E0 337: Topics in Advanced Cryptography 9/Oct/23

Lecture 12

Instructors: Dr.Bhavana Kanukurthi, Dr.Chaya Ganesh *Scribe: Girisha Shankar*

1 Welcome to E0 337

1.1 Course Information

Contact information and office hours:

- **Lecturer:** Bhavana Kanukurthi (bhavana@iisc.ac.in, Chaya Ganesh (chaya@iisc.ac.in).
- **Presenter:** Bhargav Thankey (thankeyd@iisc.ac.in).

1.2 Course Topics

The course will cover the following topics:

- *Rational Proofs* by Pablo Azar and Silvio Micali - STOC'2012

2 Introduction

We have seen interactive proof systems where an unbounded prover interacts with a bounded verifier to prove a certain relation $\mathcal{R}(x, y)$ by providing a polynomial length proof (polynomial in $|x|$). The soundness of the proof system guards against a malicious prover. In this paper, authors introduce a new class of proofs called *rational proof* system where an unbounded prover and a poly time verifier interact again, on inputs a string x and a function f, so that the Verifier may learn $f(x)$. The novelty of their setting is that there are no longer honest and malicious provers, but only rational ones. The verifier rewards the prover based on the "quality" of the proof. The prover is incentivized to provide an accepting proof so as to maximize its reward.

In the following, we will discuss some of the main results from the paper.

3 The class RMA[1]

This is an extension of classical single round Merlin-Arthur class to the rational setting.

Definition 1. ($\mathsf{RMA}[1]$) $L \in \{0,1\}^*$ is in $\mathsf{RMA}[1]$ if there exists poly time computable random function $R : \{0,1\}^* \times \{0,1\}^* \mapsto \mathbb{R}_{\geq 0}$ and a poly time computable $\Pi : \{0,1\}^* \times \{0,1\}^* \mapsto \{0,1\}$ such that $\forall x \in \{0,1\}^*$:

1. there exists a unique y^* such that $y^* = \text{argmax}_y \, \mathbb{E}[R(x, y)]$
2. $x \in L \iff \Pi(x, y^*) = 1$

Definition 2. *$L \in \mathsf{PP}$ if there exists a DTM M and a polynomial p such that*
$x \in L \iff |\{y \in \{0,1\}^{p(|x|)} : M(x, y) = 1\}| \geq \dfrac{2^{p(|x|)}}{2}$.

Definition 3 (Proper Scoring Rules)**.** *S is said to be a proper scoring rule for $\mathcal{D}$ if $\forall \mathcal{D}' \neq \mathcal{D}$:*

$$\sum_{\omega \in \Omega} \mathcal{D}(\omega) S(\mathcal{D}, \omega) > \sum_{\omega \in \Omega} \mathcal{D}(\omega) S(\mathcal{D}', \omega)$$

Remark There exist S which can be computed in poly time and lies in $[0, 1]$.

Theorem 4. $\mathsf{PP} \subseteq \mathsf{RMA}[1]$

Proof. $\mathsf{MAXSAT} = \{\varphi : \#\mathsf{SAT}$ assignments of $\varphi \geq 2^n/2\}$.
Merlin knows $\#\varphi$.
Let Y be a 0/1 RV which is 0 with probability $1 - \frac{\#\varphi}{2^n}$ and 1 with probability $\frac{\#\varphi}{2^n}$. Let this distribution be $\mathcal{D}$. We would like Merlin to send $\mathcal{D}$ instead of $\mathcal{D}'$.

Protocol 1:

1. Merlin sends $y \in \{0, \ldots, 2^n\}$ to Arthur.
2. Arthur samaples $(r_1, \ldots, r_n)$ uniformly at random from $\{0, 1\}^n$ and computes $b = \varphi(r_1, \ldots, r_n)$. Arthur also computes $S(y, b)$ and pays it as the reward to Merlin.
3. Arthur accepts if and only if $y \geq \frac{2^n}{2}$.

   $$\Pr[b = 0] = 1 - \frac{\#\varphi}{2^n} \text{ and } \Pr[b = 0] = \frac{\#\varphi}{2^n}$$

   i.e., b's distribution is $\mathcal{D}$.

$$\begin{aligned} \mathbb{E}[R(x, y)] &= \Pr[b = 0]S(y, 0) + \Pr[b = 1]S(y, 1) \\ &= \sum_{\omega \in \{0,1\}} \mathcal{D}(\omega) S(\mathcal{D}', \omega) \\ \implies \operatorname*{argmax}_y \mathbb{E}[R(x, y)] &= \#\varphi \end{aligned}$$

□

4 The class RMA[k]

This is the class RMA with k rounds, where Merlin goes first.

Notations:

1. Views: $\mathcal{P}_i = (\mathcal{P}_{i-1}, \mathcal{T}_{i-1}, r_i)$
   $\mathcal{V}_i = (\mathcal{V}_{i-1}, \mathcal{T}_{i-1}, a_i, s_i)$
2. Messages: a_i, b_i
3. Randomness: r_i, s_i
4. Transcript: $\mathcal{T}_i = (\mathcal{T}_{i-1}, a_i, b_i)$
   Initial transcript: $(\mathcal{P}_0, \mathcal{V}_0, \mathcal{T}_0) = (x)$
   Final transcript : $\mathcal{T}$

The protocol is public coins if a_i contains r_i and b_i contains s_i.

