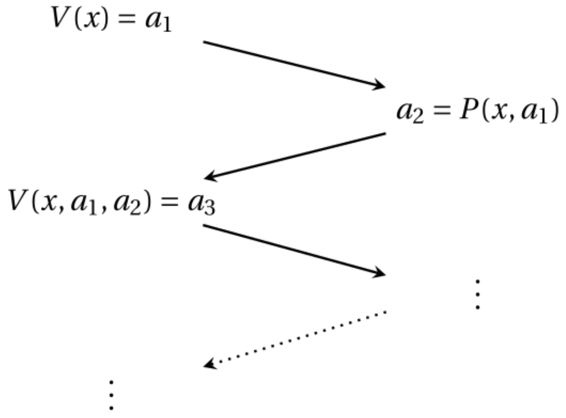
CS 6810: Theory of Computing **Fall 2023**

Lecture 23: Nov 9, 2023

Lecturer: Eshan Chattopadhyay *Scribe: Evan Williams*

1 Introduction

Recall from last lecture the setting of *interactive* proofs. That is, we have an interactive proof system where an all-powerful prover P and a deterministic, polynomial-time verifier V interact. The verifier asks questions while the prover responds, and at the end the verifier decides whether or not to accept the input. For a language L and an input x, the prover wants to convince the verifier that $x \in L$. Crucially, all communication between the prover and the verifier are $\text{poly}(|x|)$, where x is the certificate.



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

- *(completeness)* $x \in L \implies \exists P \Pr[\mathsf{out}_V\langle V, P\rangle(x) = 1] > \frac{2}{3}$
- *(soundness)* $x \notin L \implies \forall P \Pr[\mathsf{out}_V\langle V, P\rangle(x) = 1] < \frac{1}{3}$

where any prover P can have unbounded computational power and where $\mathsf{out}_V\langle P, V\rangle(x)$ is the output of verifier V at the end of k rounds of interaction between P and V (beginning at V) when given input x.

2 Arthur-Merlin Protocols (Public Coins)

Note that we defined $\mathsf{IP}[k]$ such that the randomness of the verifier is **private**. Now we consider what happens if the prover P has access to the verifier's randomness. In an Arthur-Merlin protocol, Arthur and Merlin take the roles of verifier and prover, respectively, and Arthur's actions are limited to either rolling coins and sending the result to Merlin or deciding to terminate by accepting or rejecting.

Definition 2.1. (AM) *We say a language $L \in \mathsf{AM}[k]$ if L can be decided by a k round interactive proof system, where the messages sent by the verifier are random bits of polynomial length (and the verifier has no other randomness). Usually, we say $\mathsf{AM} = \mathsf{AM}[2]$, in which the verifier sends a single random string r and the prover returns a message m. Formally, $L \in \mathsf{AM}$ if:*

- *(completeness)* $x \in L \implies \exists P \Pr[V(x,r,m) = 1] > \frac{2}{3}$
- *(soundness)* $x \notin L \implies \forall P \Pr[V(x,r,m) = 1] < \frac{1}{3}$

Definition 2.2. (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 2.3. *(Goldwasser, Sipser 1987).* $\forall k$, $\mathsf{IP}[k] \subseteq \mathsf{AM}[k+2]$

We will prove the following (easier) result that uses the same key idea.

Theorem 2.4. *Graph Non-Isomorphism (GNI)* $\in \mathsf{AM}$

Recall the graph non-isomorphism problem from last lecture. We say graphs G_1 and G_2 are isomorphic ($G_1 \approx G_2$) if there is some permutation $\pi : V \to V$ such that $\pi(G_1) = G_2$. Thus, we define the graph non-isomorphism language $GNI = \{\langle G_1, G_2 \rangle : G_1 \not\approx G_2\}$.

2.1 Universal Hash Family

The main tool we use for the set lower bound protocol is a *universal hash family.* We desire to find a collection of hash functions $\mathcal{H}_{n,l} = \{h : \{0,1\}^n \to \{0,1\}^l\}$ such that $\forall x \neq y \in \{0,1\}^n$, $\Pr[h(x) = h(y)] \leq \frac{1}{L}$ where $L = 2^l$. We will use $\mathcal{H}_{n,l} = \{h_{a,b}\}_{a,b \in \mathbb{F}_{2^n}}$ where $h_{a,b} = ax + b \pmod{L}$. See the book for why we choose this family.

2.2 Set Lower Bound Protocol

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 are looking for a protocol that if $|S| \geq k$ (good), accepts with probability at least $\frac{2}{3}$ and if $|S| \leq \frac{k}{2}$ (bad), rejects with probability at least $\frac{2}{3}$. Consider:

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

Observe that if $|S| = 2n!$, $G_1 \not\approx G_2$. If $|S| = n!$, then $G_1 \approx G_2$. If we can show that the set lower bound protocol is an AM protocol, then it shows $GNI \in \mathsf{AM}$.

Pick l such that $2^{l-2} \leq k \leq 2^{l-1}$. Then, the verifier randomly samples $y \in \{0,1\}^l$ and $h \in \mathcal{H}_{n,l}$ and the prover tries to respond with some $x \in S$ such that $h(x) = y$, as well as 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 acceptance is at most $\frac{k}{2^{l+1}}$ (the proportion of the $\{0,1\}^l$ that is in the image of $h(S)$). So if $|S| > k$, for a fixed h we have that:

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

So we have that the probability of Arthur accepting is at least:

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

The public-coin interactive proof system for GNI consists of the verifier and prover running several iterations of the set lower bound protocol for the set S as defined above, where the verifier accepts iff the fraction of accepting iterations was at least $0.6p$. Using the Chernoff bound it can be seen that a constant number of iterations will suffice to ensure completeness probability at least $\frac{2}{3}$ and soundness error at most $\frac{1}{3}$ Therefore $GNI \in \mathsf{AM}$. ■

3 Perfect Completeness of MA

Theorem 3.1. *(Perfect Completeness of* MA*). For any language $L \in \mathsf{MA}$, there exists a probabilistic polynomial time verifier V such that:*

- $x \in L \implies \exists m, \Pr[V(x,m,r) = 1] = 1$
- $x \notin L \implies \forall m, \Pr[V(x,m,r) = 1] < 1/3$

Proof. For any x, define $1_{x,m} = \{r : V(x,m,r) = 1\} \subseteq \{0,1\}^l$. By standard error reduction we can assume that

- $x \in L \implies \exists m, |1_{x,m}| \geq (1-\epsilon)L$
- $x \notin L \implies \forall m, |1_{x,m}| < \epsilon L,$

where $\epsilon = 2^{-n}$ and $L = 2^l$. If the probability of success is large ($x \in L$) then 1_x is large. Now we use the trick (that we say in Lecture 19) that was used to place BPP in PH. We proved that for $t = poly(n)$, there exist vectors $v_1, ..., v_t$ such that for all S, $|S| \geq (1-\epsilon)L$, $\bigcup_{i=1}^t (S + v_i) = \{0,1\}^l$. The rest of the proof is now direct.

Next lecture, we will show that $\mathsf{MA} \subseteq \mathsf{AM}$.