A formal model of interaction b/w two parties

- special turing m/c's, prover and verifier trying to ascertain language membership.

- prover
  - presents proof of what it wants the verifier to think
  - might not be trustworthy

- Verifier
  - verifies that the proof is correct.

- often useful in zero-knowledge proofs.
  - the prover wants to prove something to the verifier without revealing the entirety of its knowledge.

---

special TM (interactive TM)

- A TM with additional tapes
  - i/p tape (read only)
  - random tape (read only)
  - Work tape (read/write)
  - Incoming communication tape (read only)
  - Outgoing communication tape (write only)
  - output tape (write only)

classmate

Date / /

Interactive protocol

- ordered pair of ITM's (A, B)
- A and B share an input tape
- A's write only tape ⇒ B's read only (commn) (commn)
- operates in stages

  * One m/c operates in each stage; other is idle.
  * Within a stage
    → m/c does some internal computation
    → Then does one of the following
      - Terminates the protocol
      - Write a m/c on its commn. tape and goes idle
      - if the m/c is B, can accept or reject
  * B computes first in stage 1.

- A is computationally unbounded
- B must operate in polynomial time in the length of its i/p string.

Date / /

Interactive proof system

- Imagine an interactive protocol (P,V)
- It's an interactive proof-system for the language L if:

$\forall x \in L$, $Pr[V \text{ accepts}] > 2/3$

$\forall x \notin L$ $Pr[V \text{ accepts}] < 1/3$.

- Completeness
  - ↳ Accept strings in L with high probability.
- Soundness.
  - ↳ Accept strings not in L with low probability.

→ NP problems —

* All problems in NP have IPS
* Languages in NP are verifiable. in polynomial time using certificate
* Prof system (P,V):
  - stage 1: V requests a certificate
  - stage 2: P computes the answer to the problem in NP and provides it to V
  - stage : V performs the polynomial time verification

- No randomness in this case.
- IP = NP (if No randomness)

Interactive proof systems examples.

Date __/__/____

Graph 3-Coloring with Commitments

" Given a graph $G=(N,E)$, Does there exist a coloring with 3 colors such that no adjacent nodes are of the same color "

→ Let $m = |E|$

Proof System (P, V)

— P wants to convince V that there exist a valid 3-Coloring, which it knows exists, if there is one, without providing the coloring

— proceeds in multiple rounds

— Each rounds:

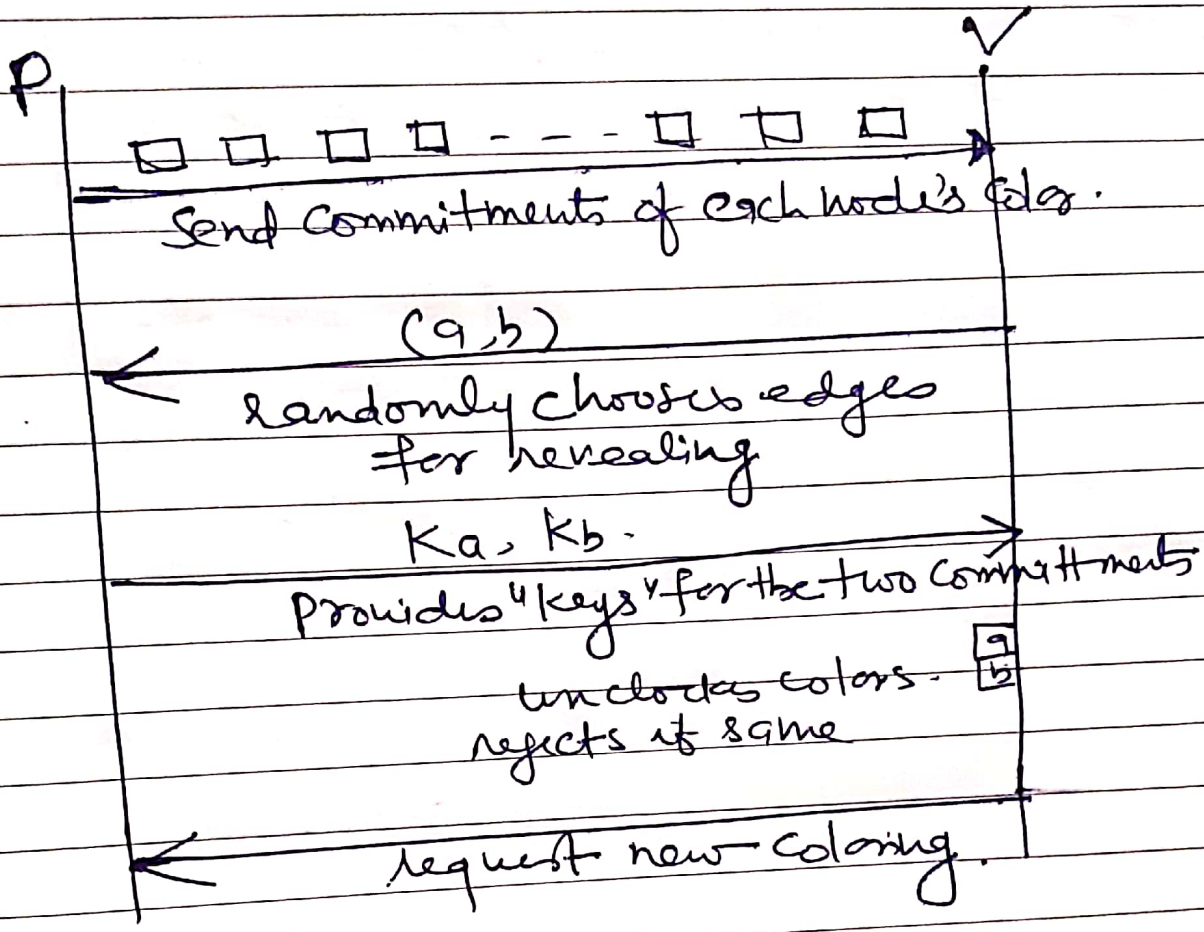
* P picks a random new coloring
* P commits to this coloring and sends securely as commitments to V

so that V cannot just decode the graph.

P can not change the Colorings once V recieves them.

* V randomly chooses an edge, and P reveals the nodes on each end
* V confirms that the nodes are of different colors, if the nodes are the same V enters a reject state.

— Repeat for m^2 rounds.
— If not rejected, accept



Completeness :-
* G is 3-Colorable, so V will never see adjacent nodes with matching colors.
* will never reject. Probability : 1

Soundness :-
* Worst case, only one edge will have invalid coloring
$\Rightarrow$ probability $= 1/m$.
* In any given round, $1 - \frac{1}{m}$ chance of being fooled.
* after m^2 rounds, $\left(1 - \frac{1}{m}\right)^{m \times m} \approx e^{-m}$.
* negligible as m grows — must be less than $1/3$