Computability and Complexity

Recitation 12, Thursday September 7, 2023

Ari Feiglin

Definition 12.1:

We define the class **MA** (Merlin-Arthur) to consist of all decision problems S where there exists a probabilistic polynomial-time algorithm A and a polynomial p such that

(1) If $x \in S$, then there exists a y whose length is bound by $p(|x|)$ where $\mathbb{P}(M(x,y)=1) \geq \frac{2}{3}$.

(2) If $x \notin S$, then for every y whose length is bound by $p(|x|)$, $\mathbb{P}(M(x,y)=0) \geq \frac{2}{3}$.

Firstly, it is obvious that $\mathbf{BPP} \subseteq \mathbf{MA}$ as if $S \in \mathbf{BPP}$ and M is the probabilistic algorithm which satisfies the condition for S to be in **BPP**, then defining $M'(x,y) = M(x)$ satisfies the condition for S to be in **MA**. And secondly, $\mathbf{NP} \subseteq \mathbf{MA}$ as if $S \in \mathbf{NP}$ and $V(x,y)$ is its polynomial-time verifier, then V satisfies the condition for $S \in \mathbf{MA}$ (for condition (1), the y is taken to be x's witness), as we get that the probabilities are exactly 1.

Exercise 12.2:

(1) We define a class similar to **MA**, $\mathbf{MA}'$, where the probability when $x \in S$ is equal to 1, and when $x \notin S$ the probability is greater than $\frac{1}{2}$.

(2) We define another class similar to **MA**, $\mathbf{MA}''$, where the probability when $x \in S$ is greater than $\frac{1}{2}$, and when $x \notin S$ the probability is equal to 1.

(1) We claim here that $\mathbf{MA}' = \mathbf{NP}$. It is clear that $\mathbf{NP} \subseteq \mathbf{MA}'$ for the same reason that $\mathbf{NP} \subseteq \mathbf{MA}$.

Now if $S \in \mathbf{MA}'$ then there exists a probabilistic algorithm M and polynomial p which satisfy the conditions for S to be in $\mathbf{MA}'$. Let us define $V(x,y,r)$ which takes as input x, a witness y, and a sequence of choices r, and it runs $M(x,y)$ with the sequence of choices r. Now, if $x \in S$ then there exists an r such that for at least half of the sequences of choices, $M(x,y)=1$. So let r be one of these sequences, and so we have that $V(x,y,r)=1$. So we have shown that

$$x \in S \implies \exists y \exists r \colon V(x,y,r) = 1$$

And if $x \notin S$ then for every y, $M(x,y)=0$ (since the probability that this occurs is 1), meaning for any r we have $V(x,y,r)=0$. So we have shown

$$x \in S \implies \exists y \exists r \colon V(x,y,r) = 1$$

(2) Here we claim $\mathbf{MA}'' = \mathbf{MA}$. If $S \in \mathbf{MA}''$ then there exists a probabilistic algorithm M which satisfies the conditions for S to be in $\mathbf{MA}''$. We amplify M by running it twice, and return one if and only if both runs returned one, let us denote this by M'. If $x \in S$ then there exists a y where $M(x,y)=1$ always and so running it twice will always return one, meaning $\mathbb{P}(M'(x,y)=1)=1$. And if $x \notin S$ then for every y, $\mathbb{P}(M'(x,y)=0) = 1 - \mathbb{P}(M'(x,y)=1) = 1 - \mathbb{P}(M(x,y)=1)^2 \geq \frac{3}{4}$, so M' satisfies the conditions for $S \in \mathbf{MA}$.

Now, if $S \in \mathbf{MA}$ suppose M satisfies the conditions for S to be in M:

$$x \in S \implies \exists y \colon \mathbb{P}(M(x,y)=1) \geq \frac{2}{3}, \qquad x \in S \implies \forall y \colon \mathbb{P}(M(x,y)=0) \geq \frac{2}{3}$$

When showing that $\mathbf{BPP} \subseteq \Sigma_2$, that there exists a deterministic algorithm $M'(x,y,r)$ (q is a bound on the runtime and lengths of x,y,r) which returns the correct solution with a probability greater than $1 - \frac{1}{2q}$. We can then define $M^*(x,y,\overline{s},r)$ where $\overline{s} = s_1, \ldots, s_q$ is a sequence of masks of length q and M^* runs $M'(x,y,r \otimes s_i)$ for every $1 \leq i \leq q$ and returns one if and only if M' returns one at least once.

We showed in the proof that

$$x \in S \implies \exists y, \overline{s} \forall r \colon M^*(x,y,\overline{s},r) = 1$$

and

$$x \notin S \implies \forall y, \overline{s} \colon \mathbb{P}(M^*(x,y,\overline{s},r)=0 \mid r \in \{0,1\}^q) \geq \frac{1}{2}$$

So using $y^* = (y, \bar{s})$, this means that M^* satisfies the conditions for S to be in $\mathbf{MA}'$.

Notice that in our proof, the factor of 2 is arbitrary and if we were to define $k(t) = 18\log\big((1-a)^{-1}t^2\big)$ we'd get that the probability that $M^*(x, y, \bar{s}, r) = 0$ is greater than a. So for every $0 < a < 1$ we get that $\mathbf{MA}_a = \mathbf{MA}$ ($\mathbf{MA}_a$ is where the probability that M returns one when $x \in S$ is one, and when $x \notin S$, M returns zero with a probability greater than a).

