CS221: Computational Complexity Prof. Salil Vadhan

Lecture 30: Arthur-Merlin Games

12/6 *Scribe: Noam Zeilberger*

Contents

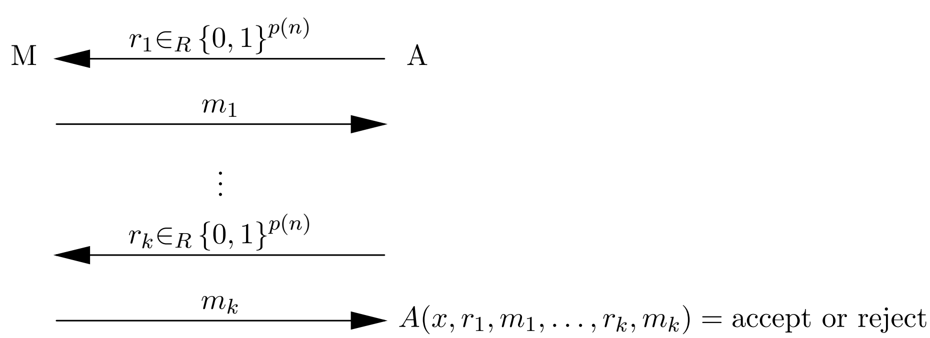
1 Remarks on $\mathbf{P}^{\#\mathbf{P}} \subseteq \mathbf{IP}$ and $\mathbf{IP} = \mathbf{PSPACE}$

- These constructions are based on specific complete problems and do not relativize.
- They provide interactive protocols with perfect completeness, hence a corollary of $\mathbf{IP} = \mathbf{PSPACE}$ is that $\mathbf{IP} = \mathbf{IP}$ with perfect completeness (a result known before $\mathbf{IP} = \mathbf{PSPACE}$).
- They rely on no hidden randomness for the verifier (i.e. they are "public coin" interactive proofs).

2 Arthur-Merlin Games

2.1 Introduction

The final remark leads to the notion of *Arthur-Merlin games*—interactive proofs between a verifier (Arthur) and a prover (Merlin) in which the verifier's messages are simply its random coin tosses:



A corollary to $\mathbf{IP} = \mathbf{PSPACE}$ is that Arthur-Merlin games are as powerful as interactive proofs:

Corollary 1 (Goldwasser, Sipser) $\mathbf{IP} = \{L \mid L$ *has an Arthur-Merlin game*$\}$

However, Arthur-Merlin games were developed by László Babai independently of Goldwasser, Micali, and Rackoff's interactive proofs, and his motivations originated from complexity theory, whereas theirs from cryptography.

Another interpretation of Arthur-Merlin games is as randomized alternation. Consider that if we assume perfect completeness, then

$$\begin{aligned} x \in L &\Rightarrow \forall r_1 \exists m_1 \forall r_2 \cdots A(x, \overline{r}, \overline{m}) = \text{accept} \\ x \notin L &\Rightarrow \exists r_1 \forall m_1 \exists r_2 \cdots A(x, \overline{r}, \overline{m}) = \text{reject} \end{aligned}$$

But in fact the soundness condition is stronger, namely that

$$x \notin L \Rightarrow \exists^+ r_1 \forall m_1 \exists^+ r_2 \cdots A(x, \overline{r}, \overline{m}) = \text{reject}$$

where "$\exists^+$" means "there exist many"/"for almost all." A similar way of thinking about Arthur-Merlin games is as "games versus Nature"—Arthur representing random choices made by Nature, like the random shuffling of a deck in Solataire (and Merlin, perhaps, the supernatural).

2.2 MA and AM

It is natural to treat the number of messages as a resources:

Definition 2 $\mathbf{AM}[k]$ *is the class of languages that have Arthur-Merlin games in which k total messages are sent, beginning with Arthur. Likewise,* $\mathbf{MA}[k]$ *is the class of languages with k-message Arthur-Merlin games in which Merlin begins.*

We write $\mathbf{AM}^+[k]$ for $\mathbf{AM}[k]$ with perfect completeness. By the above casting of Arthur-Merlin games in terms of randomized alternation, it is immediate that $\mathbf{AM}^+[k]$ and $\mathbf{MA}^+[k]$ are contained in the polynomial hierarchy, for all k. But in fact, we will prove something much stronger.

