5

31 ottobre 2007

Una L-teoria è completa se e solo se per ogni φ chiusa ($T \models \varphi$ o $T \models \neg\varphi$)

φ segue da T o non φ segue da T.

Esempio T = ordini lineari $L = \{<\}$ non è completa

φ = densità

$\mathbb{R} \models \neg\varphi$, $\mathbb{Z} \models \varphi$

$T \not\vdash \varphi$, $T \not\vdash \neg\varphi$

T = ordini lineari densi senza max e min

$$(*) \begin{cases} \neg(x<x) \\ x<y \wedge y<z \rightarrow x<z \\ x<y \vee y=x \vee y<x \end{cases}$$

$x<y \rightarrow \exists z\,(x<z \wedge z<y)$

$\forall x\, \exists y\,(y>x)$

$\forall x\, \exists y\,(y<x)$

T è completa $\Leftrightarrow \forall A,B \models T\ (A \equiv B)$

T = ordini discreti è completa e hanno come modello $\mathbb{Z}$.

In $\mathbb{Z}$ possiamo considerare come assiomi (*) e la discretezza cioè

$\forall x \exists y\,(y>x \wedge \neg\exists z(y>z \wedge z>x))$

$\forall x \exists y\,(y<x \wedge \neg\exists z(y<z \wedge z<x))$

$(\mathbb{Z},<) \models T$

$\shortparallel$

$(\mathbb{Z}\times\{0,1\}, <_{lex}) \models T$ perché la teoria è completa (da dimostrare)

58

Esempio. M L-struttura

$T = Th(M) = \{\varphi \mid M \models \varphi\}$ completa.

T completa $M \models T \Rightarrow T = Th(M)$

T = teoria ordini discreti

$\Downarrow$

$T = Th(\mathbb{Z}, <) = Th(\mathbb{Z} \times \{0,1\}, <_{lex})$

Richiediamo sempre che T sia coerente cioè $T \not\models \varphi$ ($T \models \varphi$ e $T \models \neg\varphi$).

Data una teoria T $M \models T$ si ha $T \subset Th(M)$

Se inoltre T è completa vale $T = Th(M)$

T completa $T \subset T'$ coerente $\Rightarrow T = T'$

si intende che i teoremi sono inclusi

$T' \models \varphi \Rightarrow T \models \varphi$ se no $T \models \neg\varphi$ ma allora $T' \models \neg\varphi$.

Definizione informale

Sia D un dominio di oggetti finitamente descrivibili

($D = \mathbb{N}$ $D = \mathbb{Q}$ $D = L$ formule L finito)

D dominio numerabile

$$D = \Sigma^* = \bigcup_{n \in \mathbb{N}} \Sigma^n$$

Gli altri domini sono enumerabili se possono essere messi in corrispondenza biunivoca con Σ^*

(9) $A \subset D$ è decidibile $\Leftrightarrow \exists$ algoritmo $f: D \to \{vero, F\}$
tale che $a \in A \Leftrightarrow f(a) = vero$
$a \notin A \Leftrightarrow f(a) = falso$

A è ricorsivamente enumerabile se e solo se esiste un algoritmo f
$dom(f) = D$ e $\forall a \in A \Rightarrow f(a)$ vero
$\forall a \notin A \Rightarrow f(a)$ non si ferma mai

Esempio $p(x_1, \dots x_n) = \sum c_{i_1 \dots i_n} x^{i_1} \dots x^{i_n}$ $c \in \mathbb{Z}$

$\mathbb{Z}^n \supset \{(x_1, \dots, x_n) \in \mathbb{Z}^n \mid \exists y_1 \dots y_k$ tale che
$p(y_1 \dots y_k, x_1 \dots x_n) = 0\}$

è ricorsivamente enumerabile.

10° problema di Hilbert: dato un polinomio a coefficienti interi stabilire se ha radici intere.

$D = \mathbb{Z}[x_1 \dots x_{100}]$

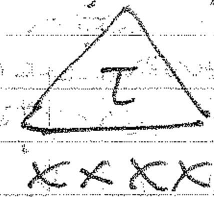
$D \supseteq A = \{p \in D \mid \exists x_1 \dots x_{100}\ p(x_1 \dots x_n) = 0\}$

$p \mapsto$ semi algoritmo $\nearrow$ vero se $\exists \bar{x}\ p(\bar{x}) = 0$
$\searrow \uparrow$ cioè non si ferma mai

I ricorsivamente enumerabili si ottengono mettendo quanti quantificatori esistenziali davanti ad insiemi ricorsivi.

L-teorie di L finita
T insieme finito di assiomi
$\{\varphi \mid T \models \varphi\} \subset$ (L-formule chiuse)
è ricorsivamente enumerabile.
L'algoritmo consiste nell'usare il metodo dei tableaux. $\vdash_{tab}$

(60) $(T \vdash_{tab} \varphi) \iff \exists$ tableau chiuso τ tale che $T, \neg\varphi$



$\{\tau \mid \tau$ tableaux$\}$ può essere messo in corrispondenza biunivoca con $\mathbb{N}$.

Teorema: se T è completa $\{\varphi \mid T \vdash \varphi\} \subset L$-formule è ricorsivo.

$\varphi \longrightarrow \boxed{Alg} \rightarrow$ vero $T \vdash \varphi$

$\qquad\qquad\qquad\rightarrow$ falso $T \nvdash \varphi$ cioè $T \vdash \neg\varphi$

La completezza assicura che dopo un numero finito di passi uno dei due rami si ferma.

ZF non è completa

I discorsi fatti si estendono a T tale che $Ass(T) \subset L$-formule sia ricorsivo o ricorsivamente enumerabile

Sia $Ass(T)$ ricorsivo, L finito
Allora $\{\varphi \mid T \vdash \varphi\}$ è ricorsivamente enumerabile.
Enumero i tableaux (tableaux $\cong \mathbb{N}$)
Controllo se nella radice alg ci sono $T, \neg\varphi$, allora $\varphi \longrightarrow \boxed{\ } \rightarrow$ vero
Altrimenti passo a controllarne un altro.

(6) Altro esempio di teoria completa

$Th(\mathbb{R}, <, +, \cdot, 0, 1)$ completa

$\{\varphi \mid \mathbb{R} \models \varphi\}$

$\|$ ||| equivalente cioè hanno gli stessi assiomi e gli stessi teoremi

$\{\varphi \mid RCF \vdash \varphi\}$

RCF Ric. Ricorsivamente assiomatizzata e completa

campi ordinati $\forall b, c$

$\exists x (x^2 + bx + c > 0) \wedge \exists x' (x'^2 + bx' + c < 0) \to \exists x'' (x''^2 + bx'' + c = 0)$

Corollario. Esiste un algoritmo per stabilire se una formula φ è vera nei reali.

Siano A e B due L-strutture

$A \subseteq B$ sottostruttura le operazioni di A sono le restrizioni di quelle di B e i domini sono inclusi.

Esempio $(\mathbb{Q}, +, \cdot) \subset (\mathbb{R}, +, \cdot)$

$A \preceq B$ è una sottostruttura elementare se è una sottostruttura e se $\forall \varphi(x_1 \ldots x_n) \in L$ e $\forall a_1 \ldots a_n \in A$

$A \models \varphi(a_1 \ldots a_n) \leftrightarrow B \models \varphi(a_1 \ldots a_n)$

Esempio. $P = \{pari\} = 2\mathbb{Z}$, $(2\mathbb{Z}, <) \subset (\mathbb{Z}, <)$

$\Rightarrow (2\mathbb{Z}, <) \cong (\mathbb{Z}, <)$

$(2\mathbb{Z}, <) \equiv (\mathbb{Z}, <)$ l'isomorfismo non implica essere una sottostruttura elementare.

ma

$(2\mathbb{Z}, <) \not\preceq (\mathbb{Z}, <)$

62

$(\mathbb{Q}, <, +, \cdot) \not\prec (\mathbb{R}, <, +, \cdot)$ perché non sono isomorfi

$(2\mathbb{Z}, +, \cdot) \not\equiv (\mathbb{Z}, +, \cdot)$

$\not\prec$ $\exists e\,(\forall z\,(ez = z))$

Teorema. Se A è una L-struttura allora esiste una sottostruttura elementare $B \preceq A$ piccola cioè $|B| \le \max\{\aleph_0, |L|\}$

LS↓

Corollario. $\exists (A, +, \cdot) \prec (\mathbb{R}, +, \cdot)$ numerabile cioè i numeri algebrici.

