Lecture 25: Interactive Proofs and Zero Knowledge
Complexity theory

Efficiently solvable: P
Efficiently verifiable: NP

Can randomness change what is (and how to) efficiently verify?

BPP (randomized P)
Central complexity theory questions:

• $P = NP$? (whatever can be efficiently verified is also efficiently solvable?)

• $P=BPP$? (is randomness necessary for efficient solvability?)
Today: Randomness affects how we can efficiently verify proofs!

- Interactive proofs
- Zero-knowledge Interactive proofs
Example: $n$ is a product of 2 primes

Alice: Prover

Bob: Verifier

If $p, q$ prime and $n = pq$ accept else reject
Example: G and G’ are isomorphic

G and G’ isomorphic (denoted $G \cong G'$) if there is a correspondence (bijection) $\varphi: V \rightarrow V'$ such that any edge $(u, v)$ in $G$ iff edge $(\varphi(u), \varphi(v))$ in $G'$.

e.g., $(1, 4)$ in $G$ and $(1', 4')$ in $G'$

$(1, 3)$ not in $G$ and $(1', 3')$ not in $G'$
Graph Isomorphism: How difficult is it?

- Not known to be in P
- In NP (proof = correspondence)
- Not known to be in Co-NP
  - How would you prove there is NO isomorphism?
- Not known to be NP-complete
  - But we don’t think it is...
Proving that $G$ and $G'$ are isomorphic

If correspondence good, ACCEPT, else REJECT

Correspondence $\varphi$
How do you prove that $G$ and $G'$ are not isomorphic?

Can’t try all $\varphi$!
Shortest classical proof is exponential in $n$
A quick detour...

• An important prehistorical note....
The Pepsi challenge: (1975)

• Can you tell the difference?
The Pepsi challenge: (1975)

• Can you tell the difference?
• A way to prove it:
  – We give you random samples of Coke and Pepsi
  – If you get it right $k$ times in a row, then we’ll believe you
• Why?
  – If you can tell the difference, you get it right every time
  – If you can’t tell the difference, you get it right with probability $\frac{1}{2}$ each time, so probability you get it right $k$ times in a row is $1/2^k$
  – i.e., if you get it right $k$ times, you either know or you are really lucky!
Proving that $G_0$ and $G_1$ are NOT isomorphic

• Bob (verifier):
  – Flips coin $c \in \{0,1\}$ picks random “shuffle” $\gamma$
  – Sends randomly shuffled version of $G_c$ i.e., $\gamma \circ G_c$ to Alice (prover)

• Alice (prover):
  (Note, if $G_0$ and $G_1$ are NOT isomorphic, then $H$ is isomorphic to only one... so Alice can figure out which one was sent)
  – If $H$ isomorphic to $G_0$ then output $b=0$
    Else output $b=1$

• Bob (verifier):
  – If Prover gets it right each time “ACCEPT” else “REJECT”
Interactive Proofs

• As in NP
  – The verifier is polynomial time
  – the prover is “all powerful”

• Two new ingredients:
  – Randomness: verifier tosses coins, can err with small probability
  – Interaction: rather than “reading” proof, verifier interacts with prover
Interactive Proofs
[Goldwasser Micali Rackoff 1985]

• Prover:
  – Knows the proof
  – No run time bounds

• Verifier:
  – Doesn’t know anything
  – Probabilistic: can toss coins
  – Polynomial time algorithm
  – Accepts or rejects the proposition
Interactive Proofs

(P,V) is *interactive proof system* for set of theorems L if

1. Completeness:
   - If proposition x is true (i.e., $x \in L$), prover can behave in a way that convinces verifier to always accept
   - i.e. Probability of acceptance = 1

2. Soundness:
   - If proposition is false (i.e., $x \notin L$), then, no matter what the prover does, verifier rejects with high probability
   - i.e., probability of accept is $\leq \frac{1}{2}$
     - If repeat k times, probability of accept $\leq \frac{1}{2^k}$
Efficient interactive proofs are MORE POWERFUL than efficient classical proofs!
The complexity class IP

- Decision problems L such that L has an interactive proof system
IP=PSPACE

• After Graph non-isomorphism, Non-SAT, 
  number of satisfying assignments,...

