CS 6810: Theory of Computing **Fall 2021**

Lecture 16: Oct 21, 2021

Lecturer: Eshan Chattopadhyay *Scribe: Ricky Shapley*

1 Interactive Proofs

We already saw that **dIP** = **NP**. So in order to make use of the potential of interaction between a verifier and a prover, we need to make the verifier probabilistic.

Definition 1.1 (**IP**)**.** *We say a language $L \in \mathbf{IP}[k]$ if there is a probabilistic polytime verifier V with private randomness such that*

$$\textit{(completeness)} \quad x \in L \implies \exists P \Pr\left[\mathsf{out}_V\langle V, P\rangle(x) = 1\right] \geq \frac{2}{3}$$

$$\textit{(soundness)} \quad x \notin L \implies \forall P \Pr\left[\mathsf{out}_V\langle V, P\rangle(x) = 1\right] < \frac{1}{3}$$

where any prover P can have unbounded computational power and where $\mathsf{out}_V\langle V, P\rangle(x)$ denotes the output of the verifier V at the end of an interaction between V and P (beginning at V) when given input x. Then we can define $\mathbf{IP} = \cup_{c\geq 1}\mathbf{IP}[n^c]$.

Theorem 1.2 ([2, 3])**. IP = PSPACE**

We will not prove this entirely. There is an interesting account about the discovery of this result by Lázló Babai [1].

2 Graph Non-isomorphism

We will gain some intuition on how this proof should work by looking at graph non-isomorphism.

We say graphs G_1 and G_2 are isomorphic ($G_1 \cong G_2$) if there is some permutation $\pi : V \to V$ such that $\pi(G_1) = G_2$. Then we define the graph isomorphism language $GI = \{\langle G_1, G_2\rangle : G_1 \cong G_2\}$. It is easy to see that $GI \in \mathbf{NP}$, as we can simply use the permutation π as the certificate.

Similarly, we will define the graph non-isomorphism language $GNI = \{\langle G_1, G_2\rangle : G_1 \ncong G_2\}$. Clearly, $GNI \in \mathbf{coNP}$, but is $GNI \in \mathbf{IP}$?

The answer is yes. Here is how we can do it: The verifier will select a random permutation π and a random bit $b \in \{1, 2\}$, then send $\pi(G_b)$ to the prover. The verifier receives back a bit b', which is the prover's guess of what b was. The verifier accepts if $b = b'$, and rejects otherwise.

Let's confirm that this shows $GNI \in \mathbf{IP}$. Suppose $G_1 \ncong G_2$. Then an honest prover can always correctly determine b from $\pi(G_b)$. If $G_1 \cong G_2$, then there is a $1/2$ chance that any prover guessed the correct b. Running this process multiple times can reduce the soundness error to below $1/3$.

3 Public Coins (Arthur-Merlin Games)

Now, we consider what happens if the prover has access to the verifier's randomness. (Here, the verifier is Arthur and the prover is Merlin, since Merlin, as a wizard, can know all of Arthur's secrets.)

Definition 3.1 (**AM**). *We say a language $L \in \mathbf{AM}[k]$ if L can be decided by a k round interactive proof, where the messages sent by the verifier are random bits of polynomial length (and the verifier has no other randomness).*

Usually, we say $\mathbf{AM} = \mathbf{AM}[2]$, in which the verifier sends a single random string r, and the prover returns a message m. Formally, $L \in \mathbf{AM}$ if

$$x \in L \implies \exists P \Pr[V(x, r, m) = 1] \geq \frac{2}{3}$$
$$x \notin L \implies \forall P \Pr[V(x, r, m) = 1] < \frac{1}{3}.$$

Definition 3.2 (**MA**). **MA** *is the class of languages where the prover first sends a message and the verifier then generates some randomness and determines inclusion in the language.*

Theorem 3.3 (Goldwasser, Sipser, 1987). $\mathbf{IP}[k] \subseteq \mathbf{AM}[k+2]$

We will prove the following easier result that uses the same main idea.

