LECTURE - 15

ZERO KNOWLEDGE PROOFS

Graph 3-coloring

Prover $\{ct_i\}_{i\in[n]}$ Verifier

$pk, \{enc(i, col_i; r_i)\}_{i\in[n]}$

$\leftarrow j_1, j_2$

$(j_1, col_{j_1}; r_{j_1}) \rightarrow$

$(j_2, col_{j_2}; r_{j_2})$

UNSOUND PROTOCOL.

$(1, col_1) \oplus r_1 = ct_1$

$\vdots$

$(i, col_i) \oplus r_i = ct_i$

$ct_1, \ldots, ct_n \rightarrow$ Verifier

$\leftarrow j_1, j_2$

$\rightarrow$

COMMITMENTS

Set of PPT algorithms

* Commit $(1^\lambda, m; r) \rightarrow c$
* Verify $(1^\lambda, c, m, r) \rightarrow$ accept or reject.

that satisfy

* Correctness : $\forall\ m, r$
  Verify $(1^\lambda, c, m, r)$ = accept
  if c = Commit $(1^\lambda, m; r)$

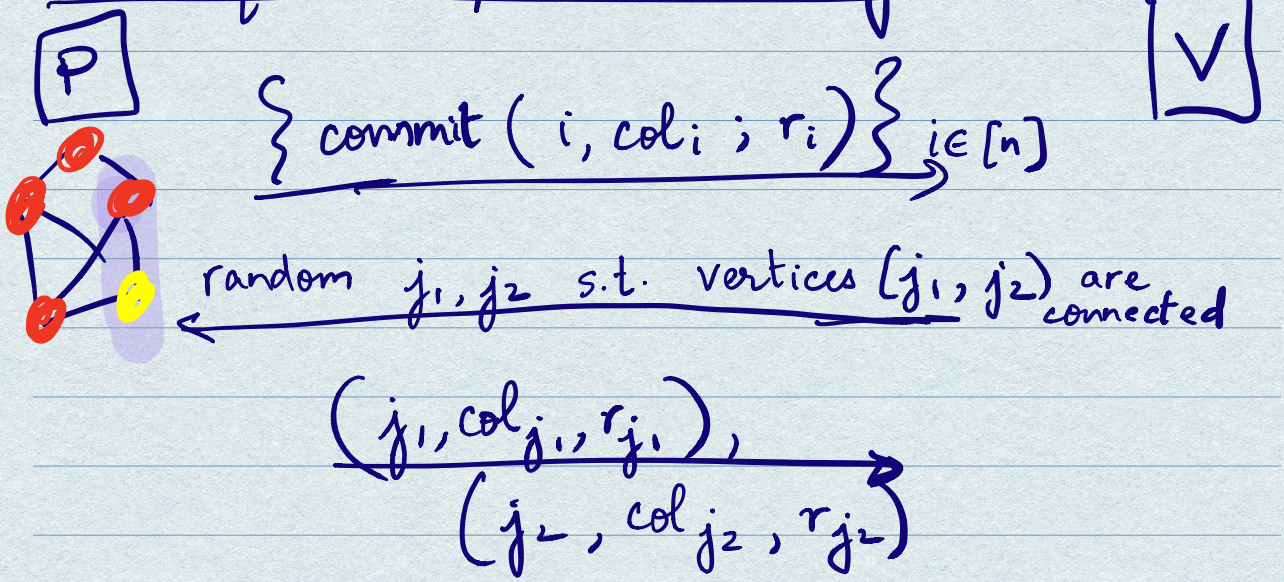
* Hiding (Computational) :

$\forall\ m_1, m_2$
Commit $(1^\lambda, m_1; r) \approx_c$ Commit $(1^\lambda, m_2; r)$

* Binding (Perfect) : $\forall\ c, m_0, r_0, m_1, r_1,$ $m_0 \neq m_1$

If Verify$(1^\lambda, c, m_0, r_0)$ = accept then Verify$(1^\lambda, c, m_1, r_1)$ = reject

ZK for Graph 3-coloring



accept if and only if:

1) Verify($\hat{I}$, $c_{j_1}, j_1, col_{j_1}, r_{j_1}$)
2) " j_2
3) $col_{j_1} \neq col_{j_2}$.

