6.842 Randomness and Computation	February 23, 2022

Homework 1

Yuchong Pan — *MIT ID: 911346847*

1. *Collaborators and sources:* none.

Proof. We construct an approximation scheme $\mathcal{B}$ for f as follows: On input (x, ε, δ), run $\mathcal{A}(x, \varepsilon)$ independently for $k := \lceil 12 \log(1/\delta) \rceil$ times with outputs $y_1, \ldots, y_k$, and output a median of $y_1, \ldots, y_k$.

Let $t_{\mathcal{A}}(x, \varepsilon)$ be the running time of $\mathcal{A}$ on input (x, ε). Then $\mathcal{B}$ runs in $O(k t_{\mathcal{A}}(x, \varepsilon)) = O(\log(1/\delta) t_{\mathcal{A}}(x, \varepsilon))$. Since $\mathcal{A}$ runs in time polynomial in $1/\varepsilon$ and $|x|$, then $\mathcal{B}$ runs in time polynomial in $1/\varepsilon$, $|x|$ and $\log(1/\delta)$.

By the definition of medians, if more than half of $y_1, \ldots, y_k$ fall in $[f(x)/(1+\varepsilon), f(x)(1+\varepsilon)]$, then $\mathcal{B}(x, \varepsilon, \delta) \in [f(x)/(1+\varepsilon), f(x)(1+\varepsilon)]$. Let $X_1, \ldots, X_k \in \{0, 1\}$ be random variables so that $X_i = 1$ with probability $p := \mathbb{P}[\mathcal{A}(x, \varepsilon) \notin [f(x)/(1+\varepsilon), f(x)(1+\varepsilon)]] \leq 1 - 3/4 = 1/4$. Then $\sum_{i=1}^k \mathbb{E}[X_i] = kp \leq k/4$. Therefore,

$$
\begin{aligned}
&\mathbb{P}\left[\mathcal{B}(x, \varepsilon, \delta) \notin \left[\frac{f(x)}{1+\varepsilon}, f(x)(1+\varepsilon)\right]\right] \\
&\leq \mathbb{P}\left[\text{at least half of } y_1, \ldots, y_k \text{ do not fall in } \left[\frac{f(x)}{1+\varepsilon}, f(x)(1+\varepsilon)\right]\right] \\
&= \mathbb{P}\left[\sum_{i=1}^k X_i \geq \frac{k}{2}\right] \\
&= \mathbb{P}\left[\sum_{i=1}^k X_i \geq (1+1) \cdot \frac{k}{4}\right] \\
&\leq e^{-\frac{k/4}{3}} && \text{(Chernoff bound)} \\
&= e^{-\frac{\lceil 12 \log \frac{1}{\delta} \rceil}{12}} \leq e^{-\frac{12 \log \frac{1}{\delta}}{12}} = \delta.
\end{aligned}
$$

Therefore,

$$\mathbb{P}\left[\mathcal{B}(x, \varepsilon, \delta) \in \left[\frac{f(x)}{1+\varepsilon}, f(x)(1+\varepsilon)\right]\right] = 1 - \mathbb{P}\left[\mathcal{B}(x, \varepsilon, \delta) \notin \left[\frac{f(x)}{1+\varepsilon}, f(x)(1+\varepsilon)\right]\right] \geq 1 - \delta.$$

This completes the proof. $\square$

2. *Collaborators and sources:* none.

Proof. Suppose $\binom{m}{t}2^{1-\binom{t}{2}} < 1$. To prove $R(t) > m$, it suffices to show that there exists a 2-edge-coloring of K_m such that for all $S \subset V(K_m)$ of size t, $E(K_m[S])$ is not monochromatic. We randomly color the edges of K_m red or blue, independently and equiprobably. For each $S \subset V(K_m)$ of size t, there are exactly $2^{\binom{t}{2}}$ two-colorings of $E(K_m[S])$, amongst which two are monochromatic colorings (all red and all blue), so

$$\mathbb{P}\left[E\left(K_m[S]\right) \text{ is monochromatic}\right] = \frac{2}{2^{\binom{t}{2}}} = 2^{1-\binom{t}{2}}.$$

By the union bound,

$$\begin{aligned}
&\mathbb{P}\left[\exists S \subset V\left(K_m\right), |S| = t, E\left(K_m[S]\right) \text{ is monochromatic}\right] \\
\leq &\sum_{\substack{S \subset V(K_m) \\ |S|=t}} \mathbb{P}\left[E\left(K_m[S]\right) \text{ is monochromatic}\right] \\
= &\binom{m}{t} 2^{1-\binom{t}{2}} \\
< &1.
\end{aligned}$$