Se ZF è coerente $\Rightarrow \exists B \models ZF$ $|B| \le \aleph_0$

Esercizio se A e B sono L-strutture finite allora

$A \equiv B \Rightarrow A \cong B$

Esempio. $L = \{0, 1, +\}$

$A = \mathbb{Z}/3\mathbb{Z}$ dove $(A) = \{0,1,2\}$

$A \equiv B \Rightarrow A \cong B$?

$\varphi = \exists a, b, c :$ $\boxed{\begin{array}{l} a+a=a \\ a+b=b \\ a+c=c \\ b+a=b \\ \ldots \\ c+c=b \end{array}}$ $a \ne b, a \ne c$ $b \ne c$

diagramma di A

$\forall u\,(u = a \vee u = b \vee u = c)$

Vedere definizione di elementare equivalenza.

(63)

[illegible] di Tarski - Vaught

strutture $A \subset B$

supponiamo che per ogni

formula $\exists y\, \varphi(y, x_1, \dots, x_n)$

per ogni $a_1 \dots a_n \in A$

se $B \models \exists y(\varphi(y, a_1 \dots a_n))$

allora $\exists a \in A \quad B \models \varphi(a, a_1 \dots a_n)$

Tesi: $A \preceq B$

$A \subset B \quad \varphi(\vec{x})$ è preservata se $\forall \vec{a} \in A$

$A \models \varphi(\vec{a}) \Rightarrow B \models \varphi(\vec{a})$ formule preservate all'in su

$\Leftarrow$ ... all'in giù

$\forall x \exists y\, (y > x)$ vera in $(0,1)$

falsa in $[0,1]$

non è preservata né all'in su né all'in giù perché ci sono due quantificatori diversi.

2 novembre 2007

Dimostrazione. Date $\varphi(x_1 \dots x_k)$ $a_1 \dots a_k \in A$

vale: $A \models \varphi(a_1 \dots a_k)$

$(*) \Updownarrow$

$B \models \varphi(a_1 \dots a_k)$

Se φ è atomica $(*)$ è vera per $A \subset B$

Se $\varphi = \varphi_1 \wedge \varphi_2$, $\varphi = \neg\varphi_1$, $\varphi = \varphi_1 \vee \varphi_2$ è ovvio.

Definiamo "per ogni" tramite "esiste":

$\forall x \theta \doteq \neg \exists x \neg \theta$

$\varphi = \exists x\, \varphi(x, y_1 \dots y_k)$

$A \models \exists x\, \varphi(x, a_1 \dots a_k) \Leftrightarrow \exists c \in A \;\; A \models \varphi(c, \vec{a}) \Leftrightarrow$

$\underset{\text{induzione}}{\Leftrightarrow} \exists c \in A \;\; B \models \varphi(c, \vec{a}) \underset{\text{ipotesi}}{\Leftrightarrow} B \models \exists x\, \varphi(x, \vec{a})$

(64) Teorema di Löwenheim - Skolem ↓

Sia M una L-struttura di cardinalità κ (qualunque cardinale).
Sia $A \subset dom(M)$. Sia $\lambda \leq \kappa$. Cerco una sottostruttura di M di cardinalità λ e che contenga A.
Allora $\exists N \preceq M$ $|N| = \lambda$ $A \subset dom(N)$ (cioè A è un sottoinsieme di N).
Deve essere $\lambda \geq \aleph_0, |L|, |A|$
(se $L = \{0, S\}$ allora $|L| = \aleph_0$ perché è la cardinalità dei termini)

Dimostrazione. Posso supporre $|\lambda| = A$ altrimenti considero un insieme che contiene A di cardinalità λ.
$|L_A\text{-formule}| = \lambda$.
Sia $\varphi(x) = \psi(x, a_1 \dots a_k)$ con $\psi(x, y_1 \dots y_k) \in L$
Data $\varphi(x) \in L_A$ formula tale che $M \models \exists x \varphi(x)$ scelgo $b_\varphi \in M$ $M \models \varphi(b_\varphi)$.
Sia $A_1 = \{b_\varphi \mid \varphi \in L_A\} \cup A$.
Definisco

$$\varphi(x) \in L_{A_n} - \text{formule}$$

$$M \models \exists x \varphi(x)$$

Scelgo $b_\varphi \in M$ $M \models \varphi(b_\varphi)$

$$A_{n+1} = A_n \cup \{b_\varphi \mid \varphi \in L_{A_n}\}$$

$$N = \bigcup_n A_n$$

Dato un sottoinsieme di una struttura o non c'è modo di renderlo una sottostruttura o ce n'è uno solo.
La sottostruttura deve contenere le costanti se ci sono ed

(b) essere chiuso rispetto alle operazioni

$(\mathbb{Z}, +, 0)$ gruppo. $(\mathbb{N}, +, 0)$ è una sottostruttura perché è chiusa rispetto alle operazione +.

N è una sottostruttura, cioè
se $c \in L$ $\quad c^M \in N$
$f \in L$ $\quad a_i \in L \Rightarrow f^M(a_i) \in N$

a_n " $\quad a_n$ "

Se $c \in L$ costante $M \models \exists x (x = c)$.
Allora in A_1 c'è c^M.

Se $A_1 \dots A_k \in A_n$ e $f \in L$
allora $f^M(a_1, \dots a_k) \in A_{n+1}$ perché
$M \models \exists x \underbrace{(x = f(a_1, \dots a_k))}_{L_{A_n}\text{-formula}}$

Questo dimostra che N è una sottostruttura
Bisogna dimostrare che N è elementare e per far questo basta verificare che il criterio di Tarski:
$M \models \exists x \varphi(x, \underbrace{a_1 \dots a_k}_{\in N}) \Rightarrow \exists c \in N \; M \models \varphi(c, a_1 \dots a_k)$

$\exists n \; a_1 \dots a_k \in A_n$ e lo trovo in A_{n+1}

Per induzione: $|A_n| = \lambda \; \forall n$

$|A_0| = \lambda$

$\underset{\uparrow}{\lambda} \leq |A_{n+1}| \leq |A_n| + |L_{A_n}\text{-formule}| \leq \lambda + \lambda = \lambda$
perché contiene A_n

(66) $\left|\bigcup_n A_n\right| \leq \sum_{n\in\mathbb{N}} |A_n| = \aleph_0 \cdot \lambda = \lambda$

Esempi: $\exists A \preccurlyeq (\mathbb{R},+,\cdot)$ $|A| = \aleph_0$ reali algebrici

$$(*)\begin{cases} M \models ZF & \exists A \preccurlyeq M,\ |A| = \aleph_0 \\ (N, e^*) \models ZF \end{cases}$$

M in (*) è un modello di ZF

$M \models \exists x\,(\forall y\ y \notin x)$ $\quad \phi$

$M \models \exists x\,(x = \{\phi\})$ $\quad \forall u\ u \in x \leftrightarrow u = \phi$

$\{\phi\}$ $\quad \exists x\,(x = a \cup b)$

Assioma delle parti

$M \models \exists x\,(x \ni 0$ chiuso per successione$)$

$M \models \exists x\,(x = \mathcal{P}\omega)$

$|\{\mathcal{P}\omega, \omega,$ dispari, $\ldots\}| =$ quantità numerabile.

Teorema di Lowenheim Skolem ↑

Se M è una L-struttura infinita e $k \geq |M|, |L|, \aleph_0$ allora esiste $B \succcurlyeq M$ tale che $|B| = k$.

Per avere $B \equiv M$ basta la compattezza. Infatti sia $T = Th(M) = \{\varphi \in L \mid M \models \varphi\}$

$B \models T \Rightarrow B \equiv M$

(6) $T' = \{c_i \neq c_j \mid i \neq j;\ i,j < k\} \cup T$

Ogni sottoinsieme finito di questo insieme ha un modello: basta prendere tante costanti distinte quanto $|\{c_i \neq c_j \mid \dots\}|$.