• Thm: IP=PSPACE
Complexity theory

Efficiently solvable: P, BPP (randomized P)
Efficiently verifiable: NP, IP = PSPACE

Can randomness change what is (and how to) efficiently verify? WE THINK SO!
Remarks

• If verifier doesn’t toss coins, then IP=NP
• If prover runs in poly time, then IP=probabilistic poly time
Interactive Proofs

- A third new ingredient
  - Zero Knowledge: verifier doesn’t learn anything except for the statement of the theorem

I will not tell you why G and H are not isomorphic, but I will CONVINCE you that they are not!
Zero Knowledge of Graph non-isomorphism

• Could Bob convince anyone else that the graphs are non-isomorphic?
  – The next verifier would probably pick different random shuffles...
Zero Knowledge Interactive Proofs

• After interaction, V “knows”
  – Statement of theorem is true
  – History of interaction

• Zero-knowledge: V didn’t learn anything except for truth of statement
  – i.e., given truth of statement, V could generate interactions on his own with same distribution
  – A fascinating definition... take more crypto courses!
Back to previous example: G and G’ are isomorphic

Correspondence $\varphi$

If correspondence good, Accept, else reject

Verifier learns $G \cong G'$ and correspondence
Interactive Proofs

- **Zero Knowledge**: verifier doesn’t **learn** anything except for the statement of the theorem

  I will not give you the correspondence, but I will prove that I could have if I had wanted to!
Idea for proving $G \cong G'$:

- **Alice:** (knows a correspondence $\phi$ s.t. $G = \phi \circ G'$)
  - Produces a random graph $H$ (by randomly permuting $G$ according to $\sigma$) which is isomorphic to both!
    1. This means she can give correspondence from $G$ to $H$ (i.e. $H = \sigma \circ G$)
    2. And a correspondence from $G'$ to $H$ (i.e. $H = \sigma \circ \phi \circ G'$)

- **Bob:**
  - randomly decides if Alice should demonstrate 1 or 2
    - Since he only sees one of them, he doesn’t actually see the correspondence between $G$ and $G'$
Back to proving $G = \varphi \circ G'$

- Random permute nodes of $G$ to get $H = \sigma \circ G$ ($= \sigma \circ \varphi \circ G'$)
- Send $H$ to Bob

- Toss coin $b$ and send to Alice
  - If $b=0$, send $\sigma$ (map from $G$ to $H$)
  - If $b=1$, send $\sigma \circ \varphi$ (map from $G'$ to $H$)

- Check $\sigma$ or ($\sigma \circ \varphi$)
Why does this work?

- **If** $G \cong G'$
  - Alice knows $\varphi$ demonstrating $G \cong G'$
  - Since Alice chose $\sigma$, it is no problem to compute $H=\sigma \circ \varphi \circ G'$ and to output $\sigma$ or $\sigma \circ \varphi$

- **If** $G \not\cong G'$
  - $H \cong G$ or $H \cong G'$ (or neither, but not both)
  - With probability $\frac{1}{2}$ Alice cannot demonstrate an isomorphism
Why zero knowledge?

• Bob can’t figure out \( \varphi \) from \( \sigma \) or \( \sigma \circ \varphi \)

• But could figure out \( \varphi \) from \( \sigma \) and \( \sigma \circ \varphi \)
  – So can’t repeat \( k \) times?
  – Must pick new \( \sigma \) each time!
Note: For proving graph isomorphism

- Verifier poly time
- Prover all powerful?
  - Here, Prover only needs to know the correspondence!!!
Which theorems have interactive zero knowledge proofs?

• If one-way functions exist then there exists a zero knowledge interactive proof for any IP problem
Why interactive proofs, why zero-knowledge?????

• A philosophical reason:
  – Can efficiently prove statements that are not efficiently provable with classical proofs

• A practical reason:
  – Passwords and identification
    • prove that “I am Ronitt Rubinfeld” so that no eavesdropper can mimic me later
  – Secure protocols
    • prove that I am behaving honestly
True zero-knowledge:

• Quote from a colleague in 1988:
  “I explained it [zero-knowledge] to my kids, and they understood!
  – they know that they didn’t learn anything”
6.046: some final words

• Let’s hope it wasn’t zero-knowledge!
  – nor zero-fun!

• Take more theory classes!
  – Lots of good choices – complexity, crypto, all kinds of algorithms...

• GOOD LUCK ON THE EXAM!