Definition 3 *We write* $\mathbf{AM} \stackrel{\text{def}}{=} \mathbf{AM}[2] = \mathbf{AM}^+[2]$ *and* $\mathbf{MA} \stackrel{\text{def}}{=} \mathbf{MA}[2] = \mathbf{MA}^+[2]$ *(where the equalities giving perfect completeness are by Problem Set 6). In general, a string of* $\mathbf{A}$*s and* $\mathbf{M}$*s denotes an Arthur-Merlin game where a message is sent by the player corresponding to the first symbol, then by the player corresponding to the second symbol, etc. For example,* $\mathbf{AMAM} = \mathbf{AM}[4]$*. Note that* $\mathbf{AA} = \mathbf{A}$*,* $\mathbf{MM} = \mathbf{M}$*, since separate messages sent on two successive rounds by the same player can be combined into one.*

Theorem 4 $\forall k \geq 2$ $\mathbf{AM}[k] = \mathbf{AM}$

Proof: We start by showing that $\mathbf{MA} \subseteq \mathbf{AM}$. The basic idea is to simply swap the order of the messages in the exchange, but then also use amplification in order to reduce the verifier's error rate to a sufficient extent that soundness still holds for the $\mathbf{AM}$ game. Explicitly, suppose that m_1 is the message sent by Merlin, r_1 the random string sent by Arthur, and that the original $\mathbf{MA}$ verifier A has has two-sided error rate $\epsilon = \epsilon(n)$ on inputs of length n. Then the following holds:

$$\begin{aligned} x \in \mathbf{L} &\Rightarrow \exists m_1 \Pr_{r_1}[A(x, m_1, r_1) = \text{accept}] \geq 1 - \epsilon \\ &\Rightarrow \Pr_{r_1}[\exists m_1 A(x, m_1, r_1) = \text{accept}] \geq 1 - \epsilon \end{aligned}$$

$$\begin{aligned} x \notin \mathbf{L} &\Rightarrow \forall m_1 \Pr_{r_1}[A(x, m_1, r_1) = \text{accept}] \leq \epsilon \\ &\Rightarrow \Pr_{r_1}[\exists m_1 A(x, m_1, r_1) = \text{accept}] \leq 2^{|m_1|} \cdot \epsilon \end{aligned}$$

Since we can reduce A's error rate to $2^{-\Omega(q(n))}$ using amplification with polynomially many random strings $\overline{r} = r_1, \ldots, r_{q(n)}$ and having A rule by majority, can make $\Pr_{\overline{r}}[\forall m_1\, A(x, m_1, \overline{r}) = \text{reject}] \leq 2^{|m_1|} \cdot 2^{-\Omega(q(n))}$ exponentially small by taking $q(n)$ to be a sufficiently large polynomial.

Now, to show that $\forall k \geq 2$ $\mathbf{AM}[k] = \mathbf{AM}$ we can use the identity $\mathbf{MAM} = \mathbf{AMM} = \mathbf{AM}$ and proceed by induction. ■

The following states that the Goldwasser–Sipser equivalence between private coins and public coins holds even when the number of rounds is constrained to be a constant:

Theorem 5 (Goldwasser-Sipser) $\mathbf{IP}[k] \subseteq \mathbf{AM}[O(k)]$

Corollary 6 $\forall k \geq 2$ $\mathbf{IP}[k] = \mathbf{AM} \subseteq \Pi_\mathbf{2}\mathbf{P}$

Corollary 7 Graph Nonisomorphism $\in \mathbf{AM}$

AM and **MA** should be thought of as randomized analogues of **NP**, and so unlikely to be much more powerful (e.g. like **BPP** versus **P**). This is supported by the following fact:

Theorem 8 **co-NP** $\subseteq$ **AM** $\Rightarrow$ **PH** $=$ **AM**

Proof: It suffices to show that $\Sigma_\mathbf{2}\mathbf{P} \subseteq \mathbf{AM}$ (hence that $\Sigma_\mathbf{2}\mathbf{P} \subseteq \Pi_\mathbf{2}\mathbf{P}$, which in turn implies $\mathbf{PH} = \Sigma_\mathbf{2}\mathbf{P} = \mathbf{AM}$). Consider a $\Sigma_\mathbf{2}\mathbf{P}$ statement $\exists x_1 \forall x_2\, \varphi(x_1, x_2)$. It has the $\mathbf{MA}[3]$ game in which Merlin begins by sending x_1, after which the players engage in the **AM** game for $\forall x_2\, \varphi(x_1, x_2)$ (which exists by assumption). But $\mathbf{MAM} = \mathbf{AM}$. ■

Corollary 9 *If* Graph Isomorphism *is* **NP**-*complete, then* **PH** = **AM**.

Proof: If the problem is **NP**-complete, then Graph Nonisomorphism is **co-NP**-complete, thus **co-NP** $\subseteq$ **AM**. ■