Complexity Theory

Jan Křetínský

Chair for Foundations of Software Reliability
and Theoretical Computer Science
Technical University of Munich

Summer 2016

Based on slides by Jörg Kreiker

Lecture 14

Interactive Proofs

Overview

NP certificates or proof of membership

Overview

NP certificates or proof of membership

$\downarrow$

RP proofs chosen at random

Overview

NP certificates or proof of membership

↓

RP proofs chosen at random

↓

IP interactive proofs
between a prover and a verifier

Example: job interview, interactive vs. fixed questions

Agenda

- interactive proof examples
  - socks
  - graph coloring
  - graph non-isomorphism
- definition of interactive proof complexity
  - **IP**
  - public coins: **AM**

Different socks

Example

P wants to convince V that she has a red sock and a yellow sock.
V is blind and has a coin.

Interactive Proof

1. P tells V which sock is red
2. V holds red sock in her right hand, left sock in her yellow hand
3. P turns away from V
4. V tosses a coin
   4.1 heads: keep socks
   4.2 tails: switch socks
5. V asks P where the red sock is

Observations

- If P tells the truth (different colors), she will always answer correctly
- If P lies

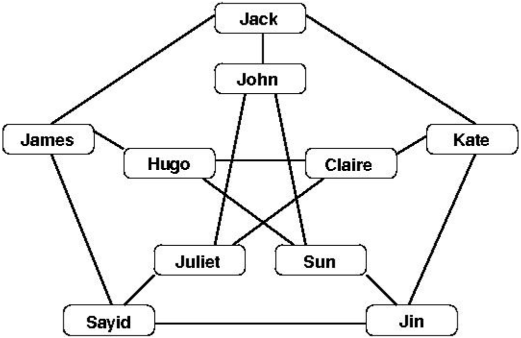
Observations

- If P tells the truth (different colors), she will always answer correctly
- If P lies
  - she can only answer correctly with probability 1/2
  - after k rounds, she gets caught lying with probability $1 - 2^{-k}$

Observations

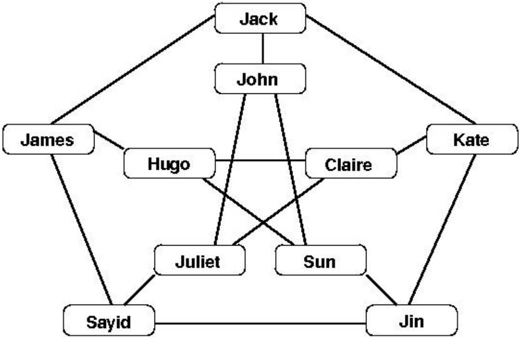
- If P tells the truth (different colors), she will always answer correctly
- If P lies
  - she can only answer correctly with probability 1/2
  - after k rounds, she gets caught lying with probability $1 - 2^{-k}$
- random choices are crucial
- P has more computational power (vision) than V
- P must not see V's coin (private coin)

Graph 3-Coloring



- P claims: G is 3-colorable
- How can she prove it to V?

Graph 3-Coloring



- P claims: G is 3-colorable
- How can she prove it to V?
- provide certificate (since $3-\mathrm{Col} \in$ **NP**), V checks it
- possible for all $L \in$ **NP** with one round if P has **NP** power

What if actual coloring should be secret?

- given a graph (V, E) with $|V| = n$
- P claims 3-colorability
- P wants to convince V of coloring $c : V \to C \quad (= \{R, G, B\})$

What if actual coloring should be secret?

- given a graph (V, E) with $|V| = n$
- P claims 3-colorability
- P wants to convince V of coloring $c : V \to C \quad (= \{R, G, B\})$

1. P randomly picks a permutation $\pi : C \to C$ and puts $\pi(c(v_i))$ in envelope i for each $1 \leq i \leq n$
2. V randomly picks edge (u_i, u_j) and opens envelopes i and j to find colors c_i and c_j
3. V accepts iff $c_i \neq c_j$

Observations

- the protocol has two rounds
- a round is an uninterrupted sequence of messages from one party

Observations

- the protocol has two rounds
- a round is an uninterrupted sequence of messages from one party
- if G is not 3-colorable, P will be caught lying after $\mathcal{O}(n^3)$ rounds with probability $1 - 2^{-n}$

Observations

- the protocol has two rounds
- a round is an uninterrupted sequence of messages from one party
- if G is not 3-colorable, P will be caught lying after $\mathcal{O}(n^3)$ rounds with probability $1 - 2^{-n}$
- V learns nothing about the actual coloring

$\Rightarrow$ zero-knowledge protocol

- by reductions, all **NP** languages have ZK protocols

Observations

- the protocol has two rounds
- a round is an uninterrupted sequence of messages from one party
- if G is not 3-colorable, P will be caught lying after $\mathcal{O}(n^3)$ rounds with probability $1 - 2^{-n}$
- V learns nothing about the actual coloring

