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

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

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. □