Lecture 10

Arthur-Merlin Games

April 29, 2004
Lecturer: Paul Beame
Notes: Ethan Phelps-Goodman

10.1 The Collapse Lemma

The main lemma of this lecture is the following:

Lemma 10.1 (Babai). $\mathsf{MA} \subseteq \mathsf{AM} = \mathsf{AM}[k] = \mathsf{MA}[k+1]$, *for any constant* k. *That is,* AM *can simulate any constant round Arthur-Merlin game.*

Proof. Suppose that there are two rounds of the Arthur-Merlin game that go in sequence MA.... We show how to simulate them by a modified game that begins AM... and has the same alternation pattern after the first two rounds. This will be enough to prove the claim because it will also allow us to convert any game sequence AMA... to AAM... $= \mathsf{AM}$... and MAM... to AMM... $= \mathsf{AM}$....

It is somewhat intuitive that AM should be more powerful than MA, because in the former Merlin gets to look at the random bits before deciding on his answer. The argument first shows that one can bound the increase in Merlin's power and then use amplification of the original protocol to ensure that this increase in Merlin's convincing power is not enough to allow him to cheat.

Start with a zero-one random variable $V(x, y, r)$. Think of V as determining whether the protocol accepts in the remaining rounds. Define $H(x, yr) = \Pr[V(x, y, r) = 1]$, where the probability is over remaining rounds of the protocol (not r). Let $\Psi(x) = MyAr\ H(x, y, r)$ be the probability that theMA... protocol accepts x. Also, say that the ys are taken from the set Y and the rs are taken from the set R. We use A for averaging over the set R and M for maximizing over the set Y.

Lemma 10.2. *For any function* H, $ArMy\ H(x, y, r) \leq |Y| MyAr\ H(x, y, r)$.

This quantifier swap will be the basis for simulating the MA... protocol by an AM... protocol. The size of Y will be exponential in the length of x, so we lose a lot of accuracy by switching from MA to AM, but we will show that this loss can be counteracted by amplifying the success probability of the original protocol sufficiently using amplification for Arthur-Merlin games which is essentially a variant of the amplification from Lemma 9.2.

Proof. We can get a crude upper bound on the maximum y by summing over all choices of y:

$$ArMy\ H(x, y, r) \leq Ar\Sigma_{y \in Y}\ H(x, y, r)$$

The averaging quantifier is really just a summation divided by the number of terms in the summation, so it commutes with the sum over y:

$$ArMy\ H(x,y,r) \leq \Sigma_{y\in Y} Ar\ H(x,y,r)$$

Next we upper bound the sum over y by the maximum y times the number of choices of y:

$$ArMy\ H(x,y,r) \leq |Y| MyAr\ H(x,y,r)$$

This gives the desired bound. □

Back to the proof of the main lemma, we started with an MA... protocol, which looks like

$$\exists y \text{Я} r\ V(x,y,r) = 1$$

Our new protocol will start by picking a sequence of random strings, $r_1 \ldots r_m \in R$, where m is polynomial in the length of x. Our new AM protocol will look like

$$\text{Я} r_1 \ldots r_m My\ Majority_{i=1}^{m}(V(x,y,r_i)).$$

Lemma 10.3. *The acceptance probability of the new* AM*... majority protocol is*

$$1 - 2^m(1-\Psi(x))^{m/2} \leq A(r_1 \ldots r_m) My\ Majority_i(V(x,y,r_i)) \leq 2^m |Y| \Psi(x)^{m/2}$$

Proof. We will prove the lower bound first. For the protocol to reject, at least half of the r_is must lead to a rejection. This give us

$$\exists I \subseteq \{1 \ldots m\},\ |I| = \lceil m/2 \rceil \text{ such that } V(x,y,r_i) \text{ rejects for all } i \in I.$$

In the new AM protocol Merlin could send the same string as in the MA protocol irrespective of the random string r_i. This would give the same success probability $\Psi(x)$, which we will use as a lower bound for the success of one invocation of $V(x,y,r_i)$. Then we have

$$\begin{aligned} \Pr[\text{all trials in } I \text{ fail}] &\leq (1-\Psi(x))^{|I|} \\ &= (1-\Psi(x))^{m/2} \end{aligned}$$

We can upper bound the number of choices of I by 2^m, so

$$\text{total failure probability } \leq 2^m(1-\Psi(x))^{m/2}$$

This gives the lower bound on success claimed in the lemma.