Therefore,

$$\begin{aligned}
&\mathbb{P}\left[\forall S \subset V\left(K_m\right) \text{of size } t, E\left(K_m[S]\right) \text{ is not monochromatic}\right] \\
= &1 - \mathbb{P}\left[\exists S \subset V\left(K_m\right), |S| = t, E\left(K_m[S]\right) \text{ is monochromatic}\right] \\
> &1 - 1 = 0.
\end{aligned}$$

This proves that there exists a 2-edge-coloring of K_m such that for all $S \subset V(K_m)$ of size t, $E(K_m[S])$ is not monochromatic. The proof is complete. $\square$

3. *Proof.* Suppose that a Boolean function f can be computed by a randomized polynomial-sized circuit family $\mathcal{C} = \{C_n\}_{n\in\mathbb{N}}$. Let $n \in \mathbb{N}$. Let $m \in \mathbb{N}$ be the number of random input bits. Define a $2^n \times 2^m$ matrix M such that

   - each row represents a possible combination of inputs $x_1, \ldots, x_n \in \{0, 1\}$;
   - each column represents a possible combination of random input bits $r_1, \ldots, r_m \in \{0, 1\}$;
   - the entry at the row representing $x_1, \ldots, x_n$ and at the column representing $r_1, \ldots, r_m$ equals the value of C_n on inputs $x_1, \ldots, x_n$ with random input bits $r_1, \ldots, r_m$.

   By the definition of polynomial-sized circuit families, each row has at least half of the entries equal to 1, so the total number of 1-entries is at least $2^n \cdot 2^m/2 = 2^{n+m-1}$. Therefore, there exists a column, representing $r_1^*, \ldots, r_m^*$, with at least half of the entries equal to 1; otherwise every column has fewer than half of the entries equal to 1, so the total number of 1-entries is less than $2^m \cdot 2^n/2 = 2^{n+m-1}$, a contradiction.

   Construct a deterministic circuit $D_n^{(1)}$ by hard-wiring random input bits $r_1 = r_1^*, \ldots, r_m = r_m^*$. Remove the column representing $r_1^*, \ldots, r_m^*$ and each row representing $x_1, \ldots, x_n$ such that the corresponding entry equals 1, resulting in a new matrix M'. Note that this removes at least half of the rows. We claim that each row of M' has at least half of the entries equal to 1; to see this, we note that the number of columns is decreased by 1, and that the number of 1-entries in each remaining row remains the same. Therefore, we apply the same argument and recurse, until every remaining row is all-zero, obtaining circuits $D_n^{(1)}, \ldots, D_n^{(k)}$. Finally, construct a deterministic circuit D_n by taking the "or" of $D_n^{(1)}, \ldots, D_n^{(k)}$.

   Since we remove at least half of the rows in each iteration, then there are at most $O(\log 2^n) = O(n)$ iterations, i.e., $k = O(n)$. Since C_n is polynomial-sized, then the size of C_n is upper bounded by $p(n)$. For each $i \in [k]$, since $D_n^{(i)}$ is obtained by hard-wiring random input bits in C_n, then the size of $D_n^{(i)}$ is upper bounded by $p(n)$. Finally, since D_n is obtained by taking the "or" of $D_n^{(1)}, \ldots, D_n^{(k)}$, then the size of D is upper bounded by $kp(n) + k = O(np(n))$, so D_n is polynomial-sized.

   Let $\mathcal{D} = \{D_n\}_{n\in\mathbb{N}}$. We show that $\mathcal{D}$ computes f. Let $x_1, \ldots, x_n \in \{0, 1\}$. If $f(x_1, \ldots, x_n) = 0$, then the row of the original matrix M representing $x_1, \ldots, x_n$ is all-zero and hence never removed, so none of $D_n^{(1)}, D_n^{(2)}, \ldots$ outputs 0 on inputs $x_1, \ldots, x_n$, which implies that D_n outputs 0. If $f(x_1, \ldots, x_n) = 1$, then the row of the original matrix M representing $x_1, \ldots, x_n$ has at least half of the entries equal to 1, and is hence removed in some iteration, say the i^{th} iteration, so $D_n^{(i)}$ outputs 1 on inputs $x_1, \ldots, x_n$, which implies that D_n outputs 1. This shows that D_n outputs $f(x_1, \ldots, x_n)$ for all combinations of inputs $x_1, \ldots, x_n \in \{0, 1\}$. Therefore, $\mathcal{D}$ is a deterministic polynomial-sized circuit family which computes f, completing the proof. □