SOUNDNESS: (Def. 1)

$\forall P^*, \forall (x^* \notin L)$,

$$\Pr_{V\text{'s coins}}\left[\text{output}_V \langle P^*(x^*), V^*(x^*)\rangle = 1\right] = \text{negl}(\lambda)$$

(can be relaxed to computational soundness: where P^* is PPT)

Unfortunately, protocol on prev. slide doesn't satisfy Def 1.

$\exists$ P^* strategy s.t.

$$\Pr[V \text{ accepts} \mid x^* \notin L] \geq \frac{1}{\#\text{edges}}$$

Def 2. "Weak Soundness".

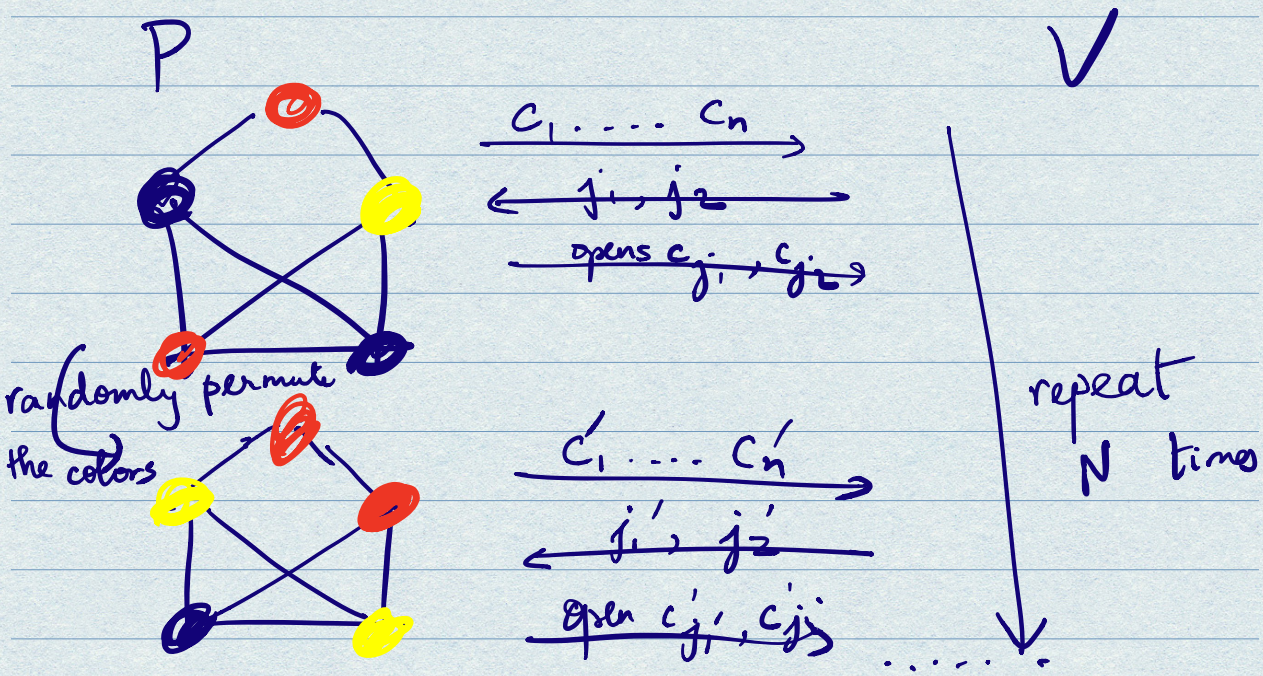
$\forall P^*$ $\forall$ $x^* \notin L$,

$$\Pr[\text{output}_V \langle P^*(x^*), V(x^*) \rangle = 1]$$

$$\leq 1 - \frac{1}{\#\text{edges}}$$

$$= 1 - \frac{1}{p(\lambda)}$$

Can we amplify soundness?



Repeat sequentially n times,

$\Pr[V \text{ accepts ALL repetitions}]$

$= \Pi \Pr[V \text{ accepts 1 repetion}]$

$= \left(1 - \frac{1}{\#\text{edges}}\right)^N$

$= \left(1 - \frac{1}{p(\lambda)}\right)^N$

$= \left(\left(1 - \frac{1}{p(\lambda)}\right)^{p(\lambda)}\right)^{\lambda} = e^{-\lambda}$.