$\exists B' \models T'$ e $B = B'|_L$ $\quad B \models T$

$|B| = |B'| \geq k$ per avere $|B'| = k$ possiamo rimpicciolirlo con LS$\downarrow$.

Esercizio. La moltiplicazione $(N, +, \cdot, 0, S)$ su N non è definibile usando solo $+, 0, S$ al primo ordine.
Al secondo possiamo definire sia $+$ che $\cdot$ usando solo 0 e S.

Secondo ordine $P(x,y,z) \equiv x \cdot y = z$

$$\forall x,y,z\ (*)\ \begin{cases} P(x,0,0) \\ P(x,y,z) \wedge (z+x=w) \rightarrow P(x,Sy,w) \end{cases}$$

Definizione $a \cdot b = c \Leftrightarrow \forall P\ ((*) \rightarrow P(a,b,c))$

L'esponenziazione x^y è definibile usando al 1° ordine $+$ e $\cdot$.

$0, S, +, \cdot \underset{\text{(posso definire)}}{\rightsquigarrow} x^y$ e quasi tutto.

Definire vuol dire che dato $\varphi(x,y,z) \in L(0,S,+)$

$\forall a,b,c \in N \quad (N,+,0,S) \models \varphi(a,b,c) \Leftrightarrow ab = c$

 Dimostriamo che + non è definibile con 0, s.

Se lo fosse l'insieme dei pari sarebbe definibile.
Non c'è $\varphi(x) \in L(s,0)$ $\forall n$ $\mathbb{N} \models \varphi(n) \leftrightarrow n$ pari

Ammettiamo per assurdo che esista $\varphi(x)$.
Prendo per LST $M \succ \mathbb{N}$ $M \neq \mathbb{N}$
$M \setminus \mathbb{N}$ sono non standard
Questi numeri sono chiusi per successore e predecessore

$$\mathbb{N} \models \forall x(x \neq 0 \to \exists! y \; sy = x)$$
$$|||$$
$$M \models$$

M è fatto come tante copie di $\mathbb{N}$.
Definiamo $f : M \to M$

$$f\restriction_{\mathbb{N}} = id_{\mathbb{N}}$$

$$f\restriction_{M \setminus \mathbb{N}}(x) = S^M(x)$$

f è un isomorfismo
$$\begin{tikzcd} a \arrow[r, "s"] \arrow[d, "f"] & b \arrow[d, "f"] \\ c \arrow[r, "s"] & d \end{tikzcd}$$

In generale $f : A \xrightarrow{\sim} B$

$$A \models \varphi(a_1 \ldots a_n) \Leftrightarrow B \models \varphi(fa_1 \ldots fa_n)$$

$\varphi(x)$ = definisce i numeri pari in $\mathbb{N}$

$$M \models \varphi(a) \leftrightarrow \varphi(fa) \quad a \in M$$

$$\mathbb{N} \models \forall x[\varphi(x) \to \neg\varphi(sx)]$$

$$M \models \forall x[\varphi(x) \to \neg\varphi(sx)]$$

$a \in M \setminus \mathbb{N}$ $\quad M \models \varphi(a) \to \neg\varphi(sa) = fa$

Assurdo.

07 novembre 2007

A, B L-strutture

$A \preceq B \overset{def}{\Leftrightarrow} A \subset B$ e per ogni $\varphi(x_1 \dots x_n) \in$ L-formule

sottostruttura $\forall a_1 \dots a_n \in A$ $A \models \varphi(a_1 \dots a_n) \Leftrightarrow$
fondamentale $B \models \varphi(a_1 \dots a_n)$

Teorema di Lowenheim-Skolem ↑
Se A è una L-struttura infinita e $k \geq |A|$ allora $\exists B \succeq A$ $|B| = k$

Se A è finita e $B \equiv A \rightarrow B \cong A$
(per esempio $\mathbb{Z}/5\mathbb{Z}$)

Posso trovare modelli non numerabili che hanno le stesse strutture di $(\mathbb{N}, s, 0, +, \cdot)$.

Dimostrazione. A L-struttura
$Th(A) = \{\varphi \in$ L-formule chiuse $| A \models \varphi\}$
$ED(A) = \{\varphi \in L_A$-formule $| A \models \varphi\}$

$L_A = L \cup \{c_a | a \in A\}$ $A \models \varphi(c_a) \Leftrightarrow A \models \varphi(a)$

$ED(A)$ è completa in L_A
$Th(A)$ " L
(completa vuol dire che si dimostra una formula o la sua negazione).

$B \models Th(A) \Leftrightarrow B \equiv A$
$B \models ED(A) \Leftrightarrow B \succeq A$ a meno di isomorfismo in quanto
$\exists f : A \preceq B$
$A \models \varphi(a_1 \dots a_n) \Leftrightarrow B \models \varphi(f a_1 \dots f a_n)$

ED = Diagramma elementare

Nota: $A' = f(A) \subset B$

$A \underset{f}{\cong} A' \prec B$

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

f iniettiva: $A \to B$

anche surgettiva $A \to A'$

φ atomica $\quad A \models \varphi(a_1 \dots a_n) \iff$

$B \models \varphi(fa_1 \dots fa_n) \iff$

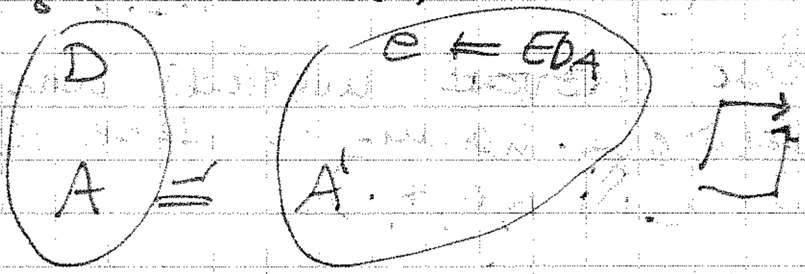
$A' \models \varphi(fa_1 \dots fa_n) \iff$

$A \cong A'$

$A' \models \varphi(fa_1 \dots fa_n) \iff A \models \varphi(a_1 \dots a_n)$

$\iff B \models \varphi(fa_1 \dots fa_n)$

Esercizio $\quad B \models ED(A) \iff \exists B' \cong B \quad B' \succeq A$



$\boxed{LST\uparrow}$ Sia A una L-struttura infinita $\kappa \geq |A|, |L|, \aleph_0$

$\exists B \succeq A \quad |B| = \kappa$.

Osservazione $T \cup ED(A)$ è coerente se e solo se $\exists B \underset{\sim}{\succeq} A$, $B \models T$

e se rimpiazzo B con una copia isomorfa $B \succeq A \quad B \models T$

Prendiamo come teoria

$T = \{c_i \neq c_j \mid i, j \in I, i \neq j\}, \quad |I| = \kappa$

$ED(A) \cup T$ è coerente (un modello $= A$ con $c_1 \dots c_N \mapsto a_1 \dots a_N \in A$)

(71) se $|B| \geq k$, $X \subset dom(B)$, $|A| = k$
con LST si ha $B' \subsetneq B$, $X \subset dom B'$.

Definizione. Una teoria è k-categorica se $\forall A, B \models T$
$|A| = |B| = k \quad A \cong B$

Una teoria può essere categorica solo se il modello è finito.

$Th(\mathbb{N}, S, 0)$ è $\aleph_0$-categorica? No

$T' = Th(\mathbb{N}, +, \cdot) \cup \{c \neq 0, c \neq S0, c \neq SS0, \dots\}$

Esempio. T = {ordini densi senza massimo e minimo} è $\aleph_0$-categorica e ha come modello numerabile $(\mathbb{Q}, <)$

$(\mathbb{Q} \cup \{\sqrt{2}\}, <) \cong (\mathbb{Q}, <)$

Teorema. Se T è k-categorica, $k \geq |L|, \aleph_0$, senza modelli finiti allora T è completa. Se inoltre T è ricorsivamente assiomatizzabile T è decidibile cioè esiste un algoritmo per riconoscere se una formula è un assioma della teoria o no.

