Interactive and zero-knowledge proofs

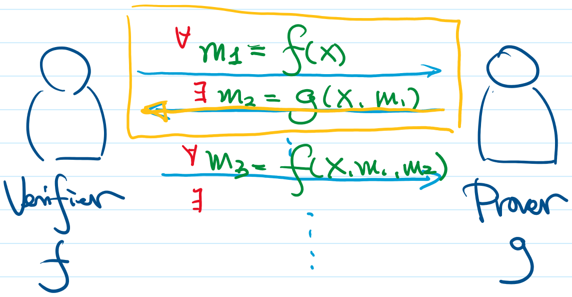
Wednesday, May 28, 2025 1:19 PM

Administrivia.

- Final Exam.
  - A few questions. covering everything up to NP-hardness reductions.
  - Practice final out tomorrow
- HW7.

¡ Probability !

Interactive Proofs



L has <u>k-round interactive proof</u>

If ∃ verifier V "poly-time" s.t. randomized BPP <u>private coin</u>

- $x \in L$: ∃prover P convinces V
all mighty
- $x \notin L$: ∀prover P, P fails to convince V

IP

~~dIP~~ := { L : L has poly-round randomized IP }

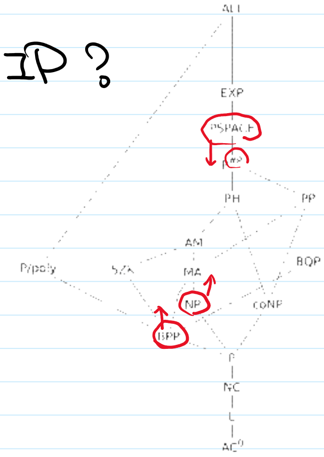
<u>Lemma.</u> dIP = NP

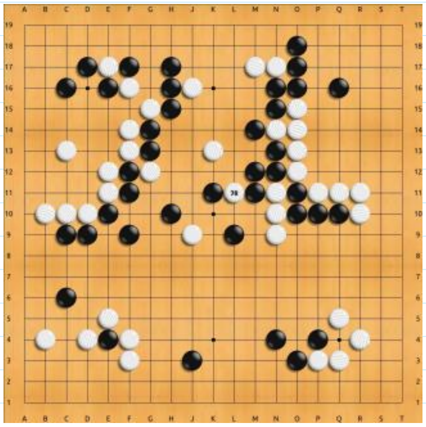
pf. sketch. Prover : generate whole message history for V. P interaction

Q. How strong is IP?

- NP ⊆ IP.
- BPP ⊆ IP.
- IP ⊆ PSPACE.

How to even prove coNP ⊆ IP?

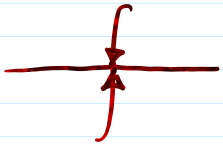




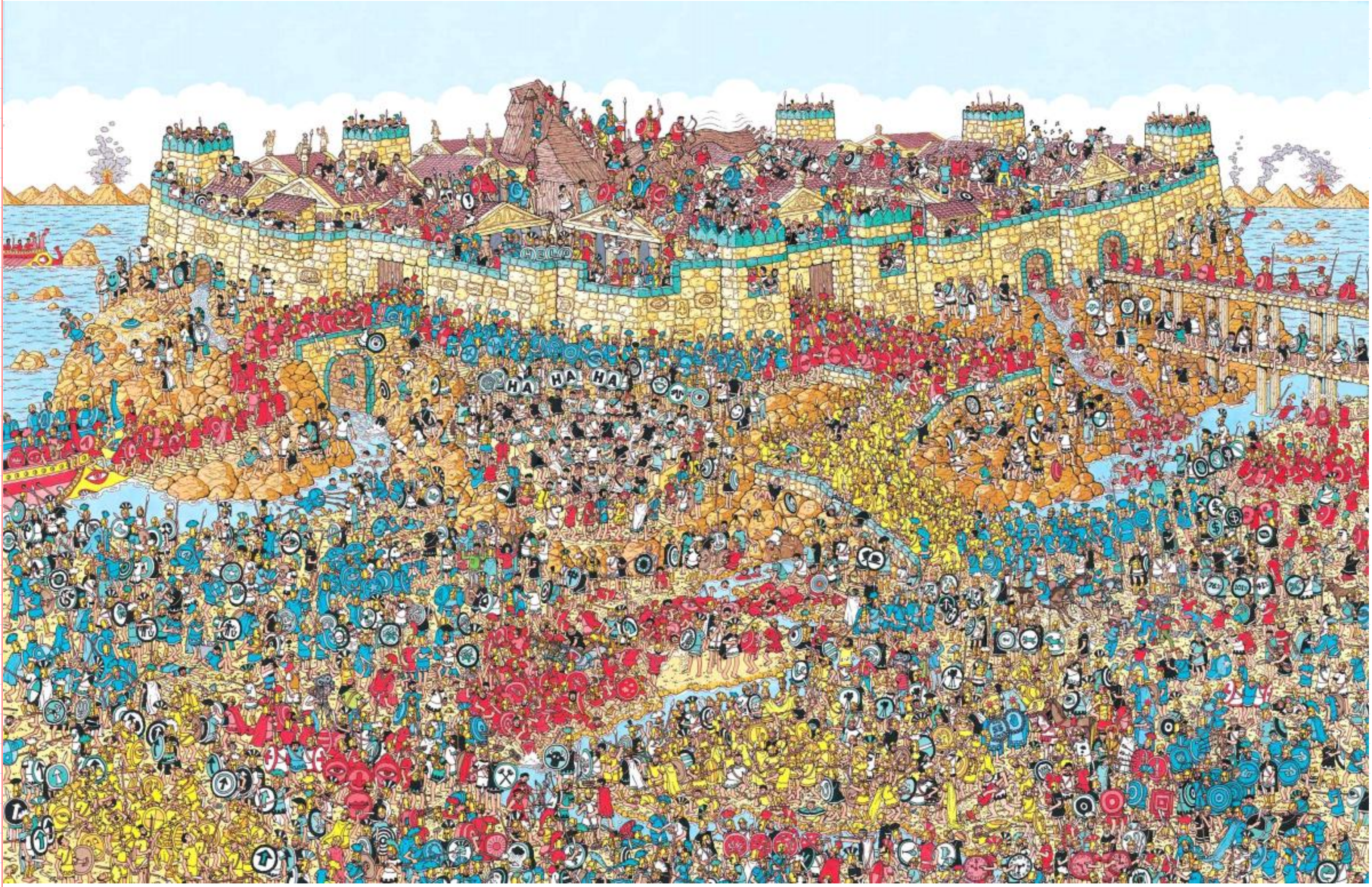
$\boxed{\text{How do we convince someone } \overset{\text{CNF}}{\phi} \text{ has no answer ?}}$

