

More on AM
Exposition by William Gasarch

1 The Class Arthur-Merlin

Recall the class AM:

Def 1.1 A set A is in AM if there exists polynomials p , and a poly predicate V such that the following hold, for all x , the following hold. Let x be of length n .

$$\begin{aligned}x \in A &\Rightarrow \Pr_{|r|=p(n)}((\exists^p y)[V(x, y, r) = 1]) \geq \frac{3}{4}. \\x \notin A &\Rightarrow \Pr_{|r|=p(n)}(\exists^p y)[V(x, y, r) = 1] \leq \frac{1}{4}.\end{aligned}$$

Exercise 1

1. Show that if you replace the $\frac{3}{4}$ with $\frac{99}{100}$ and the $\frac{1}{4}$ with $\frac{1}{100}$ in the above definition, you still get AM.
2. Show that if you replace the $\frac{3}{4}$ with $1 - \frac{1}{2^{|x|}}$ and the $\frac{1}{4}$ with $\frac{1}{2^{|x|}}$ in the above definition, you still get AM.

We can also define MA - where Merlin goes first. The intuition is that Merlin first sends y and then Arthur generates $q(n)$ strings $r_1, \dots, r_{q(n)} \in \{0, 1\}^{p(n)}$ and evaluates $V(x, y, r_1), \dots, V(x, y, r_{q(n)})$. If most are true then Arthur accepts. Formally.

Def 1.2 A set A is in MA if there exists polynomials p , and a poly predicate V such that, for all x , the following hold. Let x be of length n .

$$\begin{aligned}x \in A &\Rightarrow (\exists^p y)[\Pr_{|r|=p(n)}[V(x, y, r) = 1] \geq \frac{3}{4}]. \\x \notin A &\Rightarrow (\forall^p y)[\Pr_{|r|=p(n)}[V(x, y, r) = 1] \leq \frac{1}{4}].\end{aligned}$$

We will show the following theorems in this writeup.

- An example of a problem in MA .
- For AM (and MA) the definitions above is equivalent to having 1-sided error, where if $x \in A$ then the prob of $V(x, y, r) = 1$ is 1.
- $MA \subseteq AM$.
- While one could define AMA and MAM etc. they all collapse down to either AM or MA.

2 An Example of a problem in MA

Def 2.1 An *algebraic circuit over mod p* is defined as having n inputs x_1, \dots, x_n (which will be elements of $\{0, \dots, p-1\}$ and also $+$, $-$, \times gates. The gates have fanin-2 and fanout-1. All of the gates compute \pmod{p} . We can define an algebraic circuit computing a function on n variables in the obvious way.

Notation 2.2 If C and C' are algebraic circuits then $C \equiv C'$ means that, for all inputs $x_1, \dots, x_n \in \{0, \dots, p-1\}$. $C(x) = C'(x)$.

Here is a problem that is in MA :

$$SHORTCIRCUIT = \{(C, s) \mid (\exists C')[C' \text{ has } \leq s \text{ gates } C \equiv C']\}.$$

Here is the protocol for it

1. Input(C, s)
2. Merlin sends Arthur a Circuit C' .
3. Arthur first checks that C' has $\leq s$ gates. If it does not he REJECTS. If it does he then picks n elements of $\{0, 1, \dots, p-1\}^n$ at random and plugs them into both C and C' . If they always agree then he ACCEPTS. Else he REJECTS.

We omit a formal analysis. However note that

If $(C, s) \in SHORTCIRCUIT$ then Merlin will just send the correct C' and it Arthur will accept.

If $(C, s) \notin SHORTCIRCUIT$ then whatever Merlin sends will likely not agree all of the random choices Arthur makes. A formal proof will look at the how often $C - C'$ can be zero.