Definition 5 (RIP)**.** *A language L is said to have a* Rational Interactive Proof *(RIP) if there exists $\mathcal{P}, \mathcal{V}$ and poly time computable Π, R such that $\forall x \in \{0, 1\}^*$:*

1. *All messages of $\mathcal{V}$ can be computed in poly time. Also, all messages are of length poly in $(|x|)$.*

2. $x \in L \iff \Pi(\mathcal{T}) = 1$,

3. *The prover does not want to deviate first if the protocol has been executed correctly upto rounds* $i-1$. *Then* $a_i = \text{argmax}_{a_i'} \mathbb{E}[R(\mathcal{T})]$ *and* a_i *is unique. Expectation is taken over all* $\mathcal{T}$ *consistent with* $\mathcal{P}_{i-1}, a_i'$.

Definition 6. *(*$\mathsf{RMA}[k]$*)* $L \subseteq \{0,1\}^*$ *such that* L *has* k *round RIP which is public coins.*

4.1 The counting hierarchy (CH)

- $\mathsf{CP}_0 = \mathsf{P}$
- $\mathsf{CP}_1 = \mathsf{PP}$
- $\mathsf{CP}_k = L$ such that there exists $L' \in \mathsf{CP}_{k-1}$ and a poly p such that

$$x \in L \iff |\{y \in \{0,1\}^{p(|x|)} : (x,y) \in L'\}| \geq \frac{2^{p(|x|)}}{2}$$

Theorem 7. $\mathsf{RMA} = \mathsf{CH}$ *where* $\mathsf{RMA} = \bigcup_{k \geq 1} \mathsf{RMA}[k]$

Claim 8. $\mathsf{CP}_k = \mathsf{PP}^{\mathsf{CP}_{k-1}}$. *In fact the* PP *machine needs to make just one query on each computational path.*

Proof. (of Theorem 7)

Lemma 9. $\forall k \mathsf{CP}_k \subseteq \mathsf{RMA}[k]$

Proof. By induction. Base case is Theorem 4.
Induction step: Assume every language in CP_{k-1} can be decided by 1 Arthur interacting with $k-1$ non-colluding Merlins. Let $L \in \mathsf{CP}_k$, $\mathsf{N}^{\mathsf{CP}_{k-1}}$ be the corresponding PP machine.

For a x, let the number of accepting paths of $\mathsf{N}^{\mathsf{CP}_{k-1}}$ be α. Merlin knows α.

$$y = \begin{cases} 0 \text{ w.p. } 1 - \dfrac{\alpha}{2^{p(|x|)}} \\ 1 \text{ w.p. } \dfrac{\alpha}{2^{p(|x|)}} \end{cases}$$

Protocol 2 :

1. The kth Merlin sends α.
2. Arthur picks $(r_1, \ldots, r_{p(|x|)})$ uniformly at random and checks if $(x, r_1, \ldots, r_{p(|x|)}) \in L'$ using $1, \ldots, k-1$ Merlins.
   $b = 1$ if it is in L' 0 otherwise
3. Arthur rewards Merlin with $S(\alpha, b)$.
4. Arthur accepts if and only if $\alpha \geq \dfrac{2^{p(|x|)}}{2}$.

Combining Merlins : All Merlins can collude to maximise the sum of their rewards.

Let $\Delta = \min_{i\in[k]} \min_{\mathcal{D}\neq\mathcal{D}'}[\mathbb{E}\, S(\mathcal{D},\omega) - \mathbb{E}\, S(\mathcal{D}',\omega)]$.

If the rewards were $r_1,\ldots,r_k$, pay $\sum_{i=1}^{k}\left(\frac{\Delta}{1+\Delta}\right)^{i-1} r_i$ □

Claim 10. *1. Let $f(x,r)$ be a random function in $\mathsf{FP}^{\mathcal{C}}$ where $\mathcal{C}$ is an arbitrary complexity class. Then $\mathbb{E}\, f(x,r) \in \mathsf{FP}^{\mathsf{PP}^{\mathcal{C}}}$.*

2. Let $g(x,y) \in \mathsf{FP}^{\mathcal{C}}$. Then $\operatorname{argmax}_y g(x,y) \in \mathsf{FP}^{\mathsf{NP}^{\mathcal{C}}}$.

Lemma 11. $\mathsf{RMA}[k] \subseteq \mathsf{CP}_{2k+1}$

Proof. $\mathsf{RMA}[1] \subseteq \mathsf{CP}_3$.
Let $L \in \mathsf{RMA}[1]$. Let R, Π be as in Definition 1.
$y^* = \operatorname{argmax}_y \mathbb{E}[R(x,y)]$
$\mathbb{E}[R(x,y)] \in \mathsf{FP}^{\mathsf{PP}}$.
y^* can be computed in $\mathsf{FP}^{\mathsf{NP}^{\mathsf{PP}}}$. y^* can be computed by $M^{\mathsf{NP}^{\mathsf{PP}}}$ where M is a poly time DTM.
$M^{\mathsf{NP}^{\mathsf{PP}}}$ decides L.
$L \in \mathsf{P}^{\mathsf{NP}^{\mathsf{PP}}} \subseteq \mathsf{P}^{\mathsf{PP}^{\mathsf{PP}}} \subseteq \mathsf{PP}^{\mathsf{PP}^{\mathsf{PP}}} = \mathsf{CP}_3$. □

□