Dimostrazione.
T è completa se $\forall \varphi$ allora $T \models \varphi$ o $T \models \neg\varphi$ (T ha almeno un modello, è coerente).
T è completa se e solo se $\forall A, B \models T$ $A \equiv B$.
Fissiamo $A, B \models T$. Se $|A| = |B| = k$ allora $A \cong B \Rightarrow A \equiv B$.

(72)

Sia $\lambda \geq |K|, |A|, |B|, |L|, \aleph_0$

Ottengo $A' \succ A$, $B' \succ A$, $|A'| \geq \lambda$, $|B'| \geq \lambda$

Poi $A'' \prec A'$, $B'' \prec B'$, $|B''| = |A''| = \kappa$.

$$A'', B'' \models T \quad A'' \cong B'' \quad A'' \equiv B''$$
$$\qquad\qquad\qquad\qquad\quad \equiv \quad\;\; \equiv$$
$$\qquad\qquad\qquad\qquad\quad A \quad\;\; B$$

$T_{<\text{densi}}$ = ordini lineari densi
senza max e min.
è $\aleph_0$-categorica, ma non $2^{\aleph_0}$ categorica

$$(\mathbb{R}, <) \not\cong (\mathbb{R} - \{0\}, <)$$

no $Th(\mathbb{R}, <, +, \cdot)$ è $\aleph_1$ categorica
ma non $\aleph_0$ categorica. $\aleph_1 \leq |\mathbb{R}|$

Siano $A, B \models T_{<\text{densi}}$ numerabili
$A = \{u_n \mid n \in N\}$ $B = \{v_n \mid n \in N\}$
(cioè enumero A e B in
un modo qualunque)
Definisco induttivamente
$a_0, a_1, \ldots \in A$, $b_0, b_1, b_2 \ldots \in B$
con $a_i \to b_i$
$f : a_0 = u_0 \longrightarrow v_0 = b_0$

Supponiamo di avere costruito
$f_n : \{a_0, \ldots, a_n\} \to \{b_0, \ldots, b_n\}$
isomorfismo
$a_i < a_j \Leftrightarrow b_i < b_j$
$a_i = a_j \Leftrightarrow b_i = b_j$
Sia n pari. Sia $a_{n+1} = u_i$, con
i = minimo indice in N
tale che $u_i \notin \{a_0, \ldots, a_n\}$

$$a_{n+1} \xrightarrow{f_{n+1}} b_{n+1} = \text{un qualunque } v_j$$
tale che
$$f_{n+1} : \{a_0, \ldots, a_{n+1}\} \xrightarrow{\cong} \{b_0, \ldots, b_{n+1}\}$$

(73) Sia n dispari. Sia $b_{n+1} = \bar{v}_i$ con i indice minimo $\bar{v}_i \notin \{b_0, \ldots, b_n\}$

$\bar{v}_i = b_{n+1} \longrightarrow a_{n+1} = a_j$

$f = \bigcup f_n : A \longrightarrow B$

$a_i \longmapsto b_i$ è un isomorfismo tra A e B.
È iniettiva per costruzione.
Surgettiva

9 novembre 2007

Due sistemi numerabili lineari densi senza estremi sono isomorfi. $(\mathbb{Q}, <) \cong (\mathbb{Q} \cup \sqrt{2}, <)$

Teorema. T κ-categorica è completa

PA è $\aleph_0$-categorica

Definizione. Siano A, B L-strutture. Un isomorfismo parziale finito da A a B è una coppia $((a_1 \ldots a_n), (b_1 \ldots b_n))$ $a_i \in A, b_i \in B$ con le proprietà che $a_i \mapsto b_i$ induce un isomorfismo cioè è un isomorfismo tra le strutture di A generate da $a_1 \ldots a_n$ e le strutture di B generate da $b_1 \ldots b_n$ che manda a_i in b_i.

Se questo isomorfismo esiste è unico

$I(A,B) \doteq \{(\vec{a}, \vec{b}) \mid (\vec{a}, \vec{b})$ è un isomorfismo parziale da A a $B\}$

$A = \mathbb{Z}/3\mathbb{Z}$ $\quad B = \mathbb{Z}/2\mathbb{Z}$ $\quad L = \{0, s\}$

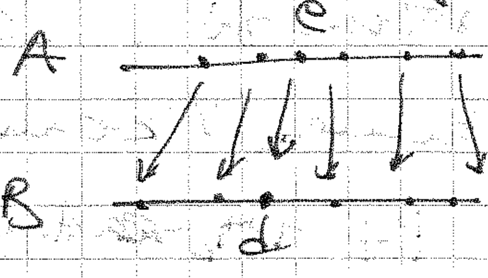
$I(A,B) = \phi$ $\quad$ $0 \mapsto 0$, $1 \mapsto 1$, $2 \mapsto 0$, $0 \mapsto 1$ $\quad$ Assurdo.

(74)

Definizione. $I(A,B)$ gode della proprietà del "va e vieni" se
$<(a_1 \ldots a_n), (b_1 \ldots b_n)> \in I(A,B) \Rightarrow$
$\forall c \in A \ \exists d \in B$ tali che
$<(a_1 \ldots a_n c) \ (b_1 \ldots b_n d)> \in I(A,B)$
$\forall b \in B \ \exists a \in A$ tali che
$< \ldots \ldots > \in \ldots$

Teorema. Se non è vuoto ($I(A,B) \neq \phi$) e $I(A,B)$ ha il va e vieni e $|A|, |B| \leq \aleph_0$ allora $A \cong B$.

Esempio. A, B ordini densi senza estremi



Dimostrazione. $|A| = |B| = \aleph_0$
$A = \{a_n \mid n \in N\}$ $B = \{b_n \mid n \in N\}$
Costruisco induttivamente una successione $a_1 a_0, \ldots \in A$ e $b_1, b_2 \ldots \in B$.
Sia $(\bar{a}, \bar{b}) \in I(A,B)$ un isomorfismo parziale.
Sia $(a_0, b_0) \in I(A,B)$. Ho già
$<(a_0 \ldots a_n), (b_0 \ldots b_n)> \in I(A,B)$
n pari pongo $a_{n+1} = a_{\frac{n}{2}}$
b_{n+1} tale che $(a_0 \ldots a_n a_{n+1}) (b_0 \ldots b_{n+1}) \in I(A,B)$.
n dispari: $b_{n+1} = b_{\frac{n+1}{2}}$ a_{n+1} tali che
$a_i \mapsto b_i$ è l'isomorfismo cercato.

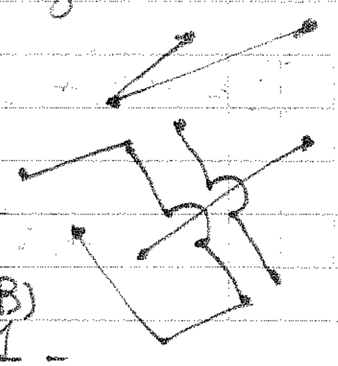
Teorema. $\phi \neq J \subset I(A,B)$, J ha il "va e vieni" allora se A e B sono numerabili ~~allora~~ $A \cong B$.
se A e B non sono numerabili $A \equiv B$

(19)

Esempio grafo casuale: infinito numerabile di punti ognuno con destro croce

V = vertici

$\{E\} = L \quad E \subset V^2$



Se A e B sono due grafi a caso numerabili $(A \cong B)$ hanno probabilità 1.

