6.842 Randomness and Computation March 7, 2022

Homework 2

Yuchong Pan *MIT ID: 911346847*

1. (a) *Collaborators and sources:* none.

Proof. Recall that the $n = 2^\ell - 1$ pairwise independent random bits are generated by $C_S = \prod_{i \in S} b_i$ for all $S \subset [\ell]$ with $S \neq \emptyset$, from ℓ truly random bits $b_1, \dots, b_\ell \in \{-1, 1\}$. First, we show that $\mathbb{P}[C_S = 1] = \mathbb{P}[C_S = -1] = 1/2$ for all $S \subset [\ell]$ with $S \neq \emptyset$. Let $b \in \{-1, 1\}$. Let $S \subset [\ell]$ be such that $S \neq \emptyset$. Then

$$\begin{aligned}
\mathbb{P}\left[C_S = 1\right] &= \frac{1}{2^{|S|}} \sum_{i=1}^{\left\lceil \frac{|S|}{2} \right\rceil} \binom{|S|}{2i-1} \\
&= \begin{cases} \frac{1}{2^{|S|}} \sum_{i=1}^{|S|/2} \left(\binom{|S|-1}{2i-2} + \binom{|S|-1}{2i-1} \right), & \text{if } |S| \text{ is even}, \\ \frac{1}{2^{|S|}} \left(\sum_{i=1}^{(|S|-1)/2} \left(\binom{|S|-1}{2i-2} + \binom{|S|-1}{2i-1} \right) + \binom{|S|}{|S|} \right), & \text{if } |S| \text{ is odd}, \end{cases} \\
&= \begin{cases} \frac{1}{2^{|S|}} \sum_{i=0}^{|S|-1} \binom{|S|-1}{i}, & \text{if } |S| \text{ is even}, \\ \frac{1}{2^{|S|}} \left(\sum_{i=0}^{|S|-2} \binom{|S|-1}{i} + \binom{|S|-1}{|S|-1} \right), & \text{if } |S| \text{ is odd}, \end{cases} \\
&= \frac{1}{2^{|S|}} \sum_{i=0}^{|S|-1} \binom{|S|-1}{i} = \frac{2^{|S|-1}}{2^{|S|}} = \frac{1}{2}.
\end{aligned}$$

Hence, $\mathbb{P}[C_S = -1] = 1 - \mathbb{P}[C_S = 1] = 1 - 1/2 = 1/2$.
Now, let $S, S' \subset [\ell]$ be such that $S \neq S'$, $S \neq \emptyset$ and $S' \neq \emptyset$. Let $b, b' \in \{-1, 1\}$. Then

$$\begin{aligned}
\mathbb{P}\left[C_S = b, C_{S'} = b'\right] &= \sum_{\beta \in \{-1,1\}} \mathbb{P}\left[C_{S \cap S'} = \beta\right] \mathbb{P}\left[C_S = b, C_{S'} = b' \;\middle|\; C_{S \cap S'} = \beta\right] \\
&= \sum_{\beta \in \{-1,1\}} \mathbb{P}\left[C_{S \cap S'} = \beta\right] \mathbb{P}\left[C_{S \setminus S'} = b\beta, C_{S' \setminus S} = b'\beta\right] \\
&= \sum_{\beta \in \{-1,1\}} \mathbb{P}\left[C_{S \cap S'} = \beta\right] \mathbb{P}\left[C_{S \setminus S'} = b\beta\right] \mathbb{P}\left[C_{S' \setminus S} = b'\beta\right] \qquad (1) \\
&= \sum_{\beta \in \{-1,1\}} \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} = 2 \cdot \frac{1}{8} = \frac{1}{4} = \frac{1}{2} \cdot \frac{1}{2} = \mathbb{P}\left[C_S = b\right] \mathbb{P}\left[C_S = b'\right].
\end{aligned}$$

Note that (1) follows from the fact that $S \setminus S'$ and $S' \setminus S$ are disjoint and thus that $C_{S \setminus S'}$ and $C_{S' \setminus S}$ are independent. This completes the proof that the $n = 2^\ell - 1$ random bits C_S for $S \subset [\ell]$ with $S \neq \emptyset$ are pairwise independent. $\square$

(b) *Collaborators and sources:* none.

For each $i \in [s], j \in [n]$, we denote by $s_{i,j}$ the (i,j)-entry of S. For each $j \in [n]$, we denote by $\mathbf{s}_j$ the j^{th} column of S. The condition of pairwise independence says that for all $j, j' \in [n]$ with $j \neq j'$ and for all $b, b' \in \{-1, 1\}$,

$$\mathop{\mathbb{P}}_{i \in [s]}\left[s_{i,j} = b, s_{i,j'} = b'\right] = \mathop{\mathbb{P}}_{i \in [s]}\left[\mathbf{x}_j^{(i)} = b, \mathbf{x}_{j'}^{(i)} = b'\right] = \frac{1}{4}. \tag{2}$$

We show that S contains at least n vectors.

