Funzioni "CALCOLABILI"

$\longrightarrow$ $Th(\mathbb{N},+,\cdot,S,0)$ è "INDECIDIBILE", cioè $\{\ulcorner\sigma\urcorner \mid \mathbb{N}\models\sigma\}\subseteq\mathbb{N}$ è <u>INDECIDIBILE</u>.

"codifica effettiva" dell'enunciato σ

$\operatorname{dom} f \subsetneq \mathbb{N}^k$

Def. "INFORMALE": una funzione $f:\mathbb{N}^k\to\mathbb{N}^h$ (anche parziale) è CALCOLABILE se esiste un "<u>programma</u>" P t.c. se ho $(n_1,\dots,n_k)$ come input restituisce $f(n_1,\dots,n_k)$ in output.

Oss.: le funzioni calcolabili sono una quantità numerabile (i programmi sono insiemi finiti di "istruzioni" date in un linguaggio al più numerabile), quindi non tutte le funzioni sono calcolabili.

Se $(n_1,\dots,n_k)\in\operatorname{dom} f$ scriviamo $f(n_1,\dots,n_k)\downarrow$ (il programma termina), altrimenti scriviamo $f(n_1,\dots,n_k)\uparrow$ (" " non si arresta).

Es.: $f(n_1,n_2)=\gcd(n_1,n_2)$ e $f(n)=n$-esimo numero primo sono calcolabili;

$f(n)=\begin{cases}1 & \text{se } \exists\, p,p+2\geq n \text{ primi}\\ 0 & \text{altrimenti}\end{cases}$ è calcolabile, sia se la congettura dei primi gemelli è vera sia se è falsa.

Es.: 10° prob. di Hilbert: $a_0+a_1x+\dots+a_nx^n$ ha radici intere?

$f(a_0,\dots,a_n)=\begin{cases}1 & \text{se } \exists x\in\mathbb{Z} \text{ t.c. } " = 0\\ 0 & \text{altrimenti}\end{cases}$ non è calcolabile.

Def.: $A\subseteq\mathbb{N}^k$ si dice DECIDIBILE se $\chi_A:\mathbb{N}^k\to\{0,1\}$ (funzione caratteristica) è calcolabile.

Def.: $A\subseteq\mathbb{N}^k$ è SEMIDECIDIBILE (o RICORSIVAMENTE NUMERABILE) se esiste f calcolabile totale t.c. $\operatorname{Im} f=A$.

Decidibile $\Longrightarrow$ semidecidibile.

Prop.: TFAE:

(1) A semidecidibile;
(2) $A=\operatorname{dom} f$ dove f è calcolabile.

Dim.: (1) $\Rightarrow$ (2) $A=\{f(n)\mid n\in\mathbb{N}\}$ dove f è calcolabile totale.
Dato x, controllo se $x=f(0)$: sì termino, no controllo se $x=f(1)$, eccetera.
Questo programma termina $\iff x\in A$.
(2) $\Rightarrow$ (1) Ho un programma P che ha un output su $x \iff x\in A$. $f:\mathbb{N}\times\mathbb{N}\to\mathbb{N}$.
$f(n,m)\longmapsto$ calcolo P con input n per m passi
Se ho un output, $f(n,m)=n$.
Altrimenti, $f(n,m)=\tilde{a}\in A$ qualunque. $\square$

Teo. (Post [informale]): se $A\subseteq\mathbb{N}^k$, TFAE:

(1) A decidibile;
(2) A e A^c decidibili;
(3) A e A^c semidecidibili.

Dim.: (1) $\Rightarrow$ (2) $\Rightarrow$ (3) facili.
(3) $\Rightarrow$ (1). $A=\{f(n)\mid n\in\mathbb{N}\}$, $A^c=\{g(n)\mid n\in\mathbb{N}\}$, f,g calcolabili totali. Dato x:
controllo se $x=f(0)$ o $x=g(0)$;
" se $x=f(1)$ o $x=g(1)$ ....
Termina, se x è dato da f restituisco 1,
se è dato da g " 0. $\square$

<u>URM-calcolabili</u>

unlimited register machine

r_0	r_1	r_2	...	r_k
0	n_1	n_2	...	n_k

Istruzioni:

$Z(n)$ $\quad r_n:=0$ "ZERO";
$S(n)$ $\quad r_n:=r_n+1$ "SUCCESSORE";
$T(n,m)$ $\quad r_m:=r_n$ "TRASFERIMENTO";
$J(m,n,q)$ "se $r_m=r_n$ allora passa all'istruzione $\#q$, altrimenti passa all'istruzione successiva" "JUMP";
STOP.

