

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

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

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

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

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

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

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 $b, b' \in \{-1, 1\}$,

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

Therefore,

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

Second, we show that $\mathbf{s}_1, \dots, \mathbf{s}_n$ are linearly independent. Suppose for the purpose of contradiction that there exist $\alpha_1, \dots, \alpha_n \in \mathbb{R}$ 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,

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

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

$$s \geq \text{rank } \mathbf{S} = n.$$

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 $S = \{\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(s)}\}$ 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:* Guanghai Ye.

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

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

Therefore,

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

By the union bound,

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

This completes the proof. □