

# Stabilire se una sequenza è casuale

Per assurdo, se esistesse un algoritmo

$$\text{RANDOM}(h) = \begin{cases} 1 & \text{se } h \text{ è casuale} \\ 0 & \text{altrimenti} \end{cases}$$

allora potremmo definire:

PARADOSSO()

```
1  for  $h$  = sequenza binaria, in ordine di lunghezza crescente
2      if  $|h| - \lceil \log_2 |h| \rceil > |P|$  and  $\text{RANDOM}(h) == 1$ 
3          return  $h$ 
```

dove  $|P| = |\text{PARADOSSO}| + |\text{RANDOM}|$  è una costante indipendente da  $h$  (perché nel testo compare solo come variabile) corrispondente alla lunghezza di un programma che genera  $h$ . La prima condizione è vera se e solo se  $h$  non è casuale, e PARADOSSO termina sicuramente perché esistono sequenze casuali di lunghezza arbitraria, restituendo una sequenza che è casuale e non casuale allo stesso tempo – assurdo.