for $N = \lambda \cdot p(\lambda)$,

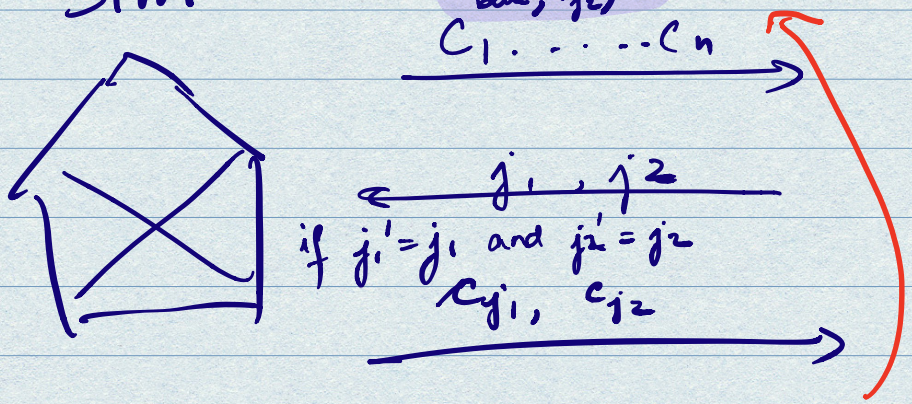
What about zero-knowledge?

Zero-Knowledge.

$\exists$ PPT Sim s.t. $\forall V^*, \forall x \in L$,

$$\text{View}_{V^*}\langle P(x), V^*(x)\rangle \approx_c \text{View}_{V^*}(\text{Sim}^{V^*}(x)).$$

Guess j_1', j_2'. Set $c_{j_1'} = \text{com}(1^\lambda, j_1', \text{red}; r_{j_1'})$, $c_{j_2'} = \text{com}(1^\lambda, j_2', \text{blue}; r_{j_2'})$



$$\Pr[(j_1', j_2') = (j_1, j_2)] = \frac{1}{\#\text{edges}} \pm \text{negl}(\lambda)$$

HONEST-VERIFIER ZK.

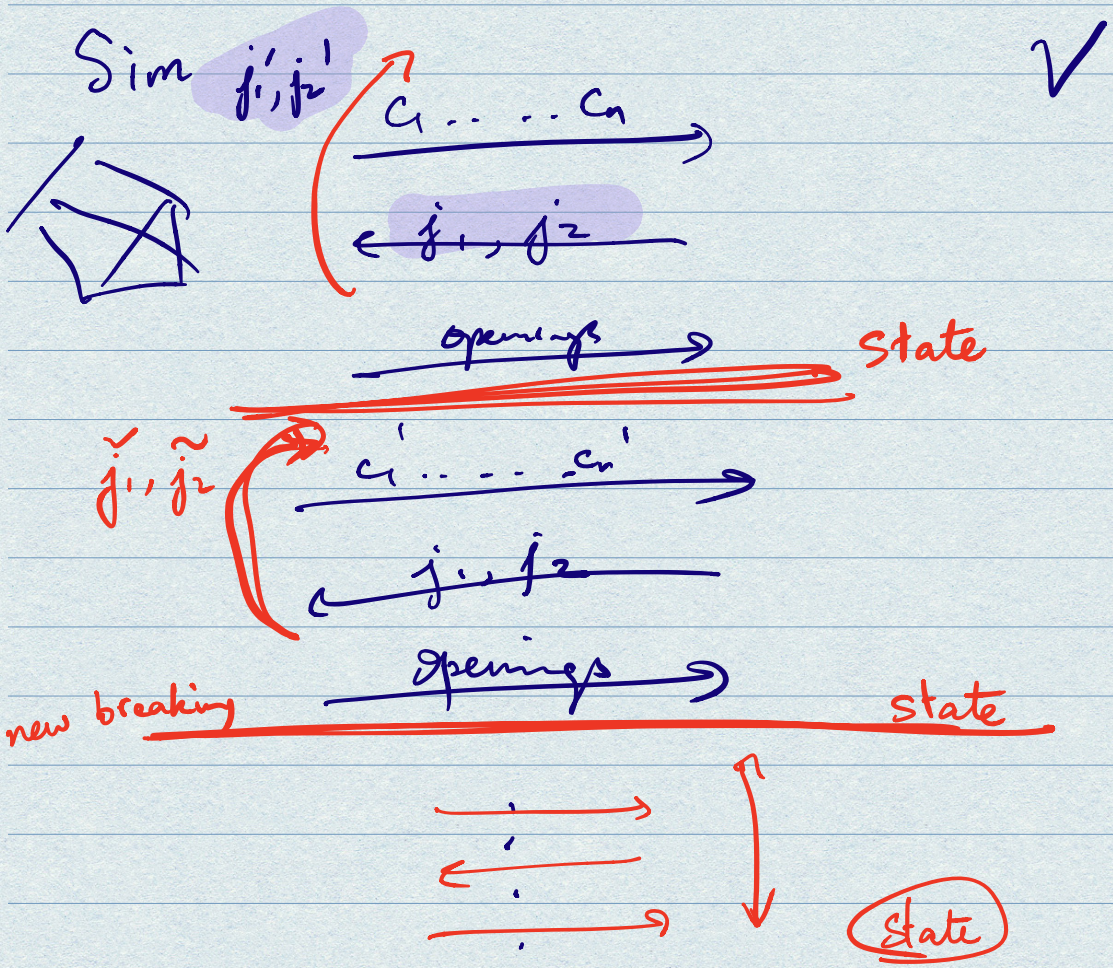
Simulator can look at V's random tape.

