18.405J/6.841J Advanced Complexity Theory April 6, 2000

Lecture 17

Lecturer: Dan Spielman *Scribe: Jordan Weitz*

1 Motivation

Say you wanted to convince your colorblind friend, Jim, that two balls, one red and one blue but otherwise indistinguishable, are different. He cannot for himself tell them apart. Let him hold the balls so that you may see them and say "The ball in your right hand is red." Now, if you are right in that you can distinguish between the balls, you should have no problem telling which ball is which if Jim put them behind his back and juggled them up. If, on the other hand, you were colorblind like Jim, you have only a 50% chance of guessing correctly. Hence, by repeating the experiment of exchanging (or not exchanging) the balls behind his back and showing them to you, Jim can be convinced to any degree of certainty that the balls are in fact distinguishable.

If both balls were red, however, and therefore indistinguishable to you at a glance, you have again only a 50% chance of guessing right. Jim can easily tell that you cannot tell the balls apart.

(This similar to publishable proofs: a verifier uses randomness to verify such as for polynomial equality. The set of languages with publishable proofs is $\mathrm{BP}\cdot\Sigma\cdot P$.)

Does this conversational proof have any other applications? One group of objects computer scientists often try to determine if they are distinguishable are graphs. If you had an oracle that told you whether two graphs are isomorphic, could you use this to convince Jim of this fact?

Let us call Jim the Verifier as he is trying to verify whether two graphs are isomorphic. Let us then call the party with the isomorphism oracle the Prover as he is trying to prove to the verifier this fact.

The Verifier has two graphs, G_1 and G_2 represented as a list of edges. A conversation between the Prover and the Verifier ensues:

Verifier: pick randomly one of G_1, G_2 then randomize the vertex numbering. Formally, let $H = \pi(G_i)$ where π is a random permutation. Show H to Prover.

Prover: Compare H to G_1 and G_2. Announce: "You showed me graph G_i." (where $G_i \cong H$).

Verifier: "Correct." Accept.

This "proof" works for exactly the same reason as it did for the colored balls. Formally, for $G_1 \ncong G_2$, the Prover can make the Verifier accept. For $G_1 \cong G_2$, however, the distribution over $\pi(G_1)$ is the same as that over $\pi(G_2)$. Hence the Prover can guess correctly only 50% of the time.

2 Interactive Proofs

Definition 1 *An* **Interactive Proof** *consists of a* **Prover**, *P(word, history), a* **Verifier**, *V(word, history, random bit string), and a* **conversation***:*

$$\begin{aligned}
&V(w, \epsilon, r) \to V_1\\
&P(w, V_1) \to P_1\\
&V(w, V_1 \cdot P_1, r) \to V_2\\
&P(w, V_1 \cdot P_1 \cdot V_2) \to P_2\\
&\vdots\\
&V(w, V_1 \cdot P_1 \cdot V_2 \cdots P_{f(|w|)}, r) \to \{\mathrm{acc}, \mathrm{rej}\}
\end{aligned}$$

We say $L \in \mathrm{IP}$ *if*

$$\exists V \in P s.t. \begin{cases} \forall w \in L\ \exists P: & \Pr_r [P \leftrightarrow V(w,r) = \mathrm{acc}] > \frac{2}{3} \\ \forall w \notin L\ \forall P: & \Pr_r [P \leftrightarrow V(w,r) = \mathrm{acc}] < \frac{1}{3} \end{cases}$$

For IP *the function* f *is polynomial. We can also define* $\mathrm{IP}(k)$ *with* $f(n) = k$ *for the languages which accept or reject after a constant,* k*, number of rounds.*

One can see from the definition of IP that the Prover does not have access to the random bits, r. The Prover gets only the word and the conversation history. What would happen if P had access to r? This is the "public coins" scenario, or as we will see, Arthur-Merlin proofs.

3 Arthur-Merlin Proofs

If the coins are public, the Verifier (Arthur) may be silent, as the Prover (Merlin) can compute any function Arthur could. So it seems that Merlin could just compute the whole conversation. This is equivalent to publishable proofs and equals $\mathrm{BP} \cdot \Sigma \cdot P$. But we can escape this bound because Arthur can choose new random bits for each step of the conversation.

Definition 2 *An* **Arthur-Merlin** *proof consists of the same three elements as Interactive proofs: a Prover, M(word, sequence of random bit strings), a Verifier, A(word), and a conversation:*

$$\begin{aligned} &A(w) \to r_1 \\ &M(w, r_1) \to M_1 \\ &A(w) \to r_2 \\ &M(w, r_1, r_2) \to M_2 \\ &\vdots \\ &A(w, r_1, \ldots, r_{f(|w|)}, M_1, \ldots, M_{f(|w|)}) \to \{\mathrm{acc}, \mathrm{rej}\} \end{aligned}$$

We say $L \in \mathrm{AM}$ *if*

$$\exists A \in P s.t. \begin{cases} \forall w \in L\ \exists M: & \Pr_{r_1, \ldots, r_{f(|w|)}} [M \leftrightarrow A(w, r_i) = \mathrm{acc}] > \frac{2}{3} \\ \forall w \notin L\ \forall M: & \Pr_{r_1, \ldots, r_{f(|w|)}} [M \leftrightarrow A(w, r_i) = \mathrm{acc}] < \frac{1}{3} \end{cases}$$

We define AM *and* $\mathrm{AM}(k)$ *as for* IP *previously.*

$\mathrm{AM}(1) = \mathrm{BP} \cdot \Sigma \cdot P$ as discussed previously.

Theorem 3 $\mathrm{IP}(k(n)) = \mathrm{AM}(\theta(k(n)))$

Theorem 4 *For constant* k*,* $\mathrm{AM}(k) \subseteq \mathrm{AM}(1)$

Theorem 5 *If graph isomorphism is NP-complete,* $\Sigma_3^P = \Pi_3^P$.

Proof Graph isomorphism is co-NP-complete, hence it is $\in \mathrm{IP}(4)$. So $NP \subseteq \mathrm{IP}(4) = \mathrm{AM}(\theta(1)) \subseteq \mathrm{AM}(1) = \mathrm{BP} \cdot \Sigma \cdot P \subseteq P/\mathrm{poly} \Rightarrow \Sigma_3^P = \Pi_3^P$. ■