Interactive Protocols

Randomization + Nondeterminism = ?

Definition: Interactive Proof System

- Question: x in L for some language L
- <A,B>, both TMs, for Alice & Bob, both read x
- A is an all-powerful prover
- B runs in random polynomial time wrt. |x|
- B sends queries b_i to A
- A answers with messages a_i
- x in L -> B accepts with prob. > 2/3
- x not in L -> B accepts with prob. < 1/3 for all A'
- Then <A,B> is an IP-system for L, L in IP

Example: Graph Nonisomorphism

- Given L <G^0, G^1>, are they non-isomorphic?
- Graph Isomorphism is in NP (probably not complete)
- Proof Idea: permute G' to get G', ask A whether G' nonisomorphic to G'

Interactive Protocols

- Interactive Protocols and the class IP
- Example: Graph Nonisomorphism
- Example: 3Coloring (Zero Knowledge)
- Arthur Merlin Protocols
- Relationships to other Classes
- IP is in PSPACE
- PSPACE = IP (Shamir’s Theorem)

Definition: Interactive Proof System

Example: 3COL

- Given G is there a 3-coloring?
- Bob can ask Alice for a coloring…
- But: Alice can convince Bob, that there is a coloring without revealing the coloring. "I prove X, but I don't give you the proof." – Zero Knowledge
- Idea: Permute coloring and send "envelopes"
A similar class: Arthur-Merlin Protocols

- Same as IP – but random bits are known to Alice.

Random $\rightarrow$ Input $x$ $\rightarrow$ Alice

\[ b_1, a_1, b_2, a_2, b_3, a_3, \ldots \]

Note: random is private to Bob

Poly number of messages

Poly length of messages

Time unbounded (PSPACE is enough)

A similar class: Arthur-Merlin Protocols

- Same as IP – but random bits are known to Alice.

Random $\rightarrow$ Input $x$ $\rightarrow$ Arthur

\[ b_1, a_1, b_2, a_2, b_3, a_3, \ldots \]

Merlin

Class AM

AM contained in IP

Relationships to other Classes

Random $\rightarrow$ Input $x$ $\rightarrow$ Bob

\[ b_1, a_1, b_2, a_2, b_3, a_3, \ldots \]

Alice

Relationships to other Classes

Random $\rightarrow$ Input $x$ $\rightarrow$ Bob

\[ b_1, a_1, b_2, a_2, b_3, a_3, \ldots \]

Alice

Relationships to other Classes

Random $\rightarrow$ Input $x$ $\rightarrow$ Bob

\[ b_1, a_1, b_2, a_2, b_3, a_3, \ldots \]

Alice

Relationships to other Classes

Random $\rightarrow$ Input $x$ $\rightarrow$ Bob

\[ b_1, a_1, b_2, a_2, b_3, a_3, \ldots \]

Alice

- NP contained in IP
- BPP contained in IP

Relationships to other Classes

Random $\rightarrow$ Input $x$ $\rightarrow$ Bob

\[ b_1, a_1, b_2, a_2, b_3, a_3, \ldots \]

Alice

- NP contained in IP
- BPP contained in IP
- Graph-Nonisomorphism in IP
- And, IP is contained in ?
**Shamir’s Theorem**

- shows $\text{QSAT}$ in $\text{AM}$
- Remember the definition of $\text{QSAT}$
- $\text{QSAT}$ is $\text{PSPACE}$ complete
- Principle Idea:
  - Translate $\text{QSAT}$ instance $\varphi$ into an arithmetical expression $A_\varphi$ with $\varphi \in \text{QSAT} \iff A_\varphi \neq 0$

---

**IP in PSPACE**

1. $\text{count} := 0$;
2. for each string $r$ with $|r| = p(|x|)$
3. $\text{acc} := \text{false}$;
4. for each string $a$ with $|a| = p(|x|)$
5. $\text{acc} := \text{acc} \land \text{Bob}(r,a)$;
6. endfor;
7. if $\text{acc}$ then $\text{count} := \text{count} + 1$;
8. endfor;
9. return $\text{count} > 2^{n^{n+1}/3}$;

---

**IP in PSPACE**

- Fix Random and $a_1, a_2, a_3, \ldots$
- Then simulating Bob is in PTIME
- Note: both, Random and $a_1, a_2, a_3, \ldots$ are of poly-length

---

**Relationships so far**

- $\text{AM} \subseteq \text{IP} \subseteq \text{PSPACE}$$\subseteq \text{AM}$
- $\text{NP} \subseteq \text{IP}$
- $\text{BPP} \subseteq \text{IP}$
- Drop Randomness
- Drop Alice

---

**IP in PSPACE**

Check for each $r$ whether Bob accepts.
Accept, if Bob accepts in $2/3$ of all cases.

---

**IP in PSPACE**

Check whether Bob accepts