**6.842 Randomness and Computation** April 4, 2022

# Homework 3

*Yuchong Pan* *MIT ID: 911346847*

1. *Collaborators and sources:* Guanghao Ye.

*Proof.* Let $\mathbf{x}^* = \langle x_1^*, \ldots, x_n^* \rangle$ be a satisfying assignment, and let $\mathbf{x} = \langle x_1, \ldots, x_n \rangle$ be the assignment in the algorithm. We denote by $d(\mathbf{x}^*, \mathbf{x})$ the number of locations at which $\mathbf{x}^*$ and $\mathbf{x}$ differ for any assignment $\mathbf{x}$. Consider an iteration of the algorithm that picks an unsatisfied clause $C_k$ involving variables $X_{k_1}$ and $X_{k_2}$. We say that a variable $X_{k_i}$ is *tight* for clause $C_k$ if its corresponding literal in $C_k$ evaluates to *true*; otherwise we say that it is *slack* for $C_k$. Then $X_{k_1}$ and $X_{k_2}$ cannot be both slack with respect to $\mathbf{x}^*$, and $X_{k_1}$ and $X_{k_2}$ must be both slack before the modification in the iteration. Table 1 indicates the change of $d(\mathbf{x}^*, \mathbf{x})$ for each combination of the tightnesses/slacknesses of $X_{k_1}$ and $X_{k_2}$ with respect to $\mathbf{x}^*$ and $\mathbf{x}$, respectively.

| $(X_{k_1}, X_{k_2})$ | (slack, tight) | (tight, slack) | (tight, tight) |
|---|---|---|---|
| (slack, tight) | $1 \to 0$ | $1 \to 2$ | $2 \to 1$ |
| (tight, slack) | $1 \to 2$ | $1 \to 0$ | $2 \to 1$ |

Table 1: Indicating the change of $d(\mathbf{x}^*, \mathbf{x})$ for each combination of the tightnesses/slacknesses of $X_{k_1}$ and $X_{k_2}$ with respect to $\mathbf{x}^*$ and $\mathbf{x}$, respectively, where rows correspond to combinations with respect to $\mathbf{x}$ after the modification in the iteration, columns correspond to combinations with respect to $\mathbf{x}^*$, and each entry indicates the change of $d(\mathbf{x}^*, \mathbf{x})$ for $X_{k_1}$ and $X_{k_2}$.

Since the algorithm complements one of the two literals uniformly at random, then Table 1 implies that $d(\mathbf{x}^*, \mathbf{x})$ decreases by 1 with probability $p_- \geq 1/2$, and increases by 1 with probability at most $p_+ \leq 1/2$, such that $p_- + p_+ = 1$.

Let $G = (V, E)$ be a path graph with $V = \{0, \ldots, n\}$ and $E = \{(i-1, i) : i \in [n]\}$, where vertex $i$ corresponds to the value of $d(\mathbf{x}^*, \mathbf{x})$ in the algorithm. Let $d_0$ be the value of $d(\mathbf{x}^*, \mathbf{x})$ at the beginning of the algorithm. Consider the following stochastic process: Start at vertex $d_0$; in each iteration, move to the left or to the right according to the change of $d(\mathbf{x}^*, \mathbf{x})$ in the iteration. For all $i, j \in V$, let $h(i, j)$ be the expected time needed to reach $j$ (for the first time) from $i$. Then $h(n, n-1) = 1$. For each $i \in [n-1]$,

$$\begin{aligned} h(i, i-1) &= \mathbb{P}[i \to i-1] \cdot 1 + \mathbb{P}[i \to i+1] \cdot (1 + h(i+1, i-1)) \\ &\leq \frac{1}{2} \cdot 1 + \frac{1}{2} (1 + h(i+1, i-1)) \qquad (1) \\ &\leq 1 + \frac{1}{2} (h(i+1, i) + h(i, i-1)). \end{aligned}$$

Note that (1) follows from the facts that $h(i+1, i-1) \geq 0$, that $\mathbb{P}[i \to i-1] \geq 1/2$ and that $\mathbb{P}[i \to i+1] \leq 1/2$. Therefore, $h(i, i-1) \leq h(i+1, i) + 2$ for each $i \in [n-1]$. Solving this recurrence relation gives $h(i, i-1) \leq 2(n-i) + 1$ for each $i \in [n]$. It follows that

$$h(d_0, 0) \leq \sum_{i=1}^{d_0} h(i, i-1) \leq \sum_{i=1}^{n} h(i, i-1) \leq \sum_{i=1}^{n} (2(n-i) + 1) = \frac{((2n-1) + 1) \cdot n}{2} = n^2.$$

