RANDOM NUMBERS (from 1st lesson)

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

show that

- there are infinitely many random numbers
- the property of being random is undecidable

Formal view :

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

(1) there are infinitely many random numbers

Recall that each computable functions is computed by infinitely many programs. Hence for each $k \in \mathbb{N}$ there is $e_1 < e_2 < \dots < e_k$ s.t. $\varphi_{e_i} = \emptyset \quad i = 1, \dots, k$

$$|\{ \varphi_i(0) \mid i \leq e_k \wedge \varphi_i(0)\downarrow \}| \leq e_k - k$$

hence there are at least k numbers $m \leq e_k$ which can't be generated by programs $e < m$

$\leadsto$ these numbers 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 R to be recursive i.e.

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

Define

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

computable

by smn there is $s : \mathbb{N} \to \mathbb{N}$ total computable

s.t.

$$g(n,x) = \varphi_{s(n)}(x)$$

$\|$

least random number $> n$

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

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

hence n_0 generates a random number $> n_0$, contradiction!

$\Rightarrow$ R not recursive.

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

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

check if some program $e < n$ outputs n on 0

$\rightsquigarrow$ R is not r.e.