6.842 Randomness and Computation April 2, 2022

Homework 2

Yuchong Pan *MIT ID: 911346847*

1. *Collaborators and sources:* Guanghao Ye.

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

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

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

Therefore,

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

It follows that

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

This completes the proof. $\square$

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

Proof. Let $p = (p_i)_{i \in A}$ be a distribution over A such that $c(p) \le (1+\varepsilon^2)/|A|$. 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. $\square$