Let $Z$ be the minimum value of $s$ needed for a specific execution of the algorithm to output a satisfying assignment. Then $\mathbb{E}[Z] = h(d_0, 0) \leq n^2$. By Markov's inequality,

$$\mathbb{P}\left[Z \geq 4n^2\right] \leq \frac{\mathbb{E}[Z]}{4n^2} \leq \frac{n^2}{4n^2} = \frac{1}{4}.$$

Therefore, if $s = 4n^2$, then the algorithm will output a satisfying assignment with probability at least $3/4$. This completes the proof. $\square$

2. (a) *Collaborators and sources:* Guanghao Ye.

*Proof.* Let $\{x, y\} \subset A$ be such that $x \neq y$. Then for a uniformly chosen pairwise independent hash function $h \in H$,

$$(h(x), h(y)) \in_U T^2.$$

Therefore,

$$\mathop{\mathbb{P}}_{h \in_U H}[h(x) = h(y)] = \sum_{z \in T} \mathop{\mathbb{P}}_{h \in_U H}[(h(x), h(y)) = (z, z)] = |T| \cdot \frac{1}{|T^2|} = t \cdot \frac{1}{t^2} = \frac{1}{t}. \tag{2}$$

It follows that

$$\begin{aligned}
\mathop{\mathbb{E}}_{h \in_U H}[\#\text{ colliding pairs for } h] &= \mathop{\mathbb{E}}_{h \in_U H}\left[\sum_{\substack{\{x,y\} \subset A \\ x \neq y}} \mathbb{1}_{\{x,y\} \text{ is a colliding pair for } h}\right] \\
&= \sum_{\substack{\{x,y\} \subset A \\ x \neq y}} \mathop{\mathbb{E}}_{h \in_U H}\left[\mathbb{1}_{\{x,y\} \text{ is a colliding pair for } h}\right] \\
&= \sum_{\substack{\{x,y\} \subset A \\ x \neq y}} \mathop{\mathbb{P}}_{h \in_U H}\left[\{x,y\} \text{ is a colliding pair for } h\right] \\
&= \sum_{\substack{\{x,y\} \subset A \\ x \neq y}} \mathop{\mathbb{P}}_{h \in_U H}[h(x) = h(y)] \\
&= |\{\{x, y\} \subset A : x \neq y\}| \cdot \frac{1}{t} \\
&= \binom{|A|}{2} \cdot \frac{1}{t} \\
&= \binom{n}{2} \cdot \frac{1}{t}.
\end{aligned}$$

This completes the proof. □

(b) *Collaborators and sources:* Guanghao Ye.

*Proof.* Let $p = (p_i)_{i \in A}$ be a distribution over $A$ such that $c(p) \le (1+\varepsilon^2)/|A|$ for some $\varepsilon > 0$. Then $\sum_{i \in A} p_i = 1$ and $\sum_{i \in A} p_i^2 \le (1+\varepsilon^2)/|A|$. Therefore,

$$
\begin{aligned}
\|p - U_A\|_1 &\le \sqrt{|A|}\,\|p - U_A\|_2 && \text{(Cauchy-Schwarz inequality)} \\
&= \sqrt{|A|}\sqrt{\sum_{i \in A}\left(p_i - \frac{1}{|A|}\right)^2} \\
&= \sqrt{|A|}\sqrt{\sum_{i \in A}\left(p_i^2 - \frac{2p_i}{|A|} + \frac{1}{|A|^2}\right)} \\
&= \sqrt{|A|}\sqrt{\sum_{i \in A} p_i^2 - \frac{2}{|A|}\sum_{i \in A} p_i + \sum_{i \in A}\frac{1}{|A|^2}} \\
&\le \sqrt{|A|}\sqrt{\frac{1+\varepsilon^2}{|A|} - \frac{2}{|A|}\cdot 1 + |A| \cdot \frac{1}{|A|^2}} \\
&= \sqrt{|A|}\sqrt{\frac{1+\varepsilon^2}{|A|} - \frac{2}{|A|} + \frac{1}{|A|}} \\
&= \sqrt{|A| \cdot \frac{1+\varepsilon^2 - 2 + 1}{|A|}} \\
&= \sqrt{\varepsilon^2} \\
&= \varepsilon.
\end{aligned}
$$

This completes the proof. □

(c) *Collaborators and sources:* Guanghao Ye.

