$

$Q \vdash (G \leftrightarrow \neg\Box G)$

$\Diamond\varphi = \text{diamante}\,\varphi = \neg\Box\neg\varphi$

Condizioni di derivabilità:

$\varphi \in \Sigma_1 \quad \mathbb{N} \models \varphi \Rightarrow PA \vdash \varphi$

$\mathbb{N} \models \Box\varphi \quad PA \vdash \varphi \to \Box\varphi$

$\Updownarrow$

$D1: PA \vdash \varphi \Rightarrow PA \vdash \Box\varphi$

$D2: PA \vdash \Box\varphi \to \Box\Box\varphi$

$D3: PA \vdash \Box A \wedge \Box(A \to B) \to \Box B$
(PA dimostra il modus ponens).

$PA \vdash \Box\varphi \to \Box\psi$

Infatti: $PA \vdash (\varphi \to \psi)$
$PA \vdash \Box(\varphi \to \psi)$
$PA \vdash \Box\varphi \to \Box\psi$

$PA \vdash (\Box A \wedge \Box B) \to \Box(A \wedge B)$

Infatti: $PA \vdash \Box A \to (\Box B \to \Box(A \wedge B))$

$PA \vdash A \to (B \to (A \wedge B))$
$PA \vdash \Box(A \to (B \to (A \wedge B)))$
$PA \vdash \Box A \to \Box(B \to (A \wedge B))$
$\to (\Box B \to \Box(A \wedge B))$

Si può rimpiazzare tutto questo con una teoria $T \supseteq PA$ e $\Box = \Box_T$.

$T \vdash \Box_T \varphi \overset{\Leftarrow}{\not\Rightarrow} T \vdash \varphi$, cioè T potrebbe dimostrare cose false.

(123) **Teorema.** Sia $Q \vdash G \leftrightarrow \neg\Box_{PA} G$

$PA \nvdash G \quad PA \nvdash \neg G$

$PA \vdash (G \leftrightarrow \neg\Box_{PA}\bot)$

Dimostrazione. $PA \vdash \neg G \to \Box_{PA}\bot$

$PA \vdash \neg G \to \Box G$ (def G)

Basta far vedere

$PA \vdash \neg G \to \Box\neg G$

$PA \vdash \neg G \to \Box G$

$\to \Box\Box G$

$\to \Box\neg G$ $(PA \vdash \Box G \leftrightarrow \neg G)$

Viceversa: $PA \vdash \bot \to G$

$PA \vdash \Box(\bot \to G)$

$PA \vdash \Box\bot \to \Box G$

$\downarrow$ def G

$\neg G$

$PA \vdash \Box\bot \leftrightarrow \neg G$

$\neg\Box\bot \leftrightarrow G$

$Con(PA)$.

Sia T una teoria ω-coerente $T \supseteq Q$, ricorsivamente assiomatizzata. Allora T è incompleta, indecidibile e $\{\ulcorner\varphi\urcorner \mid T \vdash \varphi\}$ non è ricorsivo.

Dimostrazione. $K_0 \subseteq \mathbb{N}$ RE, non RIC

(per esempio K_0 = problema della fermata),

$\exists$ RIC = RE

$\exists x \underbrace{\vartheta(x,y)}_{\Delta_0}$ $\quad K_0 = \{n \in \mathbb{N} \mid \mathbb{N} \models \exists x\,\vartheta(x,n)\}$

Per esempio $K_0 = \{x \mid \varphi_x(x)\downarrow\}$

$\{x \mid \exists t\ \varphi_x(x)|_t\}$

$\varphi \in \exists\Delta_0 \quad T \vdash \varphi \Leftrightarrow \mathbb{N} \models \varphi$ se T è ω-coerente

$n \in K_0 \Leftrightarrow \mathbb{N} \models \underbrace{\exists x \vartheta(x, \underline{n})}_{\Sigma_1} \Leftrightarrow T \vdash \exists x \vartheta(x, \underline{n})$

Se avessi un algoritmo per sapere se una qualunque formula è teorema di T allora K_0 ricorsivo.

Q e PA sono incomplete e indecidibili, cioè $\{\ulcorner \varphi \urcorner \mid Q \vdash \varphi\}$ non Ric.