For the upper bound we use the same definition of I, but want all trials in I to accept. This happens with probability:

$$\begin{aligned} \Pr[\forall i \in I.\, V(x,y,r) = 1] &= \Pi_{i\in I} \Pr[V(x,y,r) = 1] \\ &= \Pi_{i\in I} H(x,y,r) \end{aligned}$$

For any fixed y, we can average over the choices of $r_1 \dots r_m$:

$$\begin{aligned} A(r_1 \dots r_m)\ Majority_i(V(x,y,r_i)) &\leq \frac{\Sigma_{r_1 \dots r_m \in R^m} \Sigma_{I \subseteq 1 \dots m, |I| = \lceil m/2 \rceil} \Pi_{i \in I} H(x,y,r_i)}{|R|^m} \\ &\leq \Sigma_I \frac{\Sigma_{r_1 \dots r_m \in R^m} \Pi_{i \in I} H(x,y,r_i)}{|R|^m} \end{aligned}$$

We can replace the average over elements of R^m with an average over elements of R^I since only indices from I affect the probability, so:

$$\begin{aligned} A(r_1 \dots r_m) Majority_i(V(x,y,r_i)) &\leq \Sigma_I \frac{\Sigma_{\vec{r} \in R^I} \Pi_{i \in I} H(x,y,r_i)}{|R|^{|I|}} \\ &= \Sigma_I \Pi_{i \in I} \left(\Sigma_{r_i \in R} \frac{H(x,y,r_i)}{|R|} \right) \\ &= \Sigma_I \left(Ar\ H(x,y,r) \right)^{m/2} \end{aligned}$$

Now replace the arbitrary y with the best possible y:

$$\begin{aligned} MyA(r_1 \dots r_m)\ Majority_i(V(x,y,r_i)) &\leq \Sigma_I \left(MyArH(x,y,r) \right)^{m/2} \\ &= \Sigma_I (\Psi(x))^{m/2} \\ &\leq 2^m \Psi(x)^{m/2} \end{aligned}$$

Combining this with lemma 10.3 we get

$$A(r_1 \dots r_m) My\ Majority_i(V(x,y,r_i)) \leq 2^m |Y| \Psi(x)^{m/2}$$

□

Now that we have established the bounds we will set the value of the parameters. Let $m = 2 \log_2 |Y| + 4$. Assume without loss of generality that for $x \notin L$, $\Psi(x) \leq 1/8$ and for $x \in L$, $\Psi(x) \geq 7/8$. Then the probability of the new AM protocol accepting an $x \notin L$ is at most:

$$\begin{aligned} A(r_1 \dots r_m) My\ Majority_i(V(x,y,r_i)) &\leq 2^m |Y| \Psi(x)^{m/2} \\ &\leq 2^m 2^{-3m/2} |Y| \\ &= 2^{-\log_2 |Y| - 2} |Y| \\ &= \frac{1}{4} \end{aligned}$$

The probability of accepting an $x \in L$ is at least:

$$\begin{aligned} A(r_1 \dots r_m) My\ Majority_i(V(x,y,r_i)) &\geq 1 - 2^m(1-\Psi(x))^{m/2} \\ &\geq 1 - 2^m(\frac{1}{8})^{m/2} \\ &= 1 - 2^{-m/2} \\ &= 1 - 2^{-\log_2 |Y| - 2} \\ &= 1 - \frac{1}{4|Y|} \\ &\geq \frac{3}{4} \end{aligned}$$

This concludes the proof. □

10.2 Variable-round games

The proof in the last section allows any constant number of Arthur-Merlin rounds to be reduced to a single AM round. This can't be extended directly to variable round protocols because there is a polynomial blowup in each switch, which would lead to an exponential blowup in variable round protocols. The following lemma allows for variable round reductions. We will only outline the idea of the proof.

Lemma 10.4 (Babai-Moran). $\mathsf{AM}[2t(n)] \subseteq \mathsf{AM}[t(n)+1]$.

Proof Sketch. The main idea is to convert a single MAM round to an AMA round. As before, Arthur will start by sending a collection of random seeds $r_1 \dots r_m$. After Merlin gives a response $y_1 \dots y_m$ as well as $z_1, dotscz_m$, Merlin's responses for the third round of the game given the correspond choices of y_i and r_i. Arthur sends a random $i \in \{1 \dots m\}$. The protocol the proceeds as if the original game had been played with the sequence y_i, r_i, z_i had been the only interaction so far. This leaves no blowup in the number of games that must be continued (although there is a polynomial blow-up for this triple of rounds). This allows all the MAM seqeunces to be replaced by AMA sequences in parallel with a single polynomial size blow-up. The general idea is that if the overwhelming majority of continuations don't allow Merlin to cheat too much then Arthur will likely pick one on which he won't be fooled. □

10.3 AM games and the Polytime Hierarchy

We can now relate Arthur-Merlin games and the polynomial time hierarchy.