[LFKN, S'90].

Thm. IP = PSPACE (!)



Zero-knowledge Proofs.



An interactive proof (P, V) for L is zero-knowledge if

An interactive proof (P.V) for L is zero-knowledge if

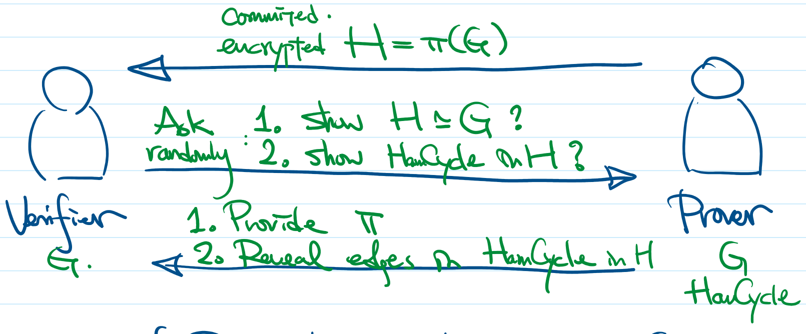
- [complete] honest V convinced w.h.p. by honest P.
- [sound] crooked $\tilde{P}$ fail to convince honest V.
- [zero-knowledge] no malicious $\tilde{V}$ learns anything beyond the statement is true.

Computationally indistinguishable : output of $\tilde{V}$ can be simulated in BPP.

Q. What problems have ZK proofs?

Thm HAMCYCLE has ZK proof.
[M. Blum'86]

Pf.



- [complete] If Prover knows Hamcycle in G, then also in H.
- [sound] If G has no Hamcycle, & $\tilde{P}$ wants to fake it, Depending on question asks by Verifier, need to generate H differently.

need to generate H differently.

- [ZK] Every round $\hat{V}$ learns either
  - $H \simeq G$. (but not Hamcycle in H)
  - H has HamCycle (but not π)

$\tilde{V}$ can very well does this by itself:

Pretend to be P

- Choose randomly coin toss : 1. choose π, $H = \pi(G)$ or 2. $H = K_n$.
- Commit H.
- Answer w/ π or Hamcycle

$\tilde{V}$ can't tell if it's P or $\tilde{V}$ pretending.

once $\tilde{V}$ hide first coin toss from itself.

Application. Secure computation.

- Public-key crypto [Diffie-Hellman'76, RSA'77]
- Secret sharing [Shamir-Blakley'79]
- Multi-party secure computation. [Yao'82]
- Fully homomorphic encryption scheme. [Gentry'09]
- Blockchains [Zcoin 2013]

Which world do we lived in? [Impagliazzo'95]

- Algorithmica: $P = NP$ and actually practical.
- Heuristica: $P \neq NP$ but efficient on avg/in practice
- Pessiland: NP problems hard on avg. no PRG.
- Cryptomania: $\exists$PRG. secure computation.

Q. Does undiscovered/under-utilized physic laws change which world we are in?

— Time travel.