*Proof.* Let $q$ be a distribution over $B \times T$ defined as in the problem. Let $x, y \in A$. If $x = y$, then $h(x) = h(y)$ for any $h \in H$. If $x \neq y$, then (2) implies that for $h$ uniformly chosen from $H$,

$$\mathop{\mathbb{P}}_{x,y \in_U W}[h(x) = h(y) \mid x \neq y] = \frac{1}{t} = \frac{1}{|T|}.$$

For any set $\Omega$,

$$\begin{aligned}
\mathop{\mathbb{P}}_{\omega_1,\omega_2 \in_U \Omega}[\omega_1 = \omega_2] &= \sum_{\omega \in \Omega} \mathop{\mathbb{P}}_{\omega_1,\omega_2 \in_U \Omega}[\omega_1 = \omega_2 = \omega] \\
&= \sum_{\omega \in \Omega} \mathop{\mathbb{P}}_{\omega_1 \in_U \Omega}[\omega_1 = \omega] \mathop{\mathbb{P}}_{\omega_2 \in_U \Omega}[\omega_2 = \omega] && \text{(independence)} \\
&= |\Omega| \cdot \frac{1}{|\Omega|} \cdot \frac{1}{|\Omega|} \\
&= \frac{1}{|\Omega|}.
\end{aligned}$$

This implies that $\mathbb{P}_{h_1,h_2 \in_U H}[h_1 = h_2] = 1/|H|$ and that $\mathbb{P}_{x_1,x_2 \in_U W}[x_1 = x_2] = 1/|W|$. Fix $h \in H$. Then

$$\begin{aligned}
\mathop{\mathbb{P}}_{x_1,x_2 \in_U W}[h(x_1) = h(x_2)] &= \mathop{\mathbb{P}}_{x_1,x_2 \in_U W}[x_1 = x_2] \mathop{\mathbb{P}}_{x_1,x_2 \in_U W}[h(x_1) = h(x_2) \mid x_1 = x_2] + \\
&\quad \mathop{\mathbb{P}}_{x_1,x_2 \in_U W}[x_1 \neq x_2] \mathop{\mathbb{P}}_{x_1,x_2 \in_U W}[h(x_1) = h(x_2) \mid x_1 \neq x_2] \\
&\leq \frac{1}{|W|} \cdot 1 + 1 \cdot \frac{1}{|T|} \\
&= \frac{1}{|W|} + \frac{1}{|T|}.
\end{aligned}$$

Therefore,

$$\begin{aligned}
c(q) &= \mathop{\mathbb{P}}_{\langle h_1,y_1\rangle,\langle h_2,y_2\rangle \in_q H \times T}[\langle h_1, y_1\rangle = \langle h_2, y_2\rangle] \\
&= \mathop{\mathbb{P}}_{\substack{h_1,h_2 \in_U H \\ x_1,x_2 \in_U W}}[h_1 = h_2, h_1(x_1) = h_2(x_2)] \\
&= \mathop{\mathbb{P}}_{h_1,h_2 \in_U H}[h_1 = h_2] \mathop{\mathbb{P}}_{\substack{h_1,h_2 \in_U H \\ x_1,x_2 \in_U W}}[h_1(x_1) = h_2(x_2) \mid h_1 = h_2] && \text{(independence)} \\
&= \frac{1}{|H|} \mathop{\mathbb{P}}_{\substack{h \in H \\ x_1,x_2 \in_U W}}[h(x_1) = h(x_2) \mid h] \\
&\leq \frac{1}{|B|}\left(\frac{1}{|W|} + \frac{1}{|T|}\right) \\
&= \frac{1}{|B|} \cdot \frac{|T|/|W| + 1}{|T|} \\
&= \frac{1 + |T|/|W|}{|B| \cdot |T|} \\
&= \frac{1 + |T|/|W|}{|B \times T|}.
\end{aligned}$$

This completes the proof. $\square$

(d) *Collaborators and sources:* Guanghao Ye.

