6.842 Randomness and Computation March 9, 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. $\square$

(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 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 S. For each $j \in [n]$, we denote by $\mathbf{s}_j$ the j^{th} column of S.

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

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

and hence,

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

Therefore,

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

(ii) We show that $\mathbf{s}_1, \ldots, \mathbf{s}_n$ are linearly independent. Suppose that S is a pairwise independent space. Suppose for the sake of contradiction that there exist $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$ 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 $S = \{\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(s)}\}$ 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:* 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. ☐

(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

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

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

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

Proof. Let $\mathcal{B}$ be the sequential algorithm given in Algorithm 1 for finding a perfect matching in a bipartite graph, given a black box algorithm $\mathcal{A}$ that checks whether a given bipartite graph contains a perfect matching or not. In other words, for each edge $e \in E$, $\mathcal{B}$ checks whether the graph G'' obtained by removing e and its endpoints from G has a perfect matching; if so, then $\mathcal{B}$ replaces the current graph with G''; otherwise, $\mathcal{B}$ removes e from the current graph (and keeps its endpoints).

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 $\mathcal{A}(G'') = 0$ **then**
        $M \leftarrow M \cup \{e\}$
        $G' \leftarrow G''$
    else
        $G' \leftarrow (V(G'), E(G') \setminus \{e\})$
return M

Algorithm 1: A sequential algorithm for finding a perfect matching in a bipartite graph $G = (V, E)$, given a black box algorithm $\mathcal{A}$ that checks whether a given bipartite 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' such that $M' \cup \{e\}$ is a perfect matching of G; otherwise, any perfect matching of G still exists if we remove e (and keep its endpoints). This justifies the correctness of $\mathcal{B}$, completing the proof. $\square$

(b) *Collaborators and sources:* Guanghao 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.

$\mathcal{T} \leftarrow \emptyset$
foreach $(u, v) \in E$ **do**
    pick $x_{u,v} \in [n^4]$ uniformly at random
foreach $e = (u, v) \in E$ **do**
    let $A^{(e)} \in \mathbb{R}^{n \times n}$ be s.t. $\forall u', v' \in V$, $A^{(e)}_{u',v'} = x_{u',v'}$ if $(u', v') \in E \setminus \{e\}$ and 0 otherwise
    $\mathcal{T} \leftarrow \mathcal{T} \cup \{$task to compute $\det A^{(e)}$ and save the result to variable $d_e\}$
run tasks in $\mathcal{T}$ in parallel, obtaining variables d_e for $e \in E$
$M \leftarrow \{e \in E : d_e = 0\}$
return M

Algorithm 2: A randomized 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 stills 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 $\mathbb{P}[e \notin M] = 0$. Note that $\det A^{(e)}$ is the evaluation of multivariate polynomial $\det T_e$ at values $x_{u,v}$ for $(u, v) \in E \setminus \{e\}$. Therefore,

$$\begin{aligned}
\mathbb{P}[\text{Algorithm 2 is correct}] &= 1 - \mathbb{P}\left[\exists e \in M, \det T_e \not\equiv 0 \text{ or } \exists e \in E \setminus M, \det T_e \equiv 0\right] \\
&\geq 1 - \sum_{\substack{e \in E \\ \det T_e \not\equiv 0}} \mathbb{P}\left[e \in M\right] - \sum_{\substack{e \in E \\ \det T_e \equiv 0}} \mathbb{P}[e \notin M] \qquad (3) \\
&= 1 - \sum_{\substack{e \in E \\ \det T_e \not\equiv 0}} \mathbb{P}\left[\det A^{(e)} = 0\right] - \sum_{\substack{e \in E \\ \det T_e \equiv 0}} 0 \\
&\geq 1 - \sum_{\substack{e \in E \\ \det T_e \not\equiv 0}} \frac{n}{|S|} \qquad (4) \\
&\geq 1 - \sum_{e \in E} \frac{n}{n^4} = 1 - m \cdot \frac{1}{n^3} \geq 1 - n^2 \cdot \frac{1}{n^3} = 1 - \frac{1}{n} = 1 - o(1).
\end{aligned}$$

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. $\square$

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

We show that if G contains only one perfect matching of minimum weight equal to w^*, then $\det A \neq 0$ and w^* is the smallest $i \in \{0, \ldots, k\}$ such that $b_i = 1$, where the binary representation of $|\det A|$ is $\sum_{i=0}^{k} b_i 2^i$ with $b_i \in \{0,1\}$ for all $i \in \{0, \ldots, k\}$.