$\Rightarrow$ zero-knowledge protocol

- by reductions, all **NP** languages have ZK protocols
- private coins

Graph Non-Isomorphism

- **NP** languages have succinct, deterministic proofs
- **coNP** languages possibly don't
- graph isomorphism, GI, is in **NP**
- hence GNI $= \{\langle G_1, G_2 \rangle \mid G_1 \not\cong G_2\}$ is in **coNP**
- GNI has a succinct interactive proof

Interactive Proof for GNI

given: graphs G_1, G_2

- **V** pick $i \in_R \{1, 2\}$, random permutation π
- **V** use π to permute nodes of G_i to obtain graph H
- **V** send H to V
- **P** check which of G_1, G_2 was used to obtain H
- **P** let G_j be that graph and send j to V
- **V** accept iff $i = j$

Intuition

- same idea as for socks protocol
- P has unlimited computational power
- if $G_1 \cong G_2$ then P answers correctly with probability at most $1/2$
- probability can be improved by sequential or parallel repetition
- if $G_1 \ncong G_2$ then P answers correctly with probability 1
- privacy of coins crucial

Agenda

- interactive proof examples ✓
  - socks ✓
  - graph coloring ✓
  - graph non-isomorphism ✓
- definition of interactive proof complexity
  - **IP**
  - public coins: **AM**

Interaction

Definition (Interaction)

Let $f, g : \{0,1\}^* \to \{0,1\}^*$ be functions and $k \geq 0$ an integer that may depend on the input size. A k-round interaction of f and g on input $x \in \{0,1\}^*$ is the sequence $\langle f, g\rangle(x)$ of strings $a_1, \ldots, a_k \in \{0,1\}^*$ defined by

$$\begin{aligned} a_1 &= f(x) \\ a_2 &= g(x, a_1) \\ &\cdots \\ a_{2i+1} &= f(x, a_1, \ldots, a_{2i}) && \text{for } 2i < k \\ a_{2i+2} &= g(x, a_1, \ldots, a_{2i+1}) && \text{for } 2i+1 < k \end{aligned}$$

The output of f at the end of the interaction is defined by $out_f\langle f, g\rangle(x) = f(x, a_1, \ldots, a_k)$ and assumed to be in $\{0,1\}$.

This is a deterministic interaction, we need to add randomness.

Adding Randomness

Definition (IP)

For an integer $k \geq 1$ that may depend on the input size, a language L is in **IP**$[k]$, if there is a probabilistic polynomial-time TM V that can have a k-round interaction with a function $P : \{0,1\}^* \rightarrow \{0,1\}^*$ such that

- Completeness
  $x \in L \implies \exists P.Pr[out_V\langle V, P\rangle(x) = 1] \geq 2/3$
- Soundness
  $x \notin L \implies \forall P.Pr[out_V\langle V, P\rangle(x) = 1] \leq 1/3$

We define **IP** $= \bigcup_{c \geq 1}$ **IP**$[n^c]$.

- V has access to a random variable $r \in_R \{0,1\}^m$
- e.g. $a_1 = f(x, r)$ and $a_3 = f(x, a_1, r)$
- g cannot see r

$\Rightarrow$ $out_V\langle V, P\rangle(x)$ is a random variable where all probabilities are

Arthur-Merlin Protocols

Definition (AM)

- For every k the complexity class **AM**$[k]$ is defined as the subset of **IP**$[k]$ obtained when the verfier's messages are random bits only and also the only random bits used by V.
- **AM** $=$ **AM**$[2]$

Such an interactive proof is called an Arthur-Merlin proof or a public coin proof.

Agenda

- interactive proof examples ✓
  - socks ✓
  - graph coloring ✓
  - graph non-isomorphism ✓
- definition of interactive proof complexity
  - **IP** ✓
  - public coins: **AM** ✓

Basic Properties

- **NP** $\subseteq$ **IP**
- for every polynomial $p(n)$ the acceptance bounds in the definition of **IP** can be changes to
  - $2^{-p(n)}$ for soundness
  - $1 - 2^{-p(n)}$ for completeness
- the requirement for completeness can be changed to require probability 1 yielding perfect completeness
- perfect soundness collapses **IP** to **NP**

What have we learnt?

- **IP**$[k]$: languages that have k-round interactive proofs
- interaction and randomization possibly add power
  - randomization alone: **BPP** (possibly equals **P**)
  - deterministic interaction: **NP**

  ⇒ interactive proofs more succinct
- prover has unlimited computational power
- verifier is a **BPP** machine (poly-time with coins)
- coins can be private or public
- zero-knowledge protocols do exist for all **NP** languages
- soundness and completeness thresholds can be adapted

What's next?

- **AM**$[2] =$ **AM**$[k]$ AM hierarchy collapses
- **AM**$[k+2] =$ **IP**$[k]$ private coins don't help
- if graph isomorphism is **NP**-complete, the polynomial hierarchy collapses
- **IP** $=$ **PSPACE**