*Proof.* Note that it follows from the same argument of part (b) that for any distribution $\mu$ over any finite set $\Omega$, if $c(\mu) \leq (1+\varepsilon^2)/|\Omega|$ for some $\varepsilon > 0$, then $\|\mu - U_\Omega\|_1 \leq \varepsilon$. Let $\Omega = B \times T$. Let $\varepsilon = \sqrt{|T|/|W|} > 0$. Then $|T|/|W| = \varepsilon^2$. By part (c),

$$c(q) \leq \frac{1+|T|/|W|}{|B \times T|} = \frac{1+\varepsilon^2}{|\Omega|}.$$

Since $q$ is a distribution over $B \times T = \Omega$, then

$$\|q - U_{B\times T}\|_1 = \|q - U_\Omega\|_1 \leq \varepsilon = \sqrt{|T|/|W|}.$$

This completes the proof. $\square$

3. *Collaborators and sources:* Guanghao Ye.

*Proof.* Let $A$ be a randomized one-sided error polynomial time algorithm which unique-solves $\Pi$ such that for any Boolean circuit $C$ which takes an $r$-bit input, any polynomial time computable function $h : \{0,1\}^r \to \{0,1\}^{k+2}$ and any $\alpha \in \{0,1\}^{k+2}$,

$$\begin{aligned} &\mathbb{P}[A \text{ accepts } (C,h,\alpha)] \geq 1/2, && \text{if } (C,h,\alpha) \text{ has exactly one satisfying assignment,} \\ &\mathbb{P}[A \text{ rejects } (C,h,\alpha)] = 1, && \text{if } (C,h,\alpha) \text{ has no satisfying assignment.} \end{aligned}$$

For each $k \in [r]$, let $B_k$ be an algorithm presented in Algorithm 1 that, given a Boolean circuit $C$ which takes an $r$-bit input, decides the membership in CIRCUIT-SAT of $C$ using oracle calls to $A$, assuming that the number $N$ of satisfying assignments to $C$ has either $N = 0$ or $2^{k-1} \leq N \leq 2^k$. since $A$ runs in polynomial time, since we can uniformly choose $\alpha \in \{0,1\}^{k+2}$ in $O(\log 2^{k+2}) = O(k) = O(r)$ time and since we can uniformly choose a pairwise independent hash function in $O(\log(2^r \cdot 2^{k+2})) = O(r+k) = O(r)$ time, then $B_k$ runs in polynomial time for each $k \in [r]$.

uniformly choose a pairwise independent hash function $h : \{0,1\}^r \to \{0,1\}^{k+2}$
uniformly choose $\alpha \in \{0,1\}^{k+2}$
call $A$ with input $(C,h,\alpha)$
**return** *the same output as* $A$

**Algorithm 1:** An algorithm that, given a Boolean circuit $C$ which takes an $r$-bit input, decides the membership in CIRCUIT-SAT of $C$ using oracle calls to $A$, assuming that the number $N$ of satisfying assignments to $C$ has either $N = 0$ or $2^{k-1} \leq N \leq 2^k$.

Let $X$ be the number of colliding pairs of satisfying assignments for $h$, as defined in Problem 2 part (a). By the same argument for Problem 2 part (a),

$$\mathbb{E}[X] = \frac{1}{2^{k+2}}\binom{N}{2} = \frac{1}{2^{k+2}} \cdot \frac{N(N-1)}{2} < \frac{1}{2^{k+2}} \cdot \frac{2^k N}{2} = \frac{N}{8}.$$

By Markov's inequality,

$$\mathbb{P}\left[X \geq \frac{N}{4}\right] \leq \frac{\mathbb{E}[X]}{N/4} < \frac{N/8}{N/4} = \frac{1}{2}.$$

Therefore, $\mathbb{P}[X < N/4] = 1 - \mathbb{P}[X \geq N/4] > 1 - 1/2 = 1/2$. This implies that, with probability greater than $1/2$, fewer than $N/2$ satisfying assignments to $C$ are involved in some colliding pair for $h$. Hence, with probability greater than $1/2$, at least $N/2$ satisfying assignments to $C$ are not involved in any colliding pair for $h$. Conditioned on this event, the probability that there exists a unique satisfying assignment mapping to $\alpha$ is at least

$$\frac{N/2}{2^{k+2}} \geq \frac{2^{k-1}/2}{2^{k+2}} = \frac{1}{16}.$$

Since the event that at least $N/2$ satisfying assignments to $C$ are not involved in any colliding pair for $h$ and the event that there exists a unique satisfying assignment mapping to $\alpha$ are independent, then the unconditional probability that there exists a unique satisfying assignment mapping to $\alpha$ is greater than $(1/2) \cdot (1/16) = 1/32$. On the other hand, if $C$ is not satisfiable, then $A$ always rejects $(C,h,\alpha)$ for any pairwise independent hash function