Lemma 10.5. $\mathsf{AM} \subseteq \Pi_2\mathsf{P}$

Proof. The proof is a direct analogue of the Sipser-Gacs-Lautemann proof of $\mathsf{BPP} \subseteq \Sigma_2\mathsf{P} \cap \Pi_2\mathsf{P}$ (see Lecture 3 Theorem 3.5). In that proof we defined $S = \{r \mid M(x,r) = 1\}$ to be the set of random strings that lead to acceptance of M on input x. We then gave a $\Sigma_2\mathsf{P}$ algorithm that accepts the input x if and only if the set S is large. Since BPP is closed under complement, by applying the protocol to $\bar{S}$ we obtain a $\Sigma_2\mathsf{P}$ algorithm for $\bar{A}$ and thus a $\Pi_2\mathsf{P}$ algorithm for L. In particular, this $\Pi_2\mathsf{P}$ expression says that $x \in A$ if and only if

$$\forall t_1 \dots t_{p(|x|)} \in \{0,1\}^{p(|x|)} \exists^{p(|x|)} r \text{ for all } j \in \{1, \dots, p(|x|)\}.\ M(x, r \oplus t_j) = 0.$$

(Since there are only $p(|x|)$ values of j the inner portion can be recognized in polynomial time.)

For the current proof we view AM as BP $\cdot$ NP, and the set S associated with a language L defined by an AM protocol with verifier V is $S = \{r \mid \exists y\, V(x, y, r) = 1\}$. The new expression is then

$$\forall t_1 \dots t_{p(|x|)} \in \{0,1\}^{p(|x|)} \exists^{p(|x|)} r \text{ such that for all } j \in \{1, \dots, p(|x|)\},\ \exists y\, V(x, y, r \oplus t_j) = 0,$$

which is equivalent to

$$\forall t_1 \dots t_{p(|x|)} \in \{0,1\}^{p(|x|)} \exists^{p(|x|)} r \exists (y_1, \dots, y_{p(|x|)}) \text{ s.t. for all } j \in \{1, \dots, p(|x|)\},\ V(x, y_j, r \oplus t_j) = 0.$$

This is a Π_2P expression for L. □

Lemma 10.6. MA $\subseteq \Sigma_2$P $\cap\, \Pi_2$P

Proof. We can view MA as N $\cdot$ BPP. We know that BPP has a Σ_2P representation. Adding on another existential quantifier for the Merlin step gives a language that is still in Σ_2P, so MA $\subseteq \Sigma_2$P. We know that MA $\subseteq$ AM, and that AM $\subseteq \Pi_2$P, so MA $\subseteq \Pi_2$P as well. □

10.4 Graph Isomorphism is unlikely to be NP-complete

With the results from today we can easily show that GRAPH-ISOMORPHISM being NP-complete leads to the polynomial time hierarchy collapsing.

Lemma 10.7. *If* coNP $\subseteq$ AM *then* PH $= \Sigma_2$P $\cap\, \Pi_2$P $=$ AM.

Proof. Let $L \in \Sigma_2$P. We will show that under the assumption coNP $\subseteq$ AM we get $L \in$ AM $\subseteq \Pi_2$P, which causes the hierarchy to collapse at the second level. Since $L \in \Sigma_2$P, by Theorem 2.2 we can express L as

$$L = \{x \mid \exists^{p(|x|)} y.\ (x, y) \in L_1\}$$

where $L_1 \in$ coNP$\}$. If coNP $\subseteq$ AM then $L_1 \in$ AM, so $L \in$ MAM by treating the existential quantifier as a Merlin step. But by the collapse lemma from this lecture, MAM $=$ AM $\subseteq \Pi_2$P, and the hierarchy collapses to Σ_2P $=$ AM $= \Pi_2$P. □

Corollary 10.8. *If GRAPH-ISOMORPHISM is* NP*-complete then* PH $= \Sigma_2$P $\cap\, \Pi_2$P $=$ AM.

Proof. If GRAPH-ISOMORPHISM is NP-complete then GRAPH-NONISOMORPHISM is coNP-complete. We know from last lecture that GRAPH-NONISOMORPHISM $\in$ AM, implying that coNP $\subseteq$ AM. From the above lemma this causes the polynomial time hierarchy to collapse as in the conclusion. □