(E)numerabilità

Eugenio Omodeo

4 maggio 2021

1 Si possono numerare gli insiemi di numeri naturali? (No)

Può esistere una successione infinita $\boldsymbol{s}_0, \boldsymbol{s}_1, \boldsymbol{s}_2, \ldots$ formata da tutti i sottoinsiemi di

$$\mathbb{N} \quad = \quad \{0, 1, 2, 3, \ldots\}$$

(ripetizioni ammesse) ?

Teorema 1 *No!*

Dim.: Ragionando per assurdo, supponiamo che una tale successione esista: dunque, a ogni sottoinsieme (finito o infinito) S di $\mathbb{N}$ corrisponde almeno un indice $j \in \mathbb{N}$ tale che $S = \boldsymbol{s}_j$. Allora, fra gli altri, all'insieme 'diagonale' $\{\, m \in \mathbb{N} \mid m \notin \boldsymbol{s}_m \,\}$ costituito da tutti e soli i numeri naturali m che non appartengono al corrispondente insieme $\boldsymbol{s}_m$, compete un indice—chiamiamolo $\boldsymbol{m}_\star$ —tale che

$$\boldsymbol{s}_{\boldsymbol{m}_\star} \quad = \quad \{\, m \in \mathbb{N} \mid m \notin \boldsymbol{s}_m \,\} \ .$$

Ma allora avremo la doppia implicazione

$$\boldsymbol{m}_\star \in \boldsymbol{s}_{\boldsymbol{m}_\star} \quad \text{se e solo se} \quad \boldsymbol{m}_\star \notin \boldsymbol{s}_{\boldsymbol{m}_\star} \ ,$$

che ci dà la contraddizione cercata. $\dashv$

2 Si può formare un elenco di tutti gli insiemi elencabili di numeri naturali? (Sí)

Concetti intuitivi	Nozioni matematiche
calcolabile	computabile
procedimento effettivo	procedimento ricorsivo
insieme elencabile	insieme enumerabile ricorsivamente
insieme effettivo	insieme decidibile

Figura 1: Concetti intuitivi e loro omologhi in teoria della calcolabilità

Affrontiamo qui il concetto intuitivo di insieme '*elencabile*', ossia di insieme E i cui elementi possano venir generati (o 'stampati', per concretezza) tramite un procedimento '*effettivo*'. A tale concetto la teoria della computabilità sostituisce una nozione matematica rigorosa: quella di insieme *enumerabile ricorsivamente*, su cui torneremo fra poco.

Consideriamo 'elencabili', fra i sottoinsiemi di $\mathbb{N}$, non solo tutti quelli finiti ma anche un'infinità di insiemi infiniti, tra cui: i numeri dispari, i numeri primi, i multipli di un qualsiasi intero positivo fissato. Se non altro per tener conto di insiemi come questi, il procedimento algoritmico che genera gli elementi di un insieme elencabile dovrà potersi dilungare all'infinito. Restando ancora sul versante intuitivo, va precisato che l'elencazione non è da intendersi in ordine crescente. Gli elementi di un insieme possono, dunque, venir elencati alla rinfusa; tolleriamo, inoltre, che nell'elenco figurino doppioni o repliche multiple.

Anche il concetto di 'procedimento effettivo' è indistinto e informale: spesso, in letteratura, al termine 'effettivo' viene prescelto (intendendo la stessa cosa) il termine 'meccanico', 'automatico', o 'algoritmico'.

Qualsiasi testo di teoria della computabilità propone uno o piú linguaggi di programmazione che, per quanto ridotti all'essenziale, permettono di specificare tutte le operazioni 'calcolabili' dei naturali nei naturali—ci bastano le operazioni ad un solo operando. A certi valori dell'operando l'operazione associa un risultato; tuttavia ammettiamo che possano esservi valori cui un'operazione non associa alcun risultato. Serviamoci di una metafora: diciamo che in certe situazioni il dispositivo di calcolo, invece di produrre risultato, s'impantana in un'eternità di conti. Accogliendo computazioni perpetue, stiamo facendo di necessità virtú: difatti, non è possibile conciliare una versatilità completa del modello di computazione con l'adozione di un linguaggio in cui si possano specificare solo procedimenti che hanno sempre termine.

Grazie a delle tecniche note come *gödelizzazione*, si riesce a istituire una corrispondenza biunivoca fra i programmi del linguaggio adottato—che sono espressioni rispondenti a una particolare sintassi—e i numeri naturali. Tutti i programmi vengono cosí a formare una successione infinita, $\varpi_0, \varpi_1, \varpi_2, \ldots$, partendo dalla quale otteniamo la successione $\boldsymbol{f}_0(x), \boldsymbol{f}_1(x), \boldsymbol{f}_2(x), \ldots$ di tutte le operazioni (parzialmente)[1] computabili nell'operando x.