$h : \{0,1\}^r \to \{0,1\}^{k+2}$ and any $\alpha \in \{0,1\}^{k+2}$. Therefore, for each $k \in [r]$ and for any Boolean circuit $C$ which takes an $r$-bit input,

$$\begin{aligned} &\mathbb{P}\left[B_k \text{ accepts } C\right] \geq 1/32, && \text{if } C \in \mathsf{CIRCUIT\text{-}SAT}, \\ &\mathbb{P}\left[B_k \text{ rejects } C\right] = 1, && \text{if } C \notin \mathsf{CIRCUIT\text{-}SAT}. \end{aligned}$$

Let $B$ be the algorithm that first uniformly chooses $k \in [r]$, and then executes $B_k$. Since we can uniformly choose $k \in [r]$ in $O(\log r)$ time and since $B_k$ runs in polynomial time for each $k \in [r]$, then $B$ runs in polynomial time. Let $C$ be a Boolean circuit which takes an $r$-bit input. If $C \notin \mathsf{CIRCUIT\text{-}SAT}$, then $B_k$ rejects $C$ with probability 1 for any $k \in [r]$. Now, suppose $C \in \mathsf{CIRCUIT\text{-}SAT}$. Since there exists at least one value of $k \in [r]$ such that either $N = 0$ or $2^{k-1} \leq N \leq 2^k$, then $\mathbb{P}[2^{k-1} \leq N \leq 2^k] \geq 1/r$. By the previous paragraph, $B_k$ rejects $C$ with probability $1/32$ if either $N = 0$ or $2^{k-1} \leq N \leq 2^k$. Since the sampling of $k$ and the randomness of $B_k$ are independent, then $B$ accepts $C$ with probability at least $(1/32) \cdot (1/r) = 1/(32r)$. Hence, for any Boolean circuit $C$ which takes an $r$-bit input,

$$\begin{aligned} &\mathbb{P}[B \text{ accepts } C] \geq 1/(32r), && \text{if } C \in \mathsf{CIRCUIT\text{-}SAT}, \\ &\mathbb{P}[B \text{ rejects } C] = 1, && \text{if } C \notin \mathsf{CIRCUIT\text{-}SAT}. \end{aligned}$$

Let $B'$ be the algorithm that repeatedly executes $B$ for $32r$ times, and outputs "yes" if and only if any execution of $B$ outputs "yes." Since $B$ runs in polynomial time, then so does $B'$. Let $C$ be a Boolean circuit which takes an $r$-bit input. If $C \notin \mathsf{CIRCUIT\text{-}SAT}$, then any execution of $B$ outputs "no," so $B'$ outputs "no" with probability 1. If $C \in \mathsf{CIRCUIT\text{-}SAT}$,

$$\mathbb{P}\left[B' \text{ accepts } C\right] = 1 - \mathbb{P}\left[B' \text{ rejects } C\right] = 1 - \mathbb{P}[B \text{ rejects } C]^{32r} \geq \left(1 - \frac{1}{32r}\right)^{32r} \geq 1 - \frac{1}{e} > \frac{1}{2}.$$

Therefore,

$$\begin{aligned} &\mathbb{P}\left[B' \text{ accepts } C\right] > 1/2, && \text{if } C \in \mathsf{CIRCUIT\text{-}SAT}, \\ &\mathbb{P}\left[B' \text{ rejects } C\right] = 1, && \text{if } C \notin \mathsf{CIRCUIT\text{-}SAT}. \end{aligned}$$

This shows that $B'$ is a randomized one-sided error polynomial time algorithm which solves $\mathsf{CIRCUIT\text{-}SAT}$. Since $\mathsf{CIRCUIT\text{-}SAT}$ is $\mathsf{NP}$-complete, then $\mathsf{RP} = \mathsf{NP}$, completing the proof. $\square$