9/4/25

Thursday, September 4, 2025 9:09 AM

PROPERTIES OF PRG

Q → what's the next data I move to

Based on current state & input it reads

Ram Model

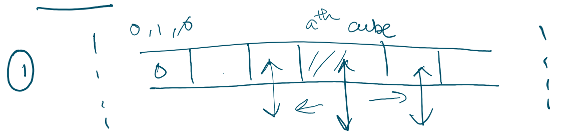
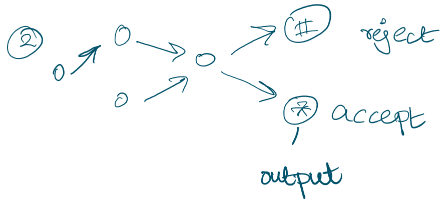


table is bounded

* can move anywhere from first to last



no input length needed

circuit → Boolean function $f(x_1, x_2, \cdots, x_n) \rightarrow \{0,1\}$

$\{0,1\}$

* length of input : n bit

$\oplus$ and gate

$\otimes$ or gate

How many gates to use to determine

Hamiltonian Cycle → 1 path that touches all points only once

Can reduce searching, optimization, and counting problem to decision problem to find a solution.

P/ NP solution is deterministic

BPP is randomness

NP hard ⇒ can't even verify the solution

defined respect to decision problems

Satisfying assignment → $f(x_1, x_2, x_3) = (x_1 \oplus x_2) \otimes x_3 = 0$

Polynomial reduction is very important to know in cryptography.

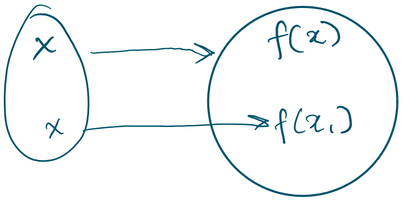
CONSTRUCTION OF PRG

m → length of output function

Anything you add to an input function, still be an input function

No fixed bits can be used for the hardcoding Bit function ($B(x)$)

Bijective



One way example → hardcore challenge

Computational class → Latest worst case handles

Find subset

$\{a_1, a_2, a_n\} \in Za \Rightarrow$ adversary

$\sum b_i a_i + \dots = 0 \bmod q$

$b_1, b, \dots, b_n$

$b_i \in \{0,1\} \Rightarrow$ solution