Corollario (Church)
$\{\varphi \mid \vdash \varphi\}$ è indecidibile nel linguaggio dell'aritmetica $L = \{0, S, +, \cdot\}$

(Formule vera in tutti i modelli:
$\vdash \forall xyz [h(h(x,y), z) = y \to \forall xy\, x = y]$)

$Q \vdash \varphi \Leftrightarrow \vdash (Q_1 \ldots Q_5) \to \varphi, \; Q = \{Q_1 \ldots Q_5\}$

12 dicembre 2007

Primo teorema di Gödel
$T \supseteq Q$, T ricorsivamente assiomatizzato, ω-coerente $\to$ T è incompleta

Teorema di Rosser:
X coerente

Teorema. dato $\alpha(x)$ esiste β $Q \vdash \beta \leftrightarrow \alpha(\ulcorner \beta \urcorner)$
(β punto fisso di α)

Notazione. $\Box \varphi = \underline{\mathrm{Teo}}_T(\ulcorner \varphi \urcorner)$

(125) $PROV_T = \{(n, \ulcorner\varphi\urcorner) \in \mathbb{N}^2 \mid T \vdash_n \varphi\}$ ricorsivo

$\underline{PROV}_T(x,y)$ $\quad (n, \ulcorner\varphi\urcorner) \in PROV_T \Rightarrow Q \vdash \underline{PROV}_T(\underline{n}, \underline{\ulcorner\varphi\urcorner})$

$(n, \ulcorner\varphi\urcorner) \notin PROV_T \Rightarrow Q \vdash \neg \underline{PROV}_T(\underline{n}, \underline{\ulcorner\varphi\urcorner})$

$\underline{TEO}_T(y) = \exists x \, \underline{PROV}_T(x,y)$

$T \vdash \varphi \Rightarrow \exists n \; T \vdash_n \varphi \Rightarrow \exists n \; Q \vdash PROV_T(\underline{n}, \ulcorner\varphi\urcorner)$

$Q \vdash \exists x \, \underline{PROV}_T(x, \ulcorner\varphi\urcorner)$

$Q \vdash Teo_T(\ulcorner\varphi\urcorner)$

$Q \vdash \Box_T \varphi$

Gödel. sia G: $Q \vdash G \leftrightarrow \neg\Box_T G$

$T \nvdash G \quad T \nvdash \neg G$

$\Box_x \varphi \Leftrightarrow \exists y \leq x \; PROV(y, \ulcorner\varphi\urcorner)$

Rosser basta la coerenza:

Esiste R chiusa

$Q \vdash R$ dice "se io sono dimostrabile la mia negazione lo è prima di me".

$(*) \; Q \vdash R \leftrightarrow \forall x \, (\Box_x R \to \exists y < x \, \Box_y \neg R)$

$T \nvdash R, \; T \nvdash \neg R$

Supponiamo per assurdo $T \vdash R$.

Allora $\exists n \; T \vdash_n R$

$Q \vdash \underline{PROV}_T(\underline{n}, \underline{\ulcorner R \urcorner})$

$Q \vdash \Box_n R$

$T \vdash \Box_n R$

da $(*)$ $T \vdash R \to (\Box_n R \to \exists y < \underline{n} \, \Box_y \neg R)$

$T \vdash \exists y < \underline{n} \, \Box_y \neg R$

$Q \vdash y < \underline{n} \leftrightarrow y = 0 \vee \dots \vee y = n-1$

$T \vdash \Box_0 \neg R \vee \dots \vee \Box_{n-1} \neg R$

(126) $T \vdash PROV_T(\underline{0}, \ulcorner \neg R \urcorner) \vee \dots \vee PROV_T(\underline{n-1}, \ulcorner \neg R \urcorner)$

$T \vdash_0 \neg R$ o ... o $T \vdash_{n-1} \neg R$

se $T \nvdash_k \neg R \quad \forall k \le n-1 \Rightarrow Q \vdash \neg PROV_T(\underline{k}, \ulcorner \neg R \urcorner)$

$k = 0, \dots, n-1$

$T \vdash \neg PROV(\underline{0}, \ulcorner \neg R \urcorner) \wedge \dots \wedge \neg PROV(\underline{n-1}, \ulcorner \neg R \urcorner)$

$T \vdash \bot$ Assurdo

$T \vdash \neg R$

$T \vdash R \wedge \neg R$ Assurdo $\Rightarrow T \nvdash R$

Sia per assurdo $T \vdash \neg R$

$\exists n \; T \vdash_n \neg R$

$Q \vdash \Box_n \neg R$

$T \vdash \Box_n \neg R$

$T \vdash (*)$

$T \vdash \neg \forall x (\Box_x R \to \exists y < x \, \Box_y \neg R)$

$T \vdash \exists x (\Box_x R \wedge \neg \exists y < x \, \Box_y \neg R)$

x deve essere minore di $n+1$

$T \vdash \exists y < n+1 \, \Box_y \neg R$

$T \vdash \exists x \le n \, \Box_x R$

(stiamo ragionando considerando al posto di $Q \rightsquigarrow Q^* = Q + (\le \text{ totale})$

$T \vdash \Box_n R$

$T \vdash_n R$ (cioè n codifica una dimostrazione di R;

altrimenti

$T \nvdash_n R, Q \vdash PROV_T(\underline{n}, \ulcorner R \urcorner)$

$Q \vdash \neg \Box_n R$

$T \vdash \neg \Box_n R$)

(127)

$T \vdash R$

$T \vdash R \wedge \neg R$ Assurdo.