Theorem 3.4. $GNI \in \mathbf{AM}$

3.1 Universal Hash Functions

For our proof, we will first need a notion of hash functions.

We desire to find a collection of hash functions $\mathcal{H}_{n,\ell} = \left\{h : \{0,1\}^n \to \{0,1\}^\ell\right\}$ where for any pair of distinct x and x', $\Pr_{h \in \mathcal{H}}[h(x) = h(x')] \leq \frac{1}{L}$ where $L = 2^\ell$. In particular, we will use $\mathcal{H}_{n,\ell} = \{h_{a,b}\}_{a,b \in \mathbb{F}_{2^n}}$, where $h_{a,b} = ax + b \pmod{2^\ell}$. (The proof of why this satisfies the desired properties can be found in the book.)

3.2 Set Lower Bound Protocol

Now we introduce the set lower bound protocol, which decides whether a set S has cardinality at least k up to a factor of 2. Formally, we have

- A set $S \subseteq \{0,1\}^n$
- A threshold k

and we desire a protocol that if $|S| > k$ accept with probability at least $\frac{2}{3}$, and if $|S| < \frac{k}{2}$ reject with probability at least $\frac{2}{3}$.

Why is this relevant to GNI? Consider

$$S = \{\langle H, \pi \rangle : H \text{ isomorphic to at least one of } G_1, G_2, \pi \in \mathrm{Aut}(H)\}$$

Then, notice that if $G_1 \cong G_2$, $|S| = n!$, but if $G_1 \ncong G_2$, $|S| = 2n!$. So if we can show that the set lower bound protocol is an **AM** protocol, then it shows that $GNI \in \mathbf{AM}$.

To achieve this, we fix ℓ such that $\frac{2^\ell}{4} \leq k \leq \frac{2^\ell}{2}$. Then the verifier randomly samples $y \in \{0,1\}^\ell$ and $h \in \mathcal{H}_{n,\ell}$, and the prover tries to respond with a some $x \in S$ such that $h(x) = y$ (including a certificate that $x \in S$). The verifier accepts if it verifies that $x \in S$ and $h(x) = y$, and rejects otherwise.

If $|S| < \frac{k}{2}$, then $|h(S)| < \frac{k}{2}$, so the probability of accepting is no more than $\frac{k}{2^{\ell+1}}$. (The probability of acceptance is equivalent to the proportion of $\{0,1\}^\ell$ that is in the image of $h(S)$.)

If $|S| > k$, for a fixed h,

$$|h(s)| \geq |S| - \sum_{x \neq x' \in S} \mathbb{1}_{h(x)=h(x')}$$

so

$$\begin{aligned}\mathbb{E}|h(s)| &\geq |S| - \sum_{x \neq x' \in S} \mathbb{E}\mathbb{1}_{h(x)=h(x')} \\ &\geq |S| - \binom{|S|}{2}\frac{1}{2^\ell}\end{aligned}$$

and this means the probability of acceptance is at least

$$\begin{aligned}\frac{|S|}{2^\ell} - \frac{|S|^2}{2^{2\ell+1}} &\geq \frac{|S|}{2^\ell}\left(1 - \frac{|S|}{2^{\ell+1}}\right) \\ &\geq \frac{k}{2^\ell}\left(1 - \frac{1}{4}\right) \\ &\geq \frac{3k}{2^{\ell+2}}.\end{aligned}$$

As we have a gap between the probabilities of acceptance, repetition can ensure that we get our desired completeness and soundness errors.

Therefore, as we have shown that this set lower bound protocol is an **AM** protocol, we can conclude that $GNI \in \mathbf{AM}$.

References

[1] László Babai. E-mail and the unexpected power of interaction. In *Proceedings Fifth Annual Structure in Complexity Theory Conference*, pages 30–44. IEEE, 1990.

[2] Carsten Lund, Lance Fortnow, Howard Karloff, and Noam Nisan. Algebraic methods for interactive proof systems. *Journal of the ACM (JACM)*, 39(4):859–868, 1992.

[3] Adi Shamir. Ip= pspace. *Journal of the ACM (JACM)*, 39(4):869–877, 1992.