MALICIOUS-VERIFIER ZK

Verifier's next-message is unpredictable.

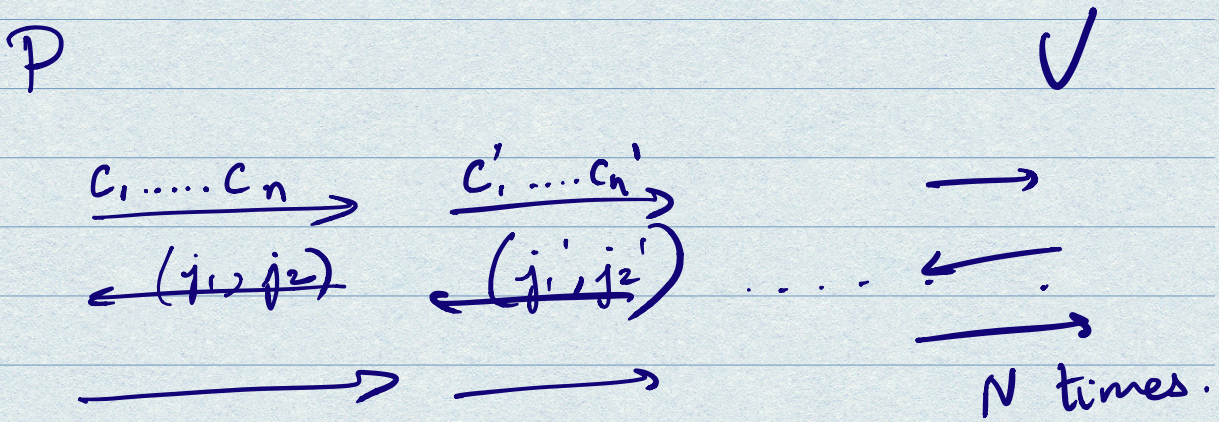
Claim: 3-message protocol satisfies ZK.

What about sequential repetition of the 3-message protocol?



Sim's running time = $(N \cdot \#\text{edges} \cdot \lambda)$

Parallel Repetition



Soundness. This satisfies Def 1.

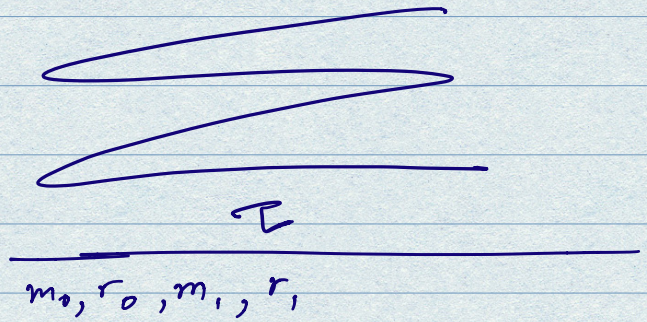
Suppose $x \notin L$.