Per Gödel: $Q \vdash G \leftrightarrow \neg \square_{PA} G$

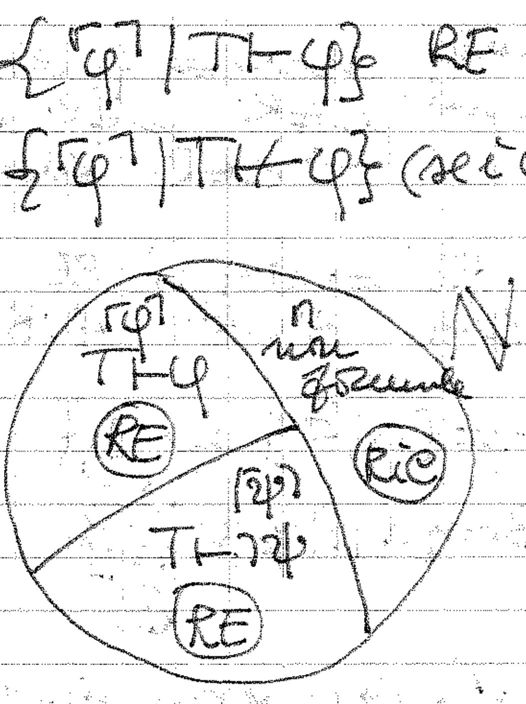
$PA \vdash G \leftrightarrow Cons(PA)$

Con Rosser non possiamo giungere alle stesse conclusioni. Il teorema di Rosser in questo caso è più debole.

Osservazione: T ricorsivamente assiomatizzata e indecidibile è incompleta.

$\{\ulcorner\varphi\urcorner \mid T \vdash \varphi\}$ RE

$\{\ulcorner\varphi\urcorner \mid T \nvdash \varphi\}$ (se è completa) $= \{\ulcorner\varphi\urcorner \mid T \vdash \neg\varphi\}$ RE



Teorema: Q è essenzialmente indecidibile, cioè ogni $T \supseteq Q$, $L(T) = L(Q)$ coerente è indecidibile

Esempio: La teoria dei campi è indecidibile ma non essenzialmente, cioè non esiste un algoritmo per sapere se una formula è vera in tutti i campi.

Q, PA, ZF sono essenzialmente indecidibili

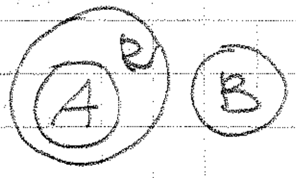
$Th(\mathbb{N},+,\cdot)$, $Th(\mathbb{Z},+,\cdot)$, $Th(\mathbb{Q},+,\cdot)$

(128) $Th(\mathbb{R},+,\cdot)$, $Th(\mathbb{C},+,\cdot)$ sono decidibili

A,B RE, $A,B \subseteq \mathbb{N}$ sono ricorsivamente inseparabili se sono disgiunti e non esiste R ricorsivo $A \subseteq R$, $R \cap B = \emptyset$

Esistono: $A = \{x \mid \varphi_x(x)\downarrow = 0\}$

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



Se R ricorsivo lì segue $\chi_R : \mathbb{N} \to \{0,1\}$ calcolabile
$\chi_R = \varphi_e$ Abbiamo $e \in R \Leftrightarrow \varphi_e(e) = 1 \Leftrightarrow e \in B$
Quindi $e \notin R$ $e \notin R \Leftrightarrow \varphi_e(e) = 0 \Leftrightarrow e \in A$
$\to e \in R$ Assurdo.