Definition 12.3:

We define the class $\mathbf{ZPP}_1$, consisting of decision problems S where there exists a probabilistic polynomial-time algorithm M, where

(1) If $x \in S$ then the probability $M(x)$ returns the correct answer is greater than $\frac{1}{2}$.

(2) For every x, $M(x)$ either returns the correct answer or $\perp$.

We also define the class $\mathbf{ZPP}_2$, consisting of decision problems S where there exists a probabilistic algorithm M, which isn't necessarily polynomial-time, such that for every x, $M(x)$ is correct and the expected runtime complexity is polynomial in $|x|$.

Finally we define $\mathbf{ZPP}_3 = \mathbf{RP} \cap \mathsf{co}\mathbf{RP}$.

Exercise 12.4:

Show that the three definitions above are equivalent:

$$\mathbf{ZPP}_1 = \mathbf{ZPP}_2 = \mathbf{ZPP}_3$$

This class is denoted **ZPP** (zero-error probabilistic polynomial time).

We will show that

$$\mathbf{ZPP}_3 \subseteq \mathbf{ZPP}_1 \subseteq \mathbf{ZPP}_2 \subseteq \mathbf{ZPP}_3$$

So we first show that $\mathbf{ZPP}_3 \subseteq \mathbf{ZPP}_1$. If $S \in \mathbf{ZPP}_3$ there exist M_S and M_{S^c} for S and S^c respectively which satisfy the conditions for S adn S^c to be in $\mathbf{RP}$. Let us define

1. **function** $M(x)$
2. **if** $(M_S(x) = 1)$ **return** 1
3. **if** $(M_{S^c}(x) = 1)$ **return** 0
4. **return** $\perp$
5. **end function**

So if $x \in S$ then

$$\mathbb{P}(M'(x) = 1) = \mathbb{P}(M_S(x)) \geq \frac{1}{2}$$

since M_S satisfies the conditions for S to be in $\mathbf{RP}$. If $x \notin S$, then $M_S(x) = 0$ by definition and so

$$\mathbb{P}(M'(x) = 0) = \mathbb{P}(M_{S^c}(x) = 1) \geq \frac{1}{2}$$

Furthermore, $M'(x)$ will either return the correct answer (since M_S and M_{S^c} will only return 1 if their answer is correct). And so $M'(x)$ will return the correct answer with a probability greater than $\frac{1}{2}$ and it always returns the correct answer, meaning $S \in \mathbf{ZPP}_1$.

Now we will show that $\mathbf{ZPP}_1 \subseteq \mathbf{ZPP}_2$. If $S \in \mathbf{ZPP}_1$, it has a polynomial-time probabilistic algorithm M which returns the correct answer with a probability greater than $\frac{1}{2}$, and if it doesn't return $\perp$ then its answer is correct. So we define M' to run $M(x)$ until it gets an answer.

1. **function** $M'(x)$
2. **while** (true)
3. $\alpha \leftarrow M(x)$
4. **if** $(\alpha \neq \perp)$ **return** α
5. **end while**
6. **end function**

$M'(x)$ will always return a correct answer. Let us denote T to be the number of times M' runs until it gives an answer. Since the probability M' returns $\perp$ is bound by $\frac{1}{2}$, T is a geometric random variable whose parameter is bound by $\frac{1}{2}$ and

so its expected value is bound by 2. Since $M(x)$ is polynomial-time, let its runtime complexity be t_M. $M'(x)$ will run M T times, and so its expected runtime is

$$\mathbb{E}[T \cdot t_M] = t_M \cdot \mathbb{E}[T] = 2t_M$$

And since t_M is polynomial, the expected runtime is polynomial, as required.

Now we will show $\mathbf{ZPP}_2 \subseteq \mathbf{ZPP}_3$ So suppose $S \in \mathbf{ZPP}_2$, so there exists a probabilistic algorithm M which always returns a correct answer, and whose expected runtime is polynomial, which we denote t_M. Let us define $M'(x)$ to run $M(x)$ for $2t_M(|x|)$ steps, and if it hasn't returned a value yet, $M'(x)$ will return zero. $M'(x)$ is obviously polynomial, since its runtime is $O(2t_M)$.

If $x \notin S$, then $M'(x)$ will always return zero (since $M(x)$ will not return one). And if $x \in S$ then

$$\mathbb{P}(M'(x) = 1) = 1 - \mathbb{P}(M'(x) = 0) = 1 - \mathbb{P}(M(x) \text{ ran more than } 2t_M(|x|) \text{ steps})$$

Let us denote the number of steps $M(x)$ took to be $T(x)$, then by definition $\mathbb{E}[T(x)] = t_M(x)$. Recall Markov's inequality, for a random variable X and $a > 0$.

$$\mathbb{P}(X > a\,\mathbb{E}[X]) \leq \frac{1}{a}$$

So we have that

$$\mathbb{P}(M'(x) = 1) = 1 - \mathbb{P}(T(x) > 2t_M(x)) \geq 1 - \frac{1}{2} = \frac{1}{2}$$

This means that if $x \in S$, then $M'(x)$ returns the correct answer with a probability greater than $\frac{1}{2}$. And if $x \notin S$, then $M'(x)$ always returns the correct answer. This means that $S \in \mathbf{RP}$.

Now, if instead of returning 0 when $M(x)$ hasn't finished, have $M'(x)$ return 1. By symmetry (since we can view $M(x)$ as acting for S^c), we get that $S^c \in \mathbf{RP}$ and so $S \in \mathbf{RP} \cap \mathsf{co}\mathbf{RP}$. So we have finished.