6.842 Randomness and Computation March 6, 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 $b_1, \ldots, b_\ell \in \{-1, 1\}$. 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. □

(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. $\square$