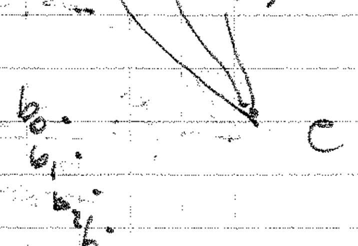
E verifica $\begin{cases} E(x,y) \leftrightarrow E(y,x) \\ \neg E(x,x) \end{cases}$ non sono orientato

I grafi casuali $L = \{E\}$

Assiomi: $E(x,y) \leftrightarrow E(y,x)$

$\neg E(x,x)$

Inoltre presi due punti a caso e quattro a caso esiste un c connesso ai primi e sconnesso agli altri



$U = \{a_1, a_2, a_3, \dots\}$

$V = \{b_1, b_2, b_3, \dots\}$

$\varphi_{k,n} : \forall a_1 \dots a_k \, \forall b_1 \dots b_n$

$\exists c \quad E(c,a_1) \wedge \dots \wedge E(c,a_k)$

$\neg E(c,b_1) \wedge \dots \wedge \neg E(c,b_k)$

T è $\aleph_0$-categorica

Se $A, B \models T$ grafi casuali allora

$\emptyset \neq I(A,B)$ ha il "va e vieni"

$\langle (a_1 \dots a_n), (b_1 \dots b_n) \rangle \in I(A,B)$

$E(a_i,a_j) \leftrightarrow E(b_i,b_j)$

$a_i \neq a_j \leftrightarrow b_i \neq b_j$

Scelgo $c \in A$. Trovare $d \in B$

$\langle (\bar{a}, c), (\bar{b}, d) \rangle \in I(A,B)$.

d deve essere connesso ai b_i connessi ai corrispondenti a_i

76

Sia $U = \{ b_i \mid E(c, a_i) \}$
$V = \{ b_i \mid \neg E(c, a_i) \}$

Esempio. T_{discr} = teoria degli ordini discreti

$L = \{ \leq \}$

Assiomi: $x \leq y \land y \leq z \Rightarrow x \leq z$
$x \leq x$
$x \leq y \land y \leq x \rightarrow x = z$

$\forall x \exists y (y = sx)$
$\forall x \exists y (y = px)$
$y = sx \leftrightarrow y > x \land \neg \exists z (y > z \land z > x)$

$y = px \leftrightarrow x = sy$ p predecessore, s successore

$(\mathbb{Z}, <) \models T_{discr}$

$(\mathbb{Z} \times \{0,1\}, <_{lex}) \models T_{discr}$

$\mathbb{Z} \not\models \underset{\mathbb{Z} \times \{0\}}{\underline{(a,0)}} < \underset{\mathbb{Z} \times \{1\}}{\underline{(b,1)}}$

$\Phi \not\models I(A,B)$ non è detto che abbia il "va e vieni"

Giocatore $\exists$ $(\mathbb{Z}, <)$ Giocatore $\forall$ $(\mathbb{Q}, <)$

$3^{\forall} \longrightarrow 3^{\exists}$
$4^{\forall} \longleftarrow 4^{\exists}$
$?^{\exists} \longleftarrow (3,5)^{\forall}$

Il giocatore $\exists$ perde

(77) **k-equivalenza** $\equiv_k$

Il giocatore $\exists$ può scrivere k mosse.

A, B L-strutture

$(a_0,\dots,a_n) \equiv_0 (b_0,\dots,b_n)$ se $(\vec{a},\vec{b}) \in I(A,B)$

$\vec{a} \equiv_{k+1} \vec{b} \iff \forall c\in A\ \exists d\in B\ (\vec{a}c)\equiv_k(\vec{b}d)$ e
$\forall d\in B\ \exists c\in A$

Esercizio. $(\equiv_{k+1}) \Rightarrow (\equiv_k)$

Teorema $A\equiv B \iff \forall k\ A\equiv_k B$ (FRAÏSSÉ)

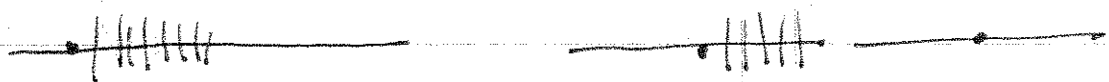
Esempio $\mathbb{Z}$ $A \equiv_\omega B$

$(\mathbb{R},<) \equiv_\infty (\mathbb{Q},<)$ perché questo gioco può non finire mai.

$\mathbb{Z} \equiv_\omega \mathbb{Z}*\mathbb{Z}$

$A+B \models T$ discreti $\Rightarrow A\equiv_\omega B \Rightarrow A\equiv B$

$\mathbb{Z} \not\equiv_\infty \mathbb{Z}+\mathbb{Z} = \mathbb{Z}\times\{0,1\}$



giocatore $\exists$ giocatore $\forall$

$a^\exists$ $(0,0)$

$b^\exists$ $(0,1)$

$(0,2)$

$(0,3)$

$\vdots$

Dopo $b-a$ mosse $\exists$ perde.

Se il gioco durasse 3 mosse $\exists$ potrebbe vincere.

(78) Teorema A, B ordini discreti $\Rightarrow$ se $A_k \equiv B_k$:

Dimostrazione Fissato k abbiamo una strategia del $\exists$. Consideriamo distanza equivalente di distanze $\leq 2^{\text{mosse rimanenti}}$

$$\vec{a} \to \vec{b} \quad a_i < a_j < b_i < b_j$$

$$d^*: A \to \mathbb{N} \cup \{\infty\} \quad d^*(a, a') = \begin{cases} d(a, a') & \text{se} < 2^k \\ \infty \end{cases}$$

$$d^*(a_i, a_j) = d^*(b_i, b_j)$$

$$\vec{a} \sim_k \vec{b} \Rightarrow \exists c \in A \; \exists d \in B \quad (\vec{a}, c) \sim_{k-1} (\vec{b}, d)$$

Corollario $\vec{a} \sim_k \vec{b} \Rightarrow \vec{a} \equiv_k \vec{b}$

14 novembre 2007

Data $f: \mathbb{N}^k \to \mathbb{N}$ vogliamo definire la nozione di calcolabilità. Intuitivamente se esiste un algoritmo che dato in input $a_1 \dots a_k \in \mathbb{N}$ fornisce in output $f(a_1 \dots a_k)$.

Esempio $MCD: \mathbb{N}^2 \to \mathbb{N} \quad (a, b) = (a-b, b)$

$$(a, 0) = a$$

Funzione non calcolabile. $L = \{+, \cdot\}$ corrispondenza biunivoca $\mathbb{N} \to \varphi$

$$n \mapsto \varphi_n$$

$$f(\varphi_n) = \begin{cases} 0 & \mathbb{N} \models \varphi_n \\ 1 & \mathbb{N} \models \neg\varphi_n \end{cases} \quad \text{non è calcolabile.}$$

Per dire che una funzione è calcolabile basta sapere se esiste un algoritmo ma non è necessario saperlo calcolare.

Esempio. $f: \mathbb{N} \to \mathbb{N}$

$$f(n) = \begin{cases} 0 & \text{se la congettura di Goldbach è vera} \\ 1 & \text{se non lo è} \end{cases}$$

f è costante quindi calcolabile.

Ogni funzione con dominio finito è calcolabile, basta fare una tabella e quindi consultarla

input	output
⋮	⋮

Macchina di Turing (1936):

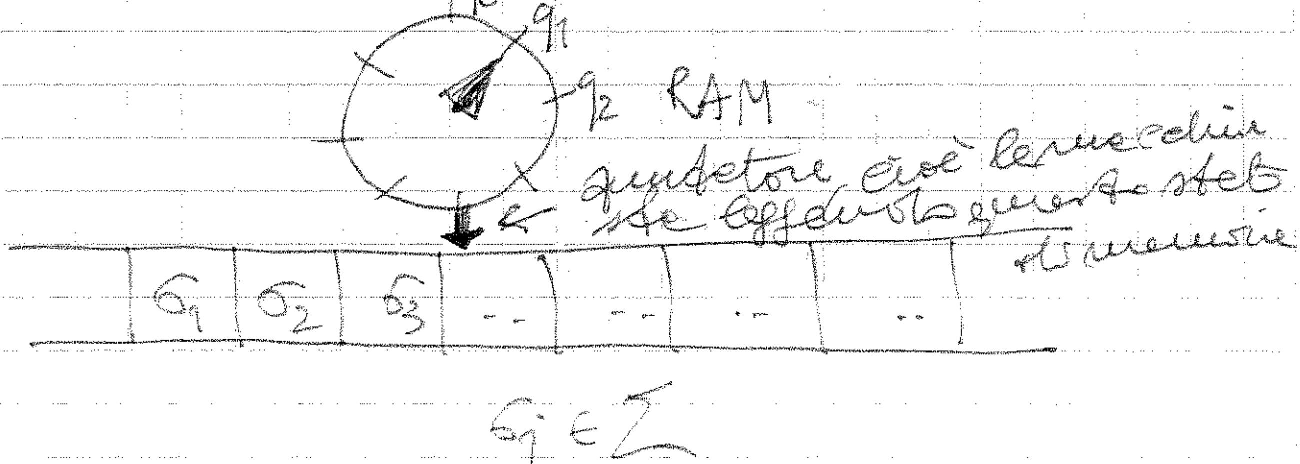
Σ = insieme finito di simboli
Q = — — stati

$$\delta: \Sigma \times Q \to \Sigma \times Q \times \{0, 1, -1\}$$

$a\ q$	$a'\ q'\ 1$
$a_1\ q_1$	$a_1'\ q_1'\ 0$

δ rappresenta il programma della macchina.