Proof. WLOG, assume that $n \geq 2$ and that $s \geq 1$. First, we show that $\mathbf{s}_j \cdot \mathbf{s}_{j'} = 0$ for all $j, j' \in [n]$ with $j \neq j'$. Let $j, j' \in [n]$ be such that $j \neq j'$. Since S is a pairwise independent space, then (2) implies that for all $b, b' \in \{-1, 1\}$,

$$\left|\left\{i \in [s] : s_{i,j} = b, s_{i,j'} = b'\right\}\right| = \frac{s}{4}.$$

Therefore,

$$\begin{aligned}
\mathbf{s}_j \cdot \mathbf{s}_{j'} = \sum_{i=1}^{s} s_{i,j} s_{i,j'} &= \left|\left\{i \in [s] : s_{i,j} = s_{i,j'}\right\}\right| - \left|\left\{i \in [s] : s_{i,j} \neq s_{i,j'}\right\}\right| \\
&= \left(\left|\left\{i \in [s] : s_{i,j} = s_{i,j'} = 1\right\}\right| + \left|\left\{i \in [s] : s_{i,j} = s_{i,j'} = -1\right\}\right|\right) - \\
&\quad \left(\left|\left\{i \in [s] : s_{i,j} = 1, s_{i,j'} = -1\right\}\right| + \left|\left\{i \in [s] : s_{i,j} = -1, s_{i,j'} = 1\right\}\right|\right) \\
&= \left(\frac{s}{4} + \frac{s}{4}\right) - \left(\frac{s}{4} + \frac{s}{4}\right) = 0.
\end{aligned}$$

Second, we show that $\mathbf{s}_1, \ldots, \mathbf{s}_n$ are linearly independent. Suppose for the purpose of contradiction that there exist $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$ that are not all zeros such that

$$\sum_{j=1}^{n} \alpha_j \mathbf{s}_j = \mathbf{0}.$$

Let $j' \in [n]$. Since $|\{i \in [s] : s_{i,j} = 1, s_{i,j'} = 1\}| = s/4 > 0$ for all $j \in [n] \setminus \{j'\}$, then $\mathbf{s}_{j'} \neq \mathbf{0}$ and hence $\|\mathbf{s}_{j'}\|^2 > 0$. Therefore,

$$\begin{aligned}
0 = \mathbf{0} \cdot \mathbf{s}_{j'} &= \left(\sum_{j=1}^{n} \alpha_j \mathbf{s}_j\right) \cdot \mathbf{s}_{j'} = \sum_{j=1}^{n} \alpha_j \left(\mathbf{s}_j \cdot \mathbf{s}_{j'}\right) = \sum_{\substack{j=1 \\ j \neq j'}}^{n} \alpha_j \left(\mathbf{s}_j \cdot \mathbf{s}_{j'}\right) + \alpha_{j'} \left(\mathbf{s}_{j'} \cdot \mathbf{s}_{j'}\right) \\
&= \sum_{\substack{j=1 \\ j \neq j'}}^{n} \alpha_j \cdot 0 + \alpha_{j'} \left\|\mathbf{s}_{j'}\right\|^2 = \alpha_{j'} \left\|\mathbf{s}_{j'}\right\|^2.
\end{aligned}$$

This implies that $\alpha_{j'} = 0/\|\mathbf{s}_{j'}\|^2 = 0$ for all $j' \in [n]$, a contradiction. Hence, $\mathbf{s}_1, \ldots, \mathbf{s}_n$ are linearly independent. It follows that

$$s \geq \operatorname{rank} \mathsf{S} = n.$$

This completes the proof. $\square$

(c) *Collaborators and sources:* none.

Proof. Note that any algorithm which generates n pairwise independent random bits samples a vector $\mathbf{x}$ from a pairwise independent space $S = \{\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(s)}\}$ on n variables. By part (b), any pairwise independent space S on n variables has size $|S| \geq n$. Therefore, any algorithm that generates n pairwise independent random bits requires at least $\log n$ truly random bits to sample a vector from a space of size n. This implies that the construction is optimal, completing the proof. $\square$

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

Proof. Let $x \in [n]$. Since w_x is chosen from S uniformly at random, then for all $s \in \mathbb{Z}$,

$$\mathbb{P}\left[w_x = s\right] = \left\{ \begin{array}{ll} 0, & \text{if } s \notin S, \\ \frac{1}{|S|}, & \text{if } s \in S, \end{array} \right\} \leq \frac{1}{|S|}.$$