3 1-sided Error

Def 3.1 A set A is in AM_1 if there exists polynomials p , and a poly predicate V such that, for all x , the following hold. Let x be of length n .

$$\begin{aligned} x \in A &\Rightarrow \Pr_{|r|=p(n)}(\exists^p y)[V(x, y, r) = 1] = 1. \\ x \notin A &\Rightarrow \Pr_{|r|=p(n)}(\exists^p y)[V(x, y, r) = 1] \leq \frac{1}{4}. \end{aligned}$$

Clearly $AM \subseteq AM_1$. We will show that $AM_1 \subseteq AM$. First some intuition. Assume $A \in AM$. We will assume the prob of error is $\leq \frac{1}{2^n}$. ($1/n$ would suffice, but $1/4$ would not.) Fix $x \in \{0, 1\}^n$. Let Note that

$$x \in A \Rightarrow |S_x| \geq (1 - \frac{1}{2^n})2^{p(n)} = 2^{p(n)} - 2^{p(n)-n}$$

$$x \notin A \Rightarrow |S_x| \leq \frac{1}{2^n}2^{p(n)} = 2^{p(n)-n}$$

So we can rethink this problem as Merlin is trying to convince Arthur that S_x is large. But he can't use the Random Hash Lemma since that would only work with high probability. We need a lemma

Lemma 3.2 *Let $S \subseteq \{0, 1\}^{p(n)}$.*

1. *If $|S| \geq 2^{p(n)} - 2^{p(n)-n}$ then for all (YES, ALL!!!) $r_1, \dots, r_n \in \{0, 1\}^{p(n)}$*

$$(\bigcap_{i=1}^{p(n)} (r_i \oplus S)) \neq \emptyset.$$

We rewrite this as

$$(\exists r \in \{0, 1\}^{p(n)}) [\bigwedge_{i=1}^{p(n)} r \oplus r_i \in S].$$

2. *If $|S| \leq 2^{p(n)-n}$ then*

$$\Pr_{r_1, \dots, r_n \in \{0, 1\}^{p(n)}} [(\bigcap_{i=1}^{p(n)} (r_i \oplus S)) \neq \emptyset] \leq \frac{1}{2^n}.$$

We rewrite this as

$$\Pr_{r_1, \dots, r_{p(n)} \in \{0, 1\}^{p(n)}} [(\exists r \in \{0, 1\}^{p(n)}) [\bigwedge_{i=1}^{p(n)} r \oplus r_i \in S] \leq \frac{1}{4}.$$

Proof:

a) We want to show that

$$\left(\bigcap_{i=1}^{p(n)} (r_i \oplus S) \right) \neq \emptyset.$$

This is equivalent to

$$\left(\bigcup_{i=1}^{p(n)} (\{0, 1\}^{p(n)} - (r_i \oplus S)) \right) \neq \{0, 1\}^{p(n)}.$$

Since $|S| \geq 2^{p(n)} - 2^{p(n)-n}$ and $|S| = |S \oplus r_i|$ we know $|S \oplus r_i| \geq 2^{p(n)} - 2^{p(n)-n}$, hence $|\{0, 1\}^{p(n)} - (S \oplus r_i)| \leq 2^{p(n)-n}$. Therefore

$$\left| \bigcup_{i=1}^{p(n)} (\{0, 1\}^{p(n)} - r_i \oplus S) \right| \leq p(n) 2^{p(n)-n} < 2^{p(n)}.$$

Hence $(\bigcup_{i=1}^{p(n)} (\{0, 1\}^{p(n)} - (r_i \oplus S)))$ is too small to be $\{0, 1\}^{p(n)}$.

2) Fix $r \in \{0, 1\}^{p(n)}$.

$$\Pr_{r_1 \in \{0, 1\}^{p(n)}} (r \in S \oplus r_1) = |S|/2^{p(n)} \leq \frac{1}{2^n}.$$

Hence

$$\Pr_{r_1, \dots, r_n \in \{0, 1\}^{p(n)}} [r \in \bigcap_{i=1}^{p(n)} S \oplus r_i] \leq \left(\frac{1}{2^n}\right)^{p(n)} = \frac{1}{2^{np(n)}}.$$

Hence

$$\Pr_{r_1, \dots, r_n \in \{0, 1\}^{p(n)}} [(\exists r \in \bigcap_{i=1}^{p(n)} S \oplus r_i)] \leq (2^{p(n)} \frac{1}{2^n})^{p(n)} = \frac{2^{p(n)}}{2^{np(n)}}.$$

This probability is $\frac{1}{2^{np(n)-p(n)}} \leq \frac{1}{4}$.

