Computability and Complexity

Lecture 12, Thursday September 7, 2023

Ari Feiglin

Definition 12.1:

Given a probabilistic algorithm $M(x)$ whose time complexity is $t(n)$, we define a deterministic algorithm $M_{\mathsf{off}}(x,r)$ which gets a second input r whose length is $t(|x|)$. $M_{\mathsf{off}}(x,r)$ runs $M(x)$ and it uses r to make the decisions for $M(x)$. For example, for its first decision the simulation of $M(x)$ will use the value of r_1 (or $r[1]$) to determine which choice to make.

M_{off} is called M's **offline algorithm**.

Without loss of generality, we can assume that all choices are binary and so for every x,

$$\mathbb{P}\Big(M_{\mathsf{off}}(x,r) \text{ is correct} \;\Big|\; r \in \{0,1\}^{t(|x|)}\Big) = \mathbb{P}(M(x) \text{ is correct})$$

This is pretty immediate (keep in mind that in the case that $M(x)$ makes fewer than $t(|x|)$ decisions, the remaining bits of r will not affect $M'(x,r)$'s running and thus will not affect the probability). Notice that the run time of $M_{\mathsf{off}}(x,r)$ is also $O(t(n))$.

Theorem 12.2:

$$\mathbf{BPP} \subseteq {}^{\mathbf{P}}\!/_{\mathsf{poly}}$$

Proof:

Let S be a problem in **BPP**, so there exists a probabilistic polynomial-time algorithm M which always has a non-zero probability of being correct. By a previous theorem, we can assume that M's probability of being correct is greater than $1-2^{-p(n)}$ for a polynomial p. Let us take $p(n) = n+1$ (the reasoning for this is that there are 2^n possible inputs, so this works).

So we know that M_{off} also satisfies this probability:

$$\mathbb{P}\Big(M_{\mathsf{off}}(x,r) \text{ is correct} \;\Big|\; r \in \{0,1\}^{t}\Big) \geq 1 - \frac{1}{2^{n+1}}$$

We need to show that there exists a sequence of advice (previously called commands), $\{a_n\}_{n=0}^{\infty}$ such that $M_{\mathsf{off}}(x, a_{|x|}) = 1$ where a_n's length is bound polynomially. We can't just take an r which makes $M_{\mathsf{off}}(x,r)$ correct, as this r may differ for every x, and the advice must be the same for all x of the same length.

We say that a sequence of choices r_n is *accurate* if for every input x of length n, $M_{\mathsf{off}}(x,r_n)$ returns the correct answer. So to define our advice, we just take accurate sequences of choices. Therefore we need to show that for every $n>0$, there exists an accurate sequence of choices. We will do this by showing that the probability a sequence of choices is accurate is non-zero, which necessitates the existence of an accurate sequence of choices. So let r_n be a random (uniformly chosen) sequence of choices of length n, we will compute the probability that it is accurate.

$$\begin{aligned}
\mathbb{P}(r_n \text{ is an accurate sequence of choices}) &= \mathbb{P}(\forall |x| = n\colon M_{\mathsf{off}}(x,r_n) \text{ is correct}) \\
&= 1 - \mathbb{P}(\exists |x| = n\colon M_{\mathsf{off}}(x,r_n) \text{ is incorrect}) \geq 1 - \sum_{|x|=n} \mathbb{P}(M_{\mathsf{off}}(x,r_n) \text{ is incorrect})
\end{aligned}$$

Now, the probability $M_{\mathsf{off}}(x,r_n)$ is incorrect is equal to the probability $M(x)$ is incorrect, which is less than $\frac{1}{2^{n+1}}$ and since there are 2^n strings of length n, we get that this is greater than

$$\geq 1 - 2^n \cdot \frac{1}{2^{n+1}} = 1 - \frac{1}{2} = \frac{1}{2}$$

And so the probability that r_n is accurate is non-zero, meaning there must exist an accurate sequence of choices of length n.

So if we take our sequence of advice to be $\{r_n\}_{n=0}^{\infty}$, then we have that firstly, $|r_n| \leq t(n)$ and so the length of the advice is polynomially bound. And for every x,

$$M_{\mathsf{off}}(x, r_{|x|}) = 1 \iff x \in S$$

since $r_{|x|}$ is accurate. This is precisely the definition of a problem being in ${}^{\mathbf{P}}\!/_{\mathsf{poly}}$, meaning $S \in {}^{\mathbf{P}}\!/_{\mathsf{poly}}$. So we have shown that **BPP** is contained within ${}^{\mathbf{P}}\!/_{\mathsf{poly}}$, as required. ■

Theorem 12.3:

$$\mathbf{BPP} \subseteq \Sigma_2$$

Proof:

Let S be a problem in **BPP**, so there exists a deterministic polynomial-time algorithm M such that

$$\mathbb{P}\Big(M(x,r) \text{ is correct } \Big|\; r \in \{0,1\}^t\Big) \geq \frac{2}{3}$$

where $t(n)$ is the polynomial runtime bound of M (this is the offline equivalent definition of **BPP**).