Therefore,

$$\mathbb{P}[\alpha(x) = w_x] = \mathbb{P}\left[w_x = \min_{\substack{i \in [k] \\ x \notin M_i}} w\left(M_i\right) - \min_{\substack{i \in [k] \\ x \in M_i}} w\left(M_i \setminus \{x\}\right)\right] \leq \frac{1}{|S|}.$$

By the union bound,

$$\mathbb{P}\left[\exists x \in [n] \text{ such that } \alpha(x) = w_x\right] \leq \sum_{x=1}^{n} \mathbb{P}\left[\alpha(x) = w_x\right] \leq n \cdot \frac{1}{|S|} = \frac{n}{|S|}.$$

This completes the proof. $\square$

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

Proof. Suppose that there exist two distinct M_j and M_ℓ with $j, \ell \in [k]$ that have the same minimum weight (compared to all other $w(M_i)$ with $i \in [k]$). Then there exists $x \in M_j \triangle M_\ell$. WLOG, suppose that $x \notin M_j$ and $x \in M_\ell$. Since M_j and M_ℓ have the same minimum weight, then

$$\begin{aligned} w\left(M_j\right) &= w\left(M_\ell\right), \\ \min_{i \in [k], x \notin M_i} w(M_i) &= w(M_j), \\ \min_{i \in [k], x \in M_i} w(M_i) &= w(M_\ell). \end{aligned}$$

Hence,

$$\begin{aligned} \alpha(x) &= \min_{\substack{i \in [k] \\ x \notin M_i}} w\left(M_i\right) - \min_{\substack{i \in [k] \\ x \in M_i}} w\left(M_i \setminus \{x\}\right) = \min_{\substack{i \in [k] \\ x \notin M_i}} w\left(M_i\right) - \min_{\substack{i \in [k] \\ x \in M_i}} \left(w\left(M_i\right) - w_x\right) \\ &= \min_{\substack{i \in [k] \\ x \notin M_i}} w\left(M_i\right) - \min_{\substack{i \in [k] \\ x \in M_i}} w\left(M_i\right) + w_x = w\left(M_j\right) - w\left(M_\ell\right) + w_x = w_x. \end{aligned}$$

This implies that

$$\begin{aligned} &\mathbb{P}\left[\exists \text{a unique } w(M_i) \text{ with } i \in [k] \text{ of minimum weight}\right] \\ &= 1 - \mathbb{P}\left[\exists \text{distinct } M_j, M_\ell \text{ with } j, \ell \in [k] \text{ that have the same minimum weight}\right] \\ &\geq 1 - \mathbb{P}\left[\exists x \in [n] \text{ such that } \alpha(x) = w_x\right] \\ &\geq 1 - \frac{n}{|S|}. \end{aligned} \tag{3}$$

Note that (3) follows from part (a). This completes the proof. □

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

Proof. Let $\mathcal{B}$ be the sequential algorithm given in Algorithm 1 for finding a perfect matching, given a black box algorithm $\mathcal{A}$ that checks whether a given graph contains a perfect matching or not. In other words, $\mathcal{B}$ removes each edge from the graph, checks whether the resulting graph has a perfect matching, and if so, adds this edge to the perfect matching.

if $\mathcal{A}(G) = 0$ **then**
    return *"G does not have a perfect matching"*
$M = \emptyset$
$G' \leftarrow G$
foreach $e = \{u, v\} \in E$ **do**
    $G' \leftarrow (V(G') \setminus \{u, v\}, E(G') \setminus \{e\})$
    if $\mathcal{A}(G') = 1$ **then**
        $M \leftarrow M \cup \{e\}$
return M

Algorithm 1: A sequential algorithm for finding a perfect matching in a graph $G = (V, E)$, given a black box algorithm $\mathcal{A}$ that checks whether a given graph contains a perfect matching.

Since $\mathcal{B}$ makes $m+1$ calls to $\mathcal{A}$, then $\mathcal{B}$ runs in time $O((m+1) \cdot T_{\mathcal{A}}^{seq}(G)) = O(m \cdot T_{\mathcal{A}}^{seq}(G))$. We show that $\mathcal{B}$ is correct. If G does not contain a perfect matching, then $\mathcal{B}$ correctly reports so. Suppose that G contains a perfect matching. If an edge $e \in E$ is in a perfect matching of G, then the graph G' obtained by removing e from G also contains a perfect matching M', and $M' \cup \{e\}$ is a perfect matching of G; otherwise, any perfect matching of G is still contained in G'. This justifies the correctness of $\mathcal{B}$, completing the proof. $\square$