Teorema. A,B RE $\Rightarrow \exists A',B'$ RE disgiunti con $A' \subseteq A$ $B' \subseteq B$ $A' \cup B' = A \cup B$

Infatti: $A = \{x \mid \exists y \underbrace{\alpha(x,y)}_{Ric}\}$

$B = \{x \mid \exists y \underbrace{\beta(x,y)}_{Ric}\}$

$A' = \{x \mid \exists y (\alpha(x,y) \land \forall z < y \ \neg\beta(x,z))\}$

$B' = \{x \mid \exists z (\beta(x,z) \land \forall y \leq z \ \neg\alpha(x,y))\}$

A' e B' sono RE per costruzione

Teorema. Q è essenzialmente indecidibile

Dimostrazione. A,B ricorsivamente inseparabili
A,B RE

$A = \{x \mid \mathbb{N} \models \exists y \ \alpha(x,y)\}$

(129) α termina in Q un insieme ricorsivo

$B = \{x \mid \mathbb{N} \models \exists y\ \beta(x,y)\}$

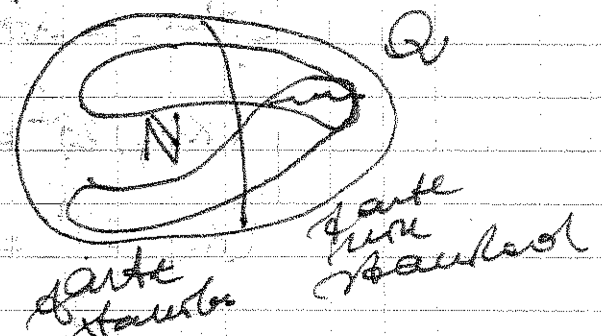
A', B' come sopra

Poiché $A \cap B = \emptyset \Rightarrow A' = A$ e $B' = B$

① $\text{"}x \in A'\text{"} \equiv \exists y(\alpha(x,y) \wedge \forall z < y\ \neg\beta(x,z))$

② $\text{"}x \in B'\text{"} \equiv \exists z(\beta(x,z) \wedge \forall y \leq z\ \neg\alpha(x,y))$

$Q \vdash \forall x\ \text{"}x \in A'\text{"} \to \neg\text{"}x \in B'\text{"}$



① e ② sono formule del tipo $\exists\Delta_0$

$\varphi \in \exists\Delta_0\ \ \mathbb{N} \models \varphi \Rightarrow Q \vdash \varphi$

$n \in A = A' \Rightarrow \mathbb{N} \models \text{"}n \in A'\text{"} \Rightarrow Q \vdash \text{"}n \in A'\text{"}$

$n \in B = B' \Rightarrow \mathbb{N} \models \text{"}n \in B'\text{"} \Rightarrow Q \vdash \text{"}n \in B'\text{"} \Rightarrow Q \vdash \neg\text{"}n \in A'\text{"} \Downarrow \boxed{Q \nvdash \text{"}n \in A'\text{"}}$

L'insieme ricorsivo che le separa è

$C = \{n \mid Q \vdash \text{"}n \in A'\text{"}\} \supset A \quad , \quad C \cap B = \emptyset$

Interpretazione fra teorie: $T_1 \rhd T_2$

$ZF \rhd PA \quad , \quad Th(\mathbb{Z},+,\cdot) \rhd Th(\mathbb{N},+,\cdot)$

$Th(\mathbb{N},+,\cdot,S,0) \supset Q$ è indecidibile

130

Cerchiamo un'interpretazione che se $T_1 \trianglerighteq_I T_2$ $\quad T_1 \vdash \varphi^I \Leftarrow T_2 \vdash \varphi$

$I : L_2 \to L_1$
$\varphi \mapsto \varphi^I$ calcolabile

Dato $x \in \mathbb{Z}$ $\quad x \in \mathbb{N} \leftrightarrow \exists abcd \; x = a^2 + b^2 + c^2 + d^2$
(Teorema di Lagrange)

$$\mathbb{N} \models \varphi \leftrightarrow \mathbb{Z} \models \varphi^I$$

$$\varphi = \ldots \forall x \ldots \exists x$$

$$\varphi^I = \ldots \forall x \geq 0 \ldots \exists x \geq 0 \ldots$$

$$(x+y=z)^I = (x+y=z)$$

$$(xy=z)^I = (xy=z)$$

$$(x=0)^I = (x=0)$$

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

$$(\forall x \varphi)^I = \forall x (x \geq 0 \to \varphi^I)$$

$$\mathbb{N} \models \varphi = \exists x \forall y \exists z (z + x = y)$$

$$\mathbb{Z} \models \ldots$$

$$\mathbb{Z} \models \exists x \geq 0 \; \forall y \geq 0 \; \exists z \geq 0 \; (z + x = y)$$

Quindi esiste I calcolabile tale che

$$\mathbb{N} \models \varphi \leftrightarrow \mathbb{Z} \models \varphi^I$$

$$\{\psi \mid \mathbb{Z} \models \psi\} \text{ ric} \Rightarrow \{\varphi \mid \mathbb{N} \models \varphi\} \text{ ric}$$

$\Rightarrow$ Assurdo