La macchina consiste di un nastro infinito (Hard Disk) e una memoria interna (RAM) finita



$\sigma_i \in \Sigma$

80

$0, 1, \sqcup \in \Sigma$, $\sqcup$ = bianco cioè non è scritto niente.

Se $\delta(\sigma_1, q_1) = (\sigma'_1, q'_1, 1)$ e il generatore incontra σ_1 allo stato q_1 a questo sostituisce q'_1 e σ'_1 e' $0, 1, -1$ dove se dopo questa operazione la macchina deve stare ferma o muoversi a destra o a sinistra.

Esempio. Somme : $\mathbb{N}^2 \to \mathbb{N}$ è Turing calcolabile.

input $3, 2 \to 5$ $\quad$ # = bianco

#	#	1	1	1	0	1	1	#

#	1	1	1	1	1	#

Σ	Q	Σ	Q	$\{0, 1, -1\}$	
#	q_0	#	q_1	1	← spostamento a destra
1	q_1	1	q_1	1	
0	q_1	1	q_2	1	q_2 nuovo stato
1	q_2	1	q_2	1	
#	q_2	#	q_3	-1	Quando si sposta a sinistra deve cancellare quello che trova
1	q_3	#	q_4	-1	
1	q_4	1	q_4	-1	
0	q_4	0	q_4	-1	
#	q_4	#	q_{fine}	0	

81

$\text{Turing}_g : (\Sigma')^* \rightharpoonup (\Sigma')^*$

$\Sigma' = \Sigma \setminus \{\#\}$, $(\Sigma')^*$ stringhe finite di elementi di Σ'

$\rightharpoonup$ funzioni parziali, cioè potrebbe non arrestarsi mai.

Tesi di Church =

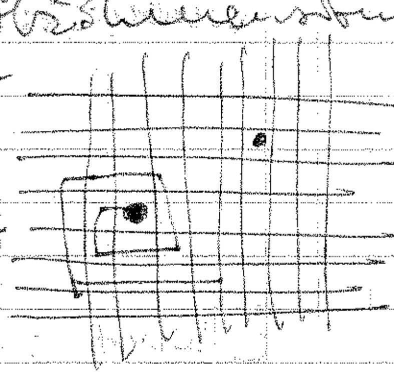
Turing calcolabile = intuitivamente calcolabile

(concetto intuitivo e concetto calcolabile)

È una tesi perché collega due argomenti diversi

Osservazione: se a è infinito tutte le funzioni risultano calcolabili.

Trovare un algoritmo che fa incontrare due galline su un quadro bidimensionale. Si fa muovere una gallina a spirale e si marca con 1 le caselle che ha già percorso.



Corollario della tesi di Church

Le funzioni calcolabili parziali da $\Sigma^* \to \Sigma^*$ sono $\aleph_0$ perché i programmi per macchine di Turing sono numerabili.

Esempio. $f: \mathbb{N} \to \{0,1\}$

$$f(n) = \begin{cases} 1 & \text{se fra } n \text{ giorni piove} \\ 0 & \end{cases}$$

f non è calcolabile perché le funzioni calcolabili se aumentiamo la velocità calcolano in metà tempo.

PR: Funzioni primitive ricorsive $f: \mathbb{N}^k \to \mathbb{N}$
totali (non parziali) cioè si terminano sempre
Sono contenute nelle calcolabili intuitive

$$Z : \mathbb{N} \to \mathbb{N} \quad Z(n) = 0 \quad \in PR$$
$$S : \mathbb{N} \to \mathbb{N} \quad S(n) = n+1 \quad \in PR$$
$$\pi_i : \mathbb{N}^n \to \mathbb{N} \quad \pi_i(a_1 \dots a_n) = a_i \quad \in PR$$

Composizione: $h, g_i \in PR \Rightarrow f \in PR$

$$f(x_1 \dots x_n) = h(g_1(x_1 \dots x_n), \dots, g_k(x_1 \dots x_n))$$

Ricorsione: $f(n+1, \vec{a}) = h(n, f(n, \vec{a}), \vec{a})$

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

$$h, g \in PR \to f \in PR$$

Esempi: $+, \cdot, x^y \in PR$

$$x \dot{-} y = \begin{cases} 0 & \text{se } x < y \\ x - y & \end{cases} \quad \in PR$$

$$x + 0 = x$$
$$x + (n+1) = S(x+n)$$

$$g(x,y) = f(y,x) = f(\pi_2(x,y), \pi_1(x,y))$$

(83)

$f(x,0) = x = \pi_1(x)$
$f(x,n+1) = S(f(x,n)) = h(n, f(x,n), x)$

$h(a,b,c) = S(b) = S(\pi_2(a,b,c))$

$x \cdot 0 = 0$
$x \cdot (n+1) = \text{somme}(xn, x)$

$x^0 = 1$
$x^{n+1} = x^n \cdot x$

$p(0) = 0$ predecessore
$p(n+1) = n = h(n, pn)$ $\quad \pi_1 = h(x,y) = x$

$x \dot{-} y$
$x \dot{-} 0 = 0$
$x \dot{-} (n+1) = p(x \dot{-} n)$

Predicato $=0$: $\chi_{=0} : \mathbb{N} \to \mathbb{N}$

$$\chi_{=0}(n) = \begin{cases} 0 & n \neq 0 \\ 1 & n = 0 \end{cases}$$

$\chi_{=0}(0) = 1$

$\chi_{=0}(n+1) = 0 = Z(n, \chi_{=0}(n)) \in PR$

$\chi_{=} : \mathbb{N}^2 \to \mathbb{N}$ $\quad \chi_{=}(x,y) = \begin{cases} 0 & \text{se } x \neq y \\ 1 & \text{se } x = y \end{cases}$

$\chi_{=}(x,y) = \chi_{=0}(x \dot{-} y) \cdot \chi_{=0}(y \dot{-} x)$

Un predicato o un insieme $\in PR$
se lo è la sua funzione caratteristica

Primi $\subset \mathbb{N}$ è primitivo ricorsiva

$P(x) \Leftrightarrow \forall u, v \leq x (u \cdot v = x \to u = 1 \vee v = 1)$

(84)

Predicato $P \subseteq \mathbb{N}^k$

$P(\vec{x})\ \vec{x} \in P$

$$\chi_P(\vec{n}) = \begin{cases} 1 & \text{se } n \in P \\ 0 & \text{se } n \notin P \end{cases}$$