Indichiamo con D_i ed R_i, rispettivamente:

- l'insieme dei valori $\boldsymbol{v}$ dell'operando tali che $\boldsymbol{f}_i(\boldsymbol{v})$ dia risultato;
- l'insieme dei risultati $\boldsymbol{f}_i(\boldsymbol{v})$ corrispondenti ai valori $\boldsymbol{v}$ in D_i.

Vi sono due modi—uno equivale all'altro, ma non lo dimostro—di caratterizzare i sottoinsiemi *enumerabili ricorsivamente* di $\mathbb{N}$ e dunque di catturare formalmente il concetto intuitivo di 'elencabilità':

- si tratta degli insiemi D_i ;
- si tratta di $\emptyset$ e di tutti quegli insiemi R_i tali che l'indice i soddisfi $D_i = \mathbb{N}$ (in altre parole, $\boldsymbol{f}_i(x)$ è un'operazione che dà sempre risultato).

[1] Il 'parzialmente', qui, vuol appunto richiamare la problematica della non-terminazione.

Fatto d'importanza cruciale—che qui mi limito a citare—: un sottoinsieme S di $\mathbb{N}$ è *decidibile*, vale a dire, è tale che l'operazione

$$f(\boldsymbol{v}) \quad = \quad \begin{cases} 1 & \text{quando } \boldsymbol{v} \quad \text{sta in} \quad S \\ 0 & \text{quando } \boldsymbol{v} \quad \text{non sta in} \quad S \end{cases}$$

sia computabile, se e solo se tanto S che il suo complemento $\mathbb{N} \setminus S$ sono enumerabili ricorsivamente.

Per 'diagonalizzazione', in analogia col § 1, è facile mostrare che un certo insieme K, enumerabile ricorsivamente, non può essere decidibile. Eccolo:

$$K \quad =_{\text{Def}} \quad \{\, m \in \mathbb{N} \mid \boldsymbol{f}_m(m) \text{ dà risultato} \,\} \ .$$

In effetti, dall'assurda ipotesi che $\mathbb{N} \setminus K = D_{\boldsymbol{m}_\star}$ valga per qualche $\boldsymbol{m}_\star$ discende la contraddizione

$$\boldsymbol{f}_{\boldsymbol{m}_\star}(\boldsymbol{m}_\star) \text{ dà risultato} \quad \text{se e solo se} \quad \boldsymbol{f}_{\boldsymbol{m}_\star}(\boldsymbol{m}_\star) \text{ non dà risultato} \ .$$

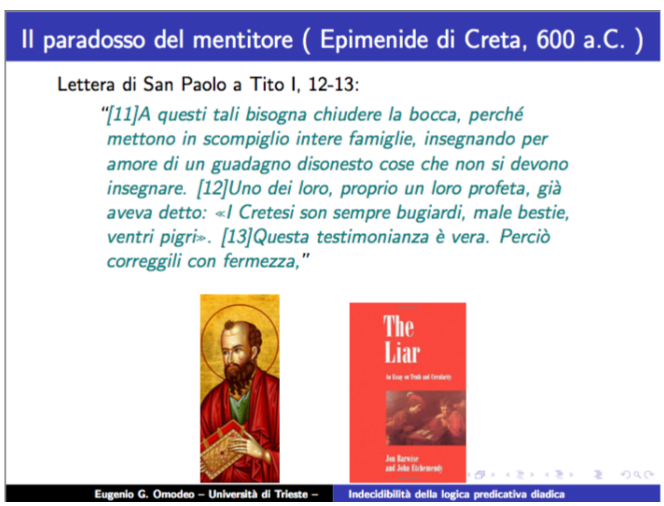

Figura 2: Diagonalizzazione (e autoreferenza): Antica fonte di sconcerto

3 Perché è importante la dimostrazione che gli insiemi diofantei e quelli enumerabili ricorsivamente sono gli stessi

Una volta stabilito che gli insiemi diofantei coincidono con quelli enumerabili ricorsivamente (questo è il senso dei due teoremi noti con gli acronimi DPR e DPRM), saremo in grado d'individuare un polinomio diofanteo parametrico $\mathbf{K}(a, x_1, \ldots, x_\ell)$ che rappresenta l'insieme indecidibile K visto alla fine del § 2. Dunque l'equazione $\mathbf{K}(\boldsymbol{a}, x_1, \ldots, x_\ell) = 0$ ha soluzione esattamente per quei numeri $\boldsymbol{a}$ che appartengono a K (vale a dire per quegli $\boldsymbol{a}$ tali che il calcolo di $\boldsymbol{f}_{\boldsymbol{a}}(\boldsymbol{a})$ dà risultato).

Un ipotetico risolutore del 10º problema di Hilbert potrebbe dunque essere sfruttato per decidere quali $\boldsymbol{a}$ appartengano a K e quali no, il che non è sostenibile.