We showed last lecture that given a probabilistic algorithm M which solves a problem in **BPP**, we can do an amplification of M to get M' which runs M k times and satisfies

$$\mathbb{P}\Big(M'(x,r) \text{ is correct } \Big|\; r \in \{0,1\}^{t(n)\cdot k(n)}\Big) \geq 1 - e^{-k(n)/18}$$

(We are viewing these algorithms as their offline equivalents.) The reason we must choose $r \in \{0,1\}^{t\cdot k}$ is since we are running M k times, so each time we run it we need a new sequence of choices. Each sequence of choices must be of length t, and so in total we need a length of $t \cdot k$. So if we define $k(n) = 18\log(2t^2(n))$, then eventually $t \geq k$ and so we get that

$$\mathbb{P}\Big(M'(x,r) \text{ is correct } \Big|\; r \in \{0,1\}^{18t\log(2t^2(n))}\Big) \geq 1 - e^{-\log(2t^2(n))} = 1 - \frac{1}{2t^2(n)} \geq 1 - \frac{1}{2t(n)k(n)}$$

Let us define $q(n) = t(n)k(n)$, so we have that $M'(x,r)$ is correct with a probability greater than $1 - \frac{1}{2q}$.

So M' utilizes q bits for r and returns a correct answer with a probability greater than $1 - \frac{1}{2q}$. Let us define $M^*(x, r, \overline{s})$ where $\overline{s}$ is a sequence of *masks*: $s_1, \ldots, s_q$ where for every i, $s_i \in \{0,1\}^q$. M^* will run M' q times, and on the ith iteration it will run $M'(x, r \otimes s_i)$ and it returns one if and only if at any point M' returns one. ($\otimes$ means XOR: exclusive-or).

function $M^*(x, r, \overline{s})$
  for (i **from** 1 **to** $q(|x|)$)
    if $(M'(x, r \otimes s_i) = 1)$ **return** 1
  end for
  return 0
end function

So we claim that M^* satisfies the requirements for Σ_2:

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

Let us first show that if $x \notin S$ then for all $\overline{s}$ there exist an r where $M^*(x, r, \overline{s}) = 0$. Let us randomly choose an r, and show that the probability $M^*(x, r, \overline{s}) = 0$ is non-zero. Notice that since r is uniformly chosen, so is $s_i \otimes r$ (since $s_i \otimes r = a$ if and only if $r = s_i \otimes a$, which has uniform probability). Thus

$$\begin{aligned}
&\mathbb{P}(M^*(x, \overline{s}, r) = 0 \mid r \in \{0,1\}^q) = \mathbb{P}(\forall i \colon M'(x, s_i \otimes r) = 0 \mid r \in \{0,1\}^q) \\
&\qquad \geq 1 - \mathbb{P}(\exists i \colon M'(x, s_i \otimes r) = 1 \mid r \in \{0,1\}^q) \geq 1 - \sum_{i=1}^{q} \mathbb{P}(M'(x, s_i \otimes r) = 1 \mid r \in \{0,1\}^q) = 1 - q \cdot \frac{1}{2q} = \frac{1}{2}
\end{aligned}$$

Since the probability that $M'(x, s_i \otimes r) = 1$ when $x \notin S$ is less than $\frac{1}{2q}$ (since as stated before, $s_i \otimes r$ distributes uniformly). So there must exist an r such that $M^*(x, r, \overline{s}) = 1$ for any $\overline{s}$, as required.

Now we will show that if $x \in S$, there exists a sequence of masks $\overline{s}$ where for every sequence of choices r, $M^*(x, r, \overline{s}) = 1$. Again here we will randomly choose a sequence of masks $\overline{s} = s_1, \ldots, s_q$ and show that with a non-zero probability, it satisfies the condition.

$$\begin{aligned}\mathbb{P}(\forall r\colon M^*(x, \overline{s}, r) = 1 \mid s_i \in \{0,1\}^q) &= \mathbb{P}(\forall r \exists i\colon M'(x, r \otimes s_i) = 1 \mid s_i \in \{0,1\}^q) \\ &= 1 - \mathbb{P}(\exists r \forall i\colon M'(x, r \otimes s_i) = 0 \mid s_i \in \{0,1\}^q) \geq 1 - \sum_{r \in \{0,1\}^q} \mathbb{P}(\forall i\colon M'(x, r \otimes s_i) = 0 \mid s_i \in \{0,1\}^q)\end{aligned}$$

Since each s_i is chosen independently, $r \otimes s_i$ is independent and so the events where $M'(x, r \otimes s_i) = 0$ are independent. This means that

$$\mathbb{P}(\forall i\colon M'(x, r \otimes s_i) = 0 \mid s_i \in \{0,1\}^q) = \prod_{i=1}^{q} \mathbb{P}(M'(x, r \otimes s_i) = 0 \mid s_i \in \{0,1\}^q) \geq \frac{1}{(2q)^q}$$

So continuing our computations, we get

$$\mathbb{P}(\forall r\colon M^*(x, \overline{s}, r) = 1 \mid s_i \in \{0,1\}^q) \geq 1 - \sum_{r \in \{0,1\}^q} \frac{1}{(2q)^q} = 1 - 2^q \cdot \frac{1}{(2q)^q} = 1 - \frac{1}{q^q}$$

This is non-zero, meaning that there must exist such a sequence of masks.

So we have shown that

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

meaning that $S \in \Sigma_2$, as required. ■

Since **BPP** is closed under complements, we have that $\mathbf{BPP} = \mathsf{co}\mathbf{BPP} \subseteq \mathsf{co}\Sigma_2 = \Pi_2$. Thus we have shown

Corollary 12.4:

$$\mathbf{BPP} \subseteq \Sigma_2 \cap \Pi_2$$