$P, Q \in \mathbb{N}^k$ PR $\to$ $P(\vec{x}) \wedge Q(\vec{x})$, $P \cap Q$

$\neg P(\vec{x})$, $\mathbb{N} \setminus P$

$P(\vec{x}) \vee Q(\vec{x})$

$R(\vec{x}, z) \equiv \forall y \leq z\ P(\vec{x}, y)$

$\in$ PR

$$\chi_{P \wedge Q}(\vec{x}) = \chi_P(\vec{x}) \cdot \chi_Q(\vec{x}) = \min\{\chi_P(\vec{x}), \chi_Q(\vec{x})\}$$

$$\chi_{\neg P}(\vec{x}) = 1 \dot{-} \chi_P(\vec{x})$$

$$R(\vec{x}, z) \equiv \forall y \leq z \Rightarrow \chi_R(\vec{x}, z) = \prod_{y \leq z} \chi_P(\vec{x}, y)$$

$$\begin{cases} \chi_R(\vec{x}, 0) = \chi_P(\vec{x}, 0) \\ \chi_R(\vec{x}, n+1) = \chi_R(\vec{x}, n) \cdot \chi_P(\vec{x}, n+1) \end{cases}$$

$$\exists y \leq z\ P \equiv \neg \forall y \leq z\ \neg P$$

Corollario $\Delta_0 \subset$ formule $(+, \cdot, 0, 1)$

Per Δ_0 ci sono solo quantificazioni limitate

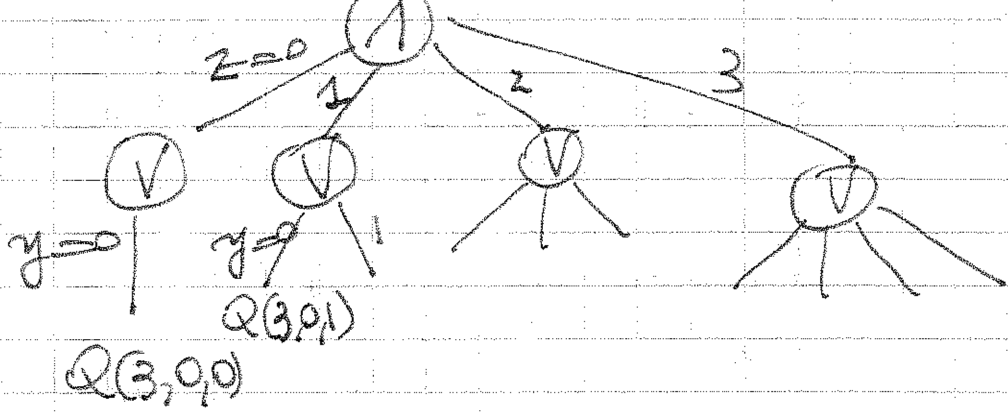
uso solo $\forall x \leq z, \exists x \leq z, \wedge, \vee, \neg ; +, \cdot, 0, 1, =$

$A \subset \mathbb{N}^k$ $A \in \Delta_0^{\mathbb{N}}$ se

$A = \{\vec{x} \mid \mathbb{N} \models \varphi(\vec{x})\}$ con $\varphi \in \Delta_0$

$\Delta_0^{\mathbb{N}} \subset$ PR $\subset$ intuitivamente calcolabile

(85) Sia $P(x) \equiv \forall z \leq x \, \exists y \leq z \; Q(x,y,z)$.
Voglio calcolare $P(3)$.



16 novembre 2007

Funzioni primitive ricorsive ⊂ funzioni calcolabili
(totali) (parziali)

<u>Minimalizzazione</u>

$f(x) = \min y \; P(x,y)$

Se P è un predicato PR allora f è intuitivamente calcolabile, però può essere parziale.

f è totale $\Leftrightarrow \forall x \exists y \; P(x,y)$

$f(x) = \mu y[g(x,y)=0]$ = minimo y tale che...

Funzioni μ-ricorsive: funzioni chiuse per Z, S, π_i^n, ricorsione, composizione, μ
μ = minimo se f è totale. Altrimenti:

Esempio. $g(1,0)=3$, $g(1,1)=\uparrow$, $g(1,2)=0$

prendo $f=\uparrow$ altrimenti non la so calcolare.

(36)

$f(x) = b \iff g(x, b) = 0$
$\forall h < b \quad g(x, h) \neq 0$ ma $\downarrow$
($\downarrow$ = definita)

$f(x) = \uparrow$ (cioè indefinita) se non esiste tale b.

$f(x) = h(g_1(x), \dots, g_k(x))$

$f(x)\downarrow \iff g_1(x)\downarrow \dots g_k(x)\downarrow$
$\quad\quad\quad\quad\quad \shortparallel \quad\quad\quad\quad \shortparallel$
$\quad\quad\quad\quad\quad a_1 \quad\quad\quad\quad a_k$

$h(a_1 \dots a_k) = \downarrow$

$f(x) = Z(g(x))$

Esempio di funzione PR:
$f(0) = a$
$f(n+1) = \dots$

Le funzioni μ-calcolabili = funzioni calcolabili di Turing.
Una tesi è che esse siano intuitivamente calcolabili.

Teorema Se f è μ-calcolabile
μ ricorsiva allora
$f(x) = U(\mu y\ P(x, y))$ con U e P
primitive ricorsive
In questo caso μ compare
con il minimo.
(Forma normale di Kleene)

Una macchina a registri ha registri
di memoria (X, Y, Z, ...)
istruzioni
- $x = 0$
- $x = x+1$
- $x = y$
- se $x = y$ vai a q.
- se $x = y$ stop, con output Z
- input

(87) Un programma è una successione finita di istruzioni $I_1 \ldots I_k$

$:=$ assegnazione.

L'esecuzione di una istruzione determina un cambiamento di stato.

Uno stato è una coppia (memoria, contatore)

$$\left.\begin{matrix} x, y, z & - & - & c \\ 3\ 3\ 4 & & & 8 \end{matrix}\right\} \text{stato}$$

Se I_8 è se $x=y \Rightarrow$ vai a 5 lo stato diviene

3 3 4 5

Queste macchine possono per esempio invertire una matrice 5x5 ma non possono invertire una matrice NxN.

Teorema. μ-ricorsive = calcolabili registri.

Dimostrazione:

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

g, h calcolabili registri $\Rightarrow$ f lo è.

1) input x, y (y è un parametro)
2) $z := g(x)$ gruppo di istruzioni per calcolare la g
3) $k := 0$ contatore
4) se $k = y$ output z
5) $z := h(x, k, z)$

6) $k := k+1$
7) vai a quello.

Esempio $f(x,2)$

	x	y	z	k
2)		a	2	$g(a)$
3)		a	2	$g(a)$
4)				0
5)				$h(a,1,g(a))$
6)				$f(a,1)$
				1

Le 2) e le 5) sono blocchi d'istruzioni

Se disponiamo di un programma per calcolare la g vogliamo un programma che calcoli f.

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

1) input x
2) $z := 0$
3) $u := g(x,z)$
4) se $u=0$ output z
5) $z := z+1$
6) vai a 3

3) è un blocco di istruzioni

Funzione parziale: dato un programma P (input $x_1 \dots x_k$) esiste una funzione $\varphi_P : N^k \to N$ tale che $\varphi_P : N^k \to N \cup \{\uparrow\}$ e $\varphi_P(\bar{a}) = \uparrow$.
$\varphi_P(\;) = \uparrow^P$ se il programma non si termina.

(89) while = minimalizzazione

for (i=1 ... n) do : ricorsione primitiva

Per assurdo sia $\mathcal{L}$ un linguaggio di programmazione che calcola tutte e sole le funzioni calcolabili. Sia P_n l'n-esimo programma

$D: \mathbb{N} \to \mathbb{N}$
$D(n) = P_n(n) + 1$.

D è intuitivamente calcolabile e totale, ma $D \neq P_z$
(D diagonale)

Minimalizzazione limitata

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

Sia $f(\vec{x}, y) = \mu z < y\, [h(\vec{x}, z) = 0]$

$$= \begin{cases} \min z < y \;\; h(\vec{x}, z) = 0 & \text{se } \exists z \\ y & \end{cases}$$

h PR $\Rightarrow$ f PR

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

$$f(\vec{x}, y+1) = \begin{cases} f(\vec{x}, y) & \text{se } \exists z < y \;\; h(\vec{x}, z) = 0 \\ y & \text{se } \neg\exists z < y \;\; h(\vec{x}, z) \wedge h(\vec{x}, y) = \\ y+1 & \text{altrimenti} \end{cases}$$

$$f(x) = \begin{cases} f_1(x) & \text{se } P_1(x) \\ f_2(x) & \text{se } P_2(x) \end{cases}$$

$f(x) = f_1(x) \cdot \chi_{P_1}(x) + f_2(x) \cdot \widehat{\chi_{P_2}}(x)$

90 Esercizio $F_0 = 1 \quad F_1 = 1$

$$F_{n+2} = F_{n+1} + F_n$$

$F(n)$ è primitiva ricorsiva

Esercizio $f(n+1) = h_1(g(n))$
$g(n+1) = h_2(f(n))$
$f_0 = g_0 = 0$

h_1, h_2 PR $\Rightarrow f, g$ PR

21 novembre 2007

Funzioni primitive ricorsive
$\cap$
funzioni μ-ricorsive totali
$\cap$
funzioni μ-ricorsive
$=$
intuitivamente calcolabili

Teorema Le funzioni μ ricorsive coincidono con le funzioni Turing calcolabili.