Un programma P è una lista finita numerata $I_1,\dots,I_n$ di istruzioni.

Es.: $+:\mathbb{N}^2\to\mathbb{N}$ è URM-calcolabile:
$T(1,0)$, $J(2,3,6)$, $S(0)$, $S(3)$, $J(0,0,2)$, STOP.

Ex.: $\cdot:\mathbb{N}\times\mathbb{N}\to\mathbb{N}$ è URM-calcolabile.

Ex.: T non è mai strettamente necessaria.

Le seguenti funzioni base sono URM-calcolabili:

- $Z:\mathbb{N}^k\to\mathbb{N}$ funzione zero;
- $S:\mathbb{N}\to\mathbb{N}$ " successore;
- $U_i^k:\mathbb{N}^k\to\mathbb{N}$ proiezione sulla i-esima componente.

I programmi si possono concatenare "con cautela".

Le funzioni URM-calcolabili sono chiuse per le seguenti operazioni:

1) se $f:\mathbb{N}^k\to\mathbb{N}$ e $g_i:\mathbb{N}^h\to\mathbb{N}$ $i=1,\dots,k$,
$f\circ(g_1,\dots,g_k):\mathbb{N}^h\to\mathbb{N}$, COMPOSIZIONE;

2) RICORSIONE PRIMITIVA: $f:\mathbb{N}^k\to\mathbb{N}$, $g:\mathbb{N}^{k+2}\to\mathbb{N}$,
$$\begin{cases}h(n_1,\dots,n_k,0)=f(n_1,\dots,n_k)\\ h(n_1,\dots,n_k,y+1)=g(n_1,\dots,n_k,y,h(n_1,\dots,n_k,y)).\end{cases}$$

Def.: f è PRIMITIVA RICORSIVA se si ottiene a partire dalle funzioni base applicando un numero finito di volte 1) e 2) sopra.

Ex.: sono funzioni PR: le costanti, l'identità, somma, prodotto, fattoriale, esponenziale, min, max, resto, gcd.

Ex.: se $f(\vec{x},y)$ è PR, anche $\sum_{i\leq y} f(\vec{x},i)$ e $\prod_{i\leq y} f(\vec{x},i)$ lo sono.

Def.: la classe $\mathcal{C}\subseteq\bigcup_k \mathrm{Fun}(\mathbb{N}^k,\mathbb{N})$ delle funzioni CALCOLABILI secondo Gödel–Kleene è la più piccola classe che contiene le funzioni base ed è chiusa per 1) e 2) sopra e
3) MINIMALIZZAZIONE: $f:\mathbb{N}^{k+1}\to\mathbb{N}$,
$$\mu y(f)(a_1,\dots,a_k)=\begin{cases}n=\min\{y\mid f(a_1,\dots,a_k,y)=0\} & \text{se esiste e se } f(a_1,\dots,a_k,t)\downarrow\ \forall t<n\\ \uparrow & \text{altrimenti}\end{cases}.$$

Ex.: se f è URM-calcolabile, anche $\mu y(f)$ lo è.

Teo.: URM-calcolabile $\iff$ GK-calcolabile.

Dim.: $\supseteq$: visto. $\subseteq$: non difficile, ma ci vuole attenzione. $\square$

Tesi di Church: le funzioni "intuitivamente" calcolabili sono le GK-calcolabili.

$\underbrace{PR}_{\text{hanno crescita "limitata"}}\subsetneq$ totali calcolabili $\subsetneq$ calcolabili.

Spoiler: ogni funzione calcolabile $f:\mathbb{N}^k\to\mathbb{N}$ è DEFINIBILE in $(\mathbb{N},+,\cdot,S,0)$, cioè $\exists\varphi$ t.c. $\mathrm{Graph}(f)=\{(n_1,\dots,n_k,m)\mid\mathbb{N}\models\varphi(n_1,\dots,n_k,m)\}$.