RANDOM NUMBERS

informal : a number $n \in \mathbb{N}$ is random if for every program P which outputs n, the size of P is larger than n

show that

- there are infinitely many random numbers
- it is not decidable to establish if a number is random

Formally

- program size $|P_e| = e$
- $n \in \mathbb{N}$ is random if for all programs $e \in \mathbb{N}$ s.t. $\varphi_e(0) = n$ it holds $e > n$

(1) there are infinitely many random numbers

Each computable function is computed by infinitely many programs.
In particular, for all $k \in \mathbb{N}$ there are $e_1 < e_2 < \dots < e_k$ s.t.
$\forall i \quad \varphi_i = \emptyset$ (always undefined)

$$|\{ \varphi_e(0) \mid 0 \le e \le e_k \wedge \varphi_e(0) \}| \le e_k - k$$

hence there are at least k numbers in $[0, e_k]$ which cannot be produced in output by a program $e \le e_k$. Hence they are random!

since this holds for every k ...

there are infinitely many random numbers.

(2) $R = \{ n \mid n \text{ is random} \}$ is not recursive

Assume that R is recursive i.e.

$$\chi_R(n) = \begin{cases} 1 & \text{if } n \in R \\ 0 & \text{otherwise} \end{cases}$$

Define

$$\begin{aligned} g(n,x) &= \text{least random number} > n \\ &= \mu z.\ z \in R \text{ and } z > n \\ &= n+1 + \mu z.\ (n+1+z \in R) \\ &= n+1 + \mu z.\ |\chi_R(n+1+z) - 1| \end{aligned}$$

computable

By smn there is $s : \mathbb{N} \to \mathbb{N}$ total computable s.t.

$$\varphi_{s(n)}(x) = g(n,x) = \text{least random number} > n$$

By the 2nd recursion theorem there is $n_0 \in \mathbb{N}$ s.t. $\varphi_{n_0} = \varphi_{s(n_0)}$

$$\varphi_{n_0}(0) = \varphi_{s(n_0)}(0) = g(n_0, 0) \underset{= K}{=} (\text{least}) \text{ random number} > n_0$$

hence n_0 is a program which generates a random number K

s.t. $n_0 < K$; contradiction.

Hence R is not recursive.

Note $\bar{R}$ is r.e.

$$sc_{\bar{R}}(n) = \mathbb{1}\left(\mu t.\ \bigvee_{e=0}^{n} S(e,0,n,t)\right) \quad \text{computable}$$

$\left\{\begin{array}{l}\text{check if some} \\ \text{program } e \leq n \text{ outputs } n \text{ on } 0\end{array}\right.$

$\leadsto$ R is not r.e.