In every parallel rep. r, $\exists\ (i_r, j_r)$ s.t. (i_r, j_r) are connected but have the same color.

$$\Pr[V \text{ accepts}] = \prod \Pr[V \text{ accepts 1 rep.}]$$
$$= \left(1 - \frac{1}{p(\lambda)}\right)^N.$$

[Post-class Discussions]

C R



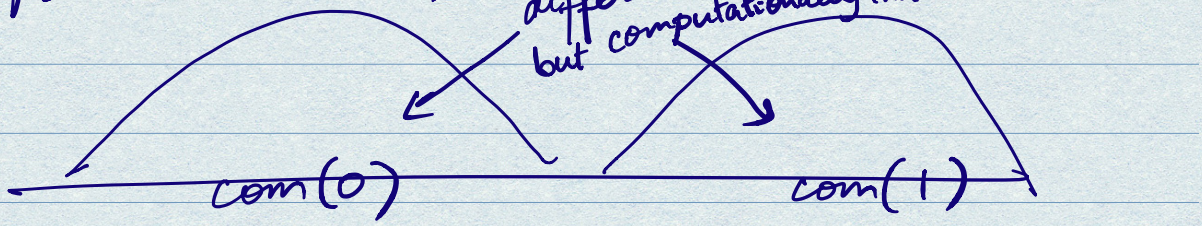
Statistical Binding.

$$\Pr_{\tau}\Big[\exists\, m_0, r_0, m_1, r_1 \;:\; \text{Verify}(\tau, m_0, r_0) = \text{acc} \;\wedge\; \text{Verify}(\tau, m_1, r_1) = \text{acc} \,\Big|\, \tau \leftarrow (C, R)\Big] = \text{negl}(\lambda)$$

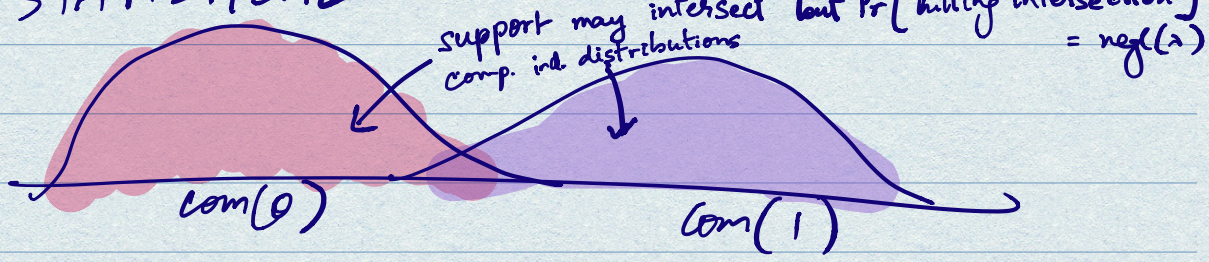
Computational Binding.

$$\Pr_{\tau}\Big[C(\tau) \to m_0, m_1, r_0, r_1 \;\wedge\; \text{Verify}(\tau, m_0, r_0) = \text{acc} \;\wedge\; \text{Verify}(\tau, m_1, r_1) = \text{acc} \,\Big|\, \tau \leftarrow (C, R)\Big]^{\text{poly}} = \text{negl}(\lambda)$$

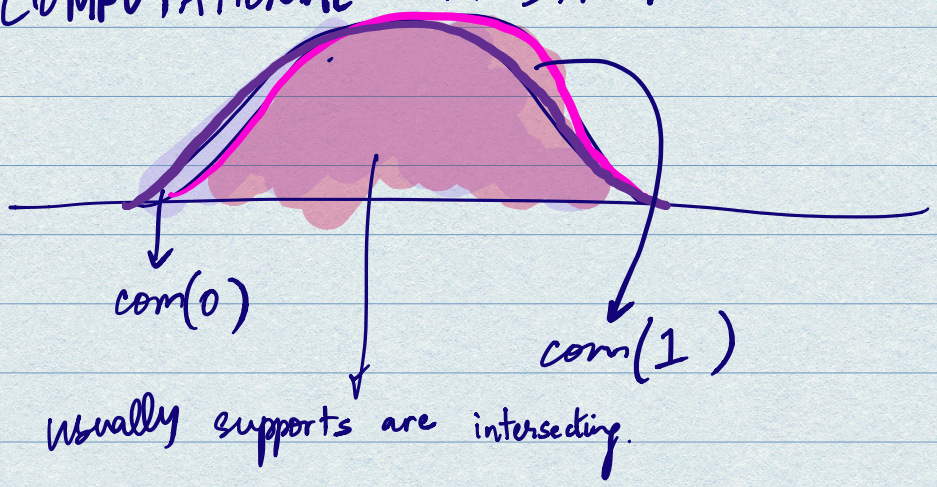
PERFECT BINDING



STATISTICAL BINDING



COMPUTATIONAL BINDING



usually supports are intersecting.