■

We now put it all together.

Theorem 3.3 $AM = AM_1$.

Proof: Clearly $AM_1 \subseteq AM$. We show that $AM \subseteq AM_1$.

Let $A \in AM$. Let $V \in P$ and p a polynomial be such that

$$x \in A \Rightarrow \Pr_{|r|=p(n)}((\exists^p y)[V(x, y, r) = 1]) \geq 1 - \frac{1}{2^n}.$$

$$x \notin A \Rightarrow \Pr_{|r|=p(n)}(\exists^p y)[V(x, y, r) = 1] \leq \frac{1}{2^n}.$$

We define, for x of length n ,

$$S_x = \{r \in \{0, 1\}^{p(n)} : (\exists^p y)[V(x, y, r) = 1]\}.$$

Here is the AM_1 protocol.

1. Input(x)
2. Arthur sends $r_1, \dots, r_{p(n)} \in \{0, 1\}^{p(n)}$.
3. Merlin sends $r \in \{0, 1\}^{p(n)}$ and $y_1, \dots, y_{p(n)}$ (He wants to send $r \in \bigcap_{i=1}^{p(n)} S_x \oplus r_i$ which means that, for all i , $1 \leq i \leq p(n)$, $r \oplus r_i \in S_x$. To show that $r \oplus r_i \in S_x$ he wants to send y_i such that $V(x, y_i, r \oplus r_i)$.)
4. Arthur tests that for all i , $1 \leq i \leq p(n)$, $V(x, y_i, r \oplus r_i)$. If this holds for all i then Arthur says YES. Otherwise says NO.

We now show that if $x \in A$ then Merlin can respond to ANY $r_1, \dots, r_{p(n)}$ that Arthur sends, and that if $x \notin A$ then Merlin will, with high probability, not be able to respond.

Assume $x \in A$. Then $|S_x| \geq 2^{p(n)} - 2^{p(n)-n}$. By Lemma 3.2.a $\bigcap_{i=1}^{p(n)} r_i \oplus S_x \neq \emptyset$. Hence Merlin can respond with a value or r in the intersection and the evidence that it is.

Assume $x \notin A$. Then $|S_x| \leq \frac{1}{4}$. By Lemma 3.2.b the probability that there is an r in the intersection is $\leq \frac{1}{4}$. One can easily show that there is an r in the intersection iff Merlin can respond. ■

4 $MA \subseteq AM$

Theorem 4.1 $MA \subseteq AM$

Proof:

Assume $A \in MA$. Hence there exists V such that

$$x \in A \Rightarrow (\exists^p y, |y| = q(n)) [\Pr_{|r|=p(n)} [V(x, y, r) = 1]] \geq \frac{3}{4}.$$

$$x \notin A \Rightarrow (\forall^p y, |y| = q(n)) [\Pr_{|r|=p(n)} [V(x, y, r) = 1]] \leq \frac{1}{4}.$$

In the AM protocol Arthur sends n values of r and challenges Merlin to produce one y that works for all of them. Formally, here is the protocol and the analysis.

1. Input(x)
2. Arthur sends Merlin $r_1, \dots, r_n \in \{0, 1\}^{p(n)}$.
3. Merlin sends Arthur y . (If $x \in A$ then Merlin will send the y he would have send originally in the MA protocol.)
4. Arthur evaluates $V(x, y, r_1), V(x, y, r_2), \dots, V(x, y, r_n)$. If the MAJORITY say YES, then accept, else reject.

If $x \in A$ then Merlin sends the y that he would have send in the original MA protocol. We know that this works for $3/4$ of the r 's that Arthur could send. Hence we need to show that if a coin has probability $3/4$ of being HEADS and you flip in n times, the probability that the majority is HEADS is $\geq 3/4$. This can be done by Chebychevs inequality (its on your HW).

If $x \notin A$ then the probability then, for any y , the probability that $V(x, y, r) = 1$ is $\leq 1/4$. Hence we need to show that if coin has probability $1/4$ of being HEADS and you flip it n times, the probability that the majority is HEADS is $\leq 1/4$. This can be done by Chebychevs inequality (its on your HW). ■