Lecture 25:

Interactive Proofs + Zero Knowledge

- Graph non isomorphism
- "deft" of IP, zero-knowledge
- Graph Isomorphism

(most of this lecture is on slides)

Announcements

Course Evaluation time!

https://web.mit.edu/subject-evaluation/
def Random_permutation of graph G:

- pick random ordering of 1..n
  y_1, ..., y_n

- relabel vertices of G by new names
  node i in G \rightarrow node y_i in G'
  edge (i,j) in G \rightarrow edge (y_i,y_j) in G'
Interactively Proving $G_0 \not= G_1$:

Alice

Repeat $K$ times

Bob

Picks random bit $c \in \{0, 1\}$

permutation $f$

$Y_0 G_c$

$b = \text{guess for } c$

Checks if Alice guessed correctly

i.e. if $b = c$

Why is this good?

if $G_0 \not= G_1$:

$Y_0 G_c \equiv G_0 \text{ or } Y_0 G_c \equiv G_1 \text{ but not both}$

So Alice knows $c$

if $G_0 \equiv G_1$:

Alice can guess $c$ with prob $\leq \frac{1}{2}$

:. after $K$ times, Alice correct on each with prob $\leq \frac{1}{2^K}$
Interactive Proof of $G \equiv G'$

Alice:
- picks random permutation $G$
  \[ H \leftarrow G \circ G \]
- sends $H$ to Bob

Bob:
- picks $b \in \{1,2,3\}$ randomly
- sends $b$ to Alice

Alice:
if $b = 1$, sends $6$ to Bob
else ($b = 2$) sends $\rho \cdot G$ to Bob

Bob:
if $b = 1$
  checks $H = 6 \circ G$
if $b = 2$
  checks $H = \rho \cdot G'$
Interactively Proving Graph Isomorphism of \((G, G')\)

\[ G = \phi \circ G' \]

Present 1) \(\phi\) — ask for isomorphism from \(H\) to \(G\)

or 2) \(60\phi\) — ask for isomorphism from \(H\) to \(G'\)

- If \(G \cong G'\), then both are isomorphic to \(H\).
  
  i.e. \(H = 6 \circ G\)
  \[ = 6 \circ \phi \circ G' \]

- If \(G \not\cong G'\), then at most one isomorphic to \(H\).

A fails with prob \(1/2\)