

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:* Guanghao Ye.

We show that

- (i) a *necessary* condition of S being a pairwise independent space is that the columns of \mathbf{S} are pairwise orthogonal;
- (ii) a pairwise independent space S contains at least n vectors.

Proof. WLOG, assume that $n \geq 2$ and that $s \geq 1$. 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} .

- (i) Suppose that S is a pairwise independent space. Let $j, j' \in [n]$ be such that $j \neq j'$. Then for all $b, b' \in \{-1, 1\}$,

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

and hence,

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

Therefore,

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

- (ii) We show that $\mathbf{s}_1, \dots, \mathbf{s}_n$ are linearly independent. Suppose that S is a pairwise independent space. Suppose for the sake 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. □

(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. □

(b) *Collaborators and sources:* Guanghai 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

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

Hence,

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

This implies that

$$\begin{aligned} &\mathbb{P}[\exists \text{ a unique } w(M_i) \text{ with } i \in [k] \text{ of minimum weight}] \\ &= 1 - \mathbb{P}[\exists \text{ distinct } M_j, M_\ell \text{ with } j, \ell \in [k] \text{ that have the same minimum weight}] \\ &\geq 1 - \mathbb{P}[\exists x \in [n] \text{ such that } \alpha(x) = w_x] \\ &\geq 1 - \frac{n}{|S|}. \end{aligned} \tag{2}$$

Note that (2) follows from part (a). This completes the proof. \square

3. (a) *Collaborators and sources:* Guanghai 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.

```

1 if  $\mathcal{A}(G) = 0$  then
2   return “ $G$  does not have a perfect matching”
3  $M = \emptyset$ 
4  $G' \leftarrow G$ 
5 foreach  $e = (u, v) \in E$  do
6    $G' \leftarrow (V(G') \setminus \{u, v\}, E(G') \setminus \{e\})$ 
7   if  $\mathcal{A}(G') = 1$  then
8      $M \leftarrow M \cup \{e\}$ 
9 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 and its endpoints from G 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

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

Proof. We claim that, with high probability, Algorithm 2 correctly finds the unique perfect matching in a bipartite graph G that has exactly one perfect matching, given an oracle for determinant computations, such that all calls to the oracle are simultaneous.

```

1  $\mathcal{T} \leftarrow \emptyset$ 
2 pick  $n^4$  random points  $S = \{s_1, \dots, s_{n^4}\}$ 
3 foreach  $e = (u, v) \in E$  do
4    $E' \leftarrow E \setminus \{e\}$ 
5   foreach  $(u', v') \in E'$  do
6     pick  $x_{u', v'} \in S$  uniformly at random
7     let  $A \in \mathbb{R}^{n \times n}$  such that  $\forall u, v \in V$ ,  $A_{u', v'}$  equals  $x_{u', v'}$  if  $(u', v') \in E'$  and 0 otherwise
8      $\mathcal{T} \leftarrow \mathcal{T} \cup \{\text{task to compute } \det A \text{ and save the result to variable } d_e\}$ 
9 run tasks in  $\mathcal{T}$  in parallel, obtaining variables  $d_e$  for  $e \in E$ 
10  $M \leftarrow \{e \in E : d_e = 0\}$ 
11 return  $M$ 

```

Algorithm 2: An algorithm for finding the unique perfect matching in a bipartite graph $G = (V, E)$ that has exactly one perfect matching, given an oracle for determinant computations, such that all calls to the oracle are simultaneous.

Note that if an edge $e \in E$ is contained in the unique perfect matching of G , then the graph G_e obtained by removing e (and keeping its endpoints) from G contains no perfect matching; otherwise, G_e still contains the unique perfect matching. Recall that G_e contains a perfect matching if and only if its (symbolic) Tutte matrix has a determinant that is a non-zero multivariate polynomial. We denote by T_e the (symbolic) Tutte matrix of G_e . This implies that an edge $e \in E$ is contained in the unique perfect matching of G if and only if $\det T_e \equiv 0$. For each $e \in E$ with $\det T_e \equiv 0$, we always have $d_e = 0$ and hence $e \in M$, so $\mathbb{P}[e \notin M] = 0$. Therefore,

$$\mathbb{P}[\text{Algorithm 2 is correct}] = 1 - \mathbb{P}[\exists e \in M, \det T_e \not\equiv 0 \text{ or } \exists e \in E \setminus M, \det T_e \equiv 0]$$

$$\geq 1 - \sum_{\substack{e \in E \\ \det T_e \not\equiv 0}} \mathbb{P}[e \in M] - \sum_{\substack{e \in E \\ \det T_e \equiv 0}} \mathbb{P}[e \notin M] \quad (3)$$

$$\begin{aligned} &= 1 - \sum_{\substack{e \in E \\ \det T_e \not\equiv 0}} \mathbb{P}[d_e = 0] - \sum_{\substack{e \in E \\ \det T_e \equiv 0}} 0 \\ &\geq 1 - \sum_{\substack{e \in E \\ \det T_e \not\equiv 0}} \frac{n}{|S|} \quad (4) \end{aligned}$$

$$\geq 1 - \sum_{e \in E} \frac{n}{n^4} = 1 - m \cdot \frac{1}{n^3} \geq 1 - n^2 \cdot \frac{1}{n^3} = 1 - \frac{1}{n} = 1 - o(1).$$

Note that (3) follows from the union bound, and that (4) follows from the Schwartz-Zippel-DeMill-Lipton theorem and the fact that the determinant of the Tutte matrix of an n -vertex bipartite graph is a multivariate polynomial of total degree at most n . This completes the proof. \square