COMP4141 Theory of Computation

Interactive Proof Systems

Ron van der Meyden

CSE, UNSW

Revision: 2014/05/20

(Credits: K Engelhardt, M Sipser, C Papadimitriou)

BPP can be understood as a probabilistic version of **P**.

What about a probabilistic version of **NP**?

Recall the guess and verify formulation of **NP**:

> *$A \in$ **NP** if there exists a polynomial p and a **P** computable function $f : \Sigma^* \times \Sigma^* \to \{0, 1\}$ such that $x \in A$ iff there exists $y \in \Sigma^*$ with $|y| \leq p(|x|)$ such that $f(x, y) = 1$.*

Here y is a polynomial size certificate for $x \in A$ that can be verified in **P**.

$\overline{\text{ISO}}$

Definition

Call two graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ *isomorphic* (and write $G_1 \simeq G_2$) if there exists a bijection $\pi : V_1 \longrightarrow V_2$ such that $E_2 = \{\ (\pi(u), \pi(v)) \mid (u, v) \in E_1\ \}$.

Theorem

$ISO = \{\ \langle G_1, G_2 \rangle \mid G_1 \simeq G_2\ \} \in \mathbf{NP}$

Proof.

The bijection could be the certificate. $\square$

The status of $\overline{ISO}$ is unclear as of yet.

Consider the following protocol between a perhaps unreliable but computationally unbounded *prover* P and a probabilistic **P** *verifier* V who both have $\langle G_1, G_2 \rangle$ as input.

1. N times:
    1. V flips a fair coin $c \in \{1, 2\}$, reorders G_c randomly, and sends the result X to P
    2. P replies by declaring the coin (1 or 2)
2. V *accepts* if P masters all N challenges; otherwise it *rejects*.

The probability for V to accept even though $G_1 \simeq G_2$ is 2^{-N} because even the smartest P can only guess as long as the coin flips are indeed secret.

Formally, a verifier is a deterministic TM that takes 3 inputs:

1. an input string w (as usual),
2. a random string r (to make up for being deterministic),
3. a partial message history h of the form $m_1 \# m_2 \# \dots m_i$ (to recall the conversation with P so far)

to compute a function $V : \Sigma^* \times \Sigma^* \times \Sigma^* \longrightarrow \Sigma^* \cup \{accept, reject\}$.

The prover takes input w and partial messages history h to compute $P : \Sigma^* \times \Sigma^* \longrightarrow \Sigma^*$.

For simplicity, assume that messages and random strings are bound by $p(|w|)$ for some polynomial p depending only on V.

Write $(V \leftrightarrow P)(w, r) = \mathit{accept}$ if there exists a $h = m_1 \# \ldots m_{2k+1}$ whereby

1. $V(w, r, m_1 \# \ldots m_{2i}) = m_{2i+1}$ for $0 \leq i \leq k$;
2. $P(w, m_1 \# \ldots m_{2i-1}) = m_{2i}$ for $0 < i \leq k$; and
3. $m_{2k+1} = \mathit{accept}$.

$$\Pr[V \leftrightarrow P \text{ accepts } w] = \Pr[(V \leftrightarrow P)(w, r) = \mathit{accept}]$$

where r is a randomly selected string of length $p(|w|)$.

Definition

$A \in \mathbf{IP}$ if a prover P and a $\mathbf{P}$ computable verifier V exist such that for every $\tilde{P}$ and w

1. $w \in A$ implies $\Pr[V \leftrightarrow P \text{ accepts } w] \geq \frac{2}{3}$, and
2. $w \notin A$ implies $\Pr[V \leftrightarrow \tilde{P} \text{ accepts } w] \leq \frac{1}{3}$.

Theorem

$\mathbf{IP} = \mathbf{PSPACE}$

Random Oracles

Consider randomly chosen oracles. It has been shown that if oracle A is chosen randomly, then with probability 1, $\mathbf{P}^A \neq \mathbf{NP}^A$.

When a question is true for almost all oracles, it is said to be *true for a random oracle*. This is sometimes taken as evidence that $\mathbf{P} \neq \mathbf{NP}$.

Unfortunately, a statement may be true for a random oracle and false for ordinary TMs at the same time; for example for almost all oracles A, $\mathbf{IP}^A \neq \mathbf{PSPACE}^A$, while $\mathbf{IP} = \mathbf{PSPACE}$.