$f(y,z) = \mu x < z \; h(x,y) = 0$ (h totale)

$= \begin{cases} \min x \text{ tale che } h(x,y) = 0, \text{ se } \exists x < z \; h(x,y) \\ z \quad \text{altrimenti} \end{cases}$

Definizione $P \subseteq \mathbb{N}^k$ (predicato)
$P(\vec{x}) \Leftrightarrow \vec{x} \in P$
P è ricorsivo (decidibile) $\Leftrightarrow \chi_P : \mathbb{N}^k \to \{0,1\}$ è μ-ricorsiva

(Ogni funzione caratteristica è totale)

(91) Definizione. P è ricorsivamente enumerabile se e solo se

1) $P = \{\vec{x} \mid \exists y\, Q(\vec{x}, y)\}$ con Q ricorsivo

2) $P = \emptyset \vee P = \{a_n \mid n \in \mathbb{N}\}$ con $n \mapsto a_n$ ricorsiva (equivalentemente μ-ricorsiva o PR)

3) esiste una funzione μ-ricorsiva h (anche parziale) tale che

$$x \in P \Rightarrow hx = 1$$
$$x \notin P \Rightarrow hx = \uparrow \quad \forall x \in \mathbb{N}^k$$

$$1) \Leftarrow 2) \Leftarrow 3)$$

$2) \Rightarrow 1)$: $P = \{a_n \mid n \in \mathbb{N}\} = \mathrm{Im}(h) \quad hn = a_n$
h μ-ricorsiva totale

$x \in P \Leftrightarrow \exists n\, [x = h(n)]$ $\quad x = h(n)$ è un predicato ricorsivo

$1) \Rightarrow 3)$: se $P = \{x \mid \exists y\, Q(x, y)\}$

pongo $h(x) = \text{costante}_1(\mu y\, Q(x, y))$

$\mathrm{Dom}(h') = P$

$3) \Rightarrow 2)$: serve il teorema della funzione universale

Teorema della funzione universale

$\{f \mid f : \mathbb{N}^n \rightharpoonup \mathbb{N} \text{ μ ricorsiva}\} = \{\varphi_e \mid e \in \mathbb{N}\}$

dove φ_e può essere scelta in modo che

$\varphi_e(\vec{x}) = U(e, \vec{x})$ con U μ ricorsiva.

$\{(e, \vec{x}, t) \mid \varphi_e(\vec{x})\downarrow_t\}$ è PR ($\downarrow_t$ = convergendo t passi)

92

$\{(e,\vec{x},t,y) \mid \varphi_e(\vec{x})_t = y\}$ è PR

$\langle , \rangle : \mathbb{N}^2 \to \mathbb{N}$

$\langle x, y \rangle = 2^x 3^y = n$ è iniettiva ma non biunivoca

Dato n possiamo ricavare x e y

$x = \mu z(\ldots)$

In generale: $U'(e,\vec{x}) = \mu n(\exists y\, t \le n$
$n = 2^y 3^t \wedge \varphi_e(x)_t = y)$

$U(e,x)$ = prima componente di $\underbrace{U'(e,x)}_{n}$

$= \mu y \le n\,(\exists t \le n\ \langle y,t\rangle = n)$

3) → 2): sia $P \subseteq \mathbb{N}^k$ $\quad x \to \boxed{x \in P?} \to 1, \uparrow$ (h)

$h = \varphi_e$ per il teorema

$x \in P \Leftrightarrow \exists t\, \underbrace{[\varphi_e(x)\downarrow_t]}_{PR}$

Teorema di Post. Un predicato $P \subset \mathbb{N}^k$ è ricorsivo se e solo se P è ricorsivamente enumerabile e $\neg P$ è ricorsivamente enumerabile

Osservazione: R.C. ⇒ R.E. $\quad Ind(0) = 1$
$Ind(x) = \mu y(y \ne 0)$

In base a questa osservazione si ha il verso ⇒ del teorema.

⇐ : $x \to \boxed{x \in P?} \to 1, \uparrow$: φ_e

$x \to \boxed{x \notin P} \to 1$: φ_s $\quad e, s \in \mathbb{N}$

(22) $\varphi_e, \varphi_s \in \{$ PR parziali $\}$

$$T(x) = \mu t\, [\underbrace{\varphi_e(x)\downarrow_t \vee \varphi_s(x)\downarrow_t}_{PR \text{ in } x,t}]$$

T è totale. $x \in P \Leftrightarrow \underbrace{\varphi_e(x)\downarrow_{T(x)}}_{PR \text{ in } x}$

Codifiche

$\langle a_1, \dots, a_n \rangle \xrightarrow{cod} \prod_{i=1}^{n} p_i^{a_i+1}$, $a_i \in N$

N^* = successioni finite di numeri

p_i = i-esimo numero primo

Non ha senso chiedere se $cod: N^* \to N$ sia PR o calcolabile

Ha senso chiedere se la funzione inversa è ricorsiva.

estrai(n,i)

estrai : $N^2 \to N$ è PR

estrai$\left(\prod_{i=1}^{n} p_i^{a_i+1}, k\right) = a^k$

$$\text{estrai}(n,i) = \mu a \leq n\, [\underbrace{p_i^{a+1} \mid n \wedge p_i^{a+2} \nmid n}_{PR(i,a,n)}]$$

$i \mapsto p_i$ è PR

$p(0) = 2$

$p(i+1) = \mu x\, (x \text{ è primo} \wedge x > p(i))$

$\leq 2p(i)$

(94) cat : $\mathbb{N}^2 \to \mathbb{N}$ concatenazione

$$\mathrm{cat}(\underbrace{\langle a_0 \dots a_n\rangle}_{\prod_{i=0}^{n} p_i^{a_i+1}}, \langle b_0 \dots b_k\rangle) = \underbrace{\langle a_0 \dots a_n b_0 \dots b_k\rangle}_{z}$$

$$\prod_{r \le x+y} p_r$$

$$\mathrm{cat}(x,y) = \mu z \le \prod p_r \quad \forall i \le lh(x) = \mu n\,[p_{n+1} \nmid x]$$

$\forall i \le lh(x)$ Estrai(x,i) = Estrai(z,i)

$\forall j \le lh(y)$ Estrai$(z, j+lh(x))$ = Estrai(y,j)

$$\begin{array}{ccc}
\mathbb{N}^* \times \mathbb{N}^* & \xrightarrow{\text{concat}} & \mathbb{N}^* \\
\text{cod}\downarrow \quad \downarrow & & \downarrow \text{cod} \\
\mathbb{N} \times \mathbb{N} & \xrightarrow[\text{cat}]{} & \mathbb{N}
\end{array}$$

Supponiamo di voler dimostrare che x^y è definibile in $(\mathbb{N}, +, \cdot, S, 0)$ cioè esiste $\varphi(x\,y\,z) \in L(+, \cdot, S, 0)$ cui $a^b = c$ se e solo se $\mathbb{N} \models_T \varphi(a,b,c)$

verifica

Se fosse $(\mathbb{N}, +, \cdot, S, 0, \text{estrai})$ x^y sarebbe definibile infatti:

$$x^y = z \Leftrightarrow \exists n\,[\text{estrai}(n, y) = z \wedge \text{estrai}(n,0) = 1 \wedge \forall i < y\ \text{estrai}(n, i+1) = \text{estrai}(n,i) \cdot x]$$

$[\dots]$ è definibile

Teorema cinese del resto.

$$MCD(a_i, a_j) = 1 \quad \forall i \neq j$$

$$\exists x : \begin{cases} x \equiv b_1 & (a_1) \\ \vdots \\ x \equiv b_k & (a_k) \end{cases}$$

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

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

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

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

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

23 novembre 2007

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

Codifica successioni finite di interi

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

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.

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

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

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

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

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

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: $f(x)=h(x,\langle f(0),\ldots,f(x-1)\rangle)=$

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

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

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

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

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

$\# =$ sharp

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

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