Proof. We assume that the random integer weights $w_{u,v}$ for every edge $(u,v) \in E$ are non-negative (as we can choose the sample space of these weights when we design the algorithm for part (f)). For each $M \subset E$, we denote $w(M) = \sum_{(u,v)\in M} w_{u,v}$. For each permutation σ of $[n]$, we deonte by $M_\sigma = \{(u, \sigma(u)) : u \in L\}$, and we have

$$\prod_{u \in L} A_{u,\sigma(u)} = \begin{cases} \prod_{u\in L} 2^{w_{u,\sigma(u)}} = 2^{\sum_{u\in L} w_{u,\sigma(u)}} = 2^{w(M_\sigma)}, & \text{if } M_\sigma \text{ is a perfect matching,} \\ 0, & \text{otherwise.} \end{cases}$$

Let $\sigma_1, \ldots, \sigma_\ell$ be permutations of $[n]$ such that M_{σ_i} is a perfect matching of G for each $i \in [\ell]$ and that $w(M_{\sigma_1}) < w(M_{\sigma_2}) \leq \ldots \leq w(M_{\sigma_\ell})$. Then

$$\begin{aligned}
\det A &= \sum_{\sigma \text{ permutation of } [n]} \operatorname{sign}(\sigma) \prod_{u\in L} A_{u,\sigma(u)}, \\
&= \sum_{\substack{\sigma \text{ permutation of } [n] \\ M_\sigma \text{ perfect matching}}} \operatorname{sign}(\sigma) \prod_{u\in L} A_{u,\sigma(u)} + \sum_{\substack{\sigma \text{ permutation of } [n] \\ M_\sigma \text{ not perfect matching}}} \operatorname{sign}(\sigma) \prod_{u\in L} A_{u,\sigma(u)} \\
&= \sum_{\substack{\sigma \text{ permutation of } [n] \\ M_\sigma \text{ perfect matching}}} \operatorname{sign}(\sigma) \cdot 2^{w(M_\sigma)} + \sum_{\substack{\sigma \text{ permutation of } [n] \\ M_\sigma \text{ not perfect matching}}} \operatorname{sign}(\sigma) \cdot 0 \\
&= \sum_{\substack{\sigma \text{ permutation of } [n] \\ M_\sigma \text{ perfect matching}}} \operatorname{sign}(\sigma) \cdot 2^{w(M_\sigma)} = \sum_{i=1}^{\ell} \operatorname{sign}(\sigma_i) \cdot 2^{w\left(M_{\sigma_i}\right)} \\
&= 2^{w\left(M_{\sigma_1}\right)} \left(\operatorname{sign}(\sigma_1) + \sum_{i=2}^{\ell} \operatorname{sign}(\sigma_i)\, 2^{w\left(M_{\sigma_i}\right) - w\left(M_{\sigma_1}\right)} \right).
\end{aligned}$$

Therefore,

$$|\det A| = 2^{w\left(M_{\sigma_1}\right)} \left| \operatorname{sign}(\sigma_1) + \sum_{i=2}^{\ell} \operatorname{sign}(\sigma_i)\, 2^{w\left(M_{\sigma_i}\right) - w\left(M_{\sigma_1}\right)} \right|. \tag{5}$$

For each $i \in \{2, \ldots, \ell\}$, since $w(M_{\sigma_i}) > w(M_{\sigma_1})$ and since weights are non-negative integers, then $2^{w(M_{\sigma_i}) - w(M_{\sigma_1})}$ is even. Since $\operatorname{sign}(\sigma_i) \in \{1, -1\}$ for all $i \in [\ell]$, then

$$\left| \operatorname{sign}(\sigma_1) + \sum_{i=2}^{\ell} \operatorname{sign}(\sigma_i)\, 2^{w\left(M_{\sigma_i}\right) - w\left(M_{\sigma_1}\right)} \right| \tag{6}$$

is odd and at least 1. Since weights are non-negative integers, then $2^{w(M_{\sigma_1})} \geq 1$, so $|\det A| \geq 1 \cdot 1 = 1$ and hence $\det A \neq 0$. Suppose that the binary representation of (6) is $1 + \sum_{i=1}^{k'} \beta_i 2^i$, where $\beta_i \in \{0,1\}$ for all $i \in [k']$. Therefore,

$$|\det A| = 2^{w\left(M_{\sigma_1}\right)} \left(1 + \sum_{i=1}^{k'} \beta_i 2^i \right) = 2^{w\left(M_{\sigma_1}\right)} + \sum_{i=1}^{k'} \beta_i 2^{w\left(M_{\sigma_1}\right) + i}.$$

This completes the proof by the uniqueness of binary representations. □

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

The property from part (c) does not necessarily hold if the random weights $w_{u,v}$ for $(u, v) \in E$ result in more than one perfect matching of minimum weight.

Proof. Consider $K_{2,2}$, i.e., $L = R = [2]$ and $E = L \times R$. Let $w_{u,v} = 1$ for all $(u, v) \in E$. There are two perfect matchings of this graph, namely $\{(1, 1), (2, 2)\}$ and $\{(1, 2), (2, 1)\}$, both of weight 2. Hence, the weights $w_{u,v}$ for $(u, v) \in E$ result in more than one perfect matching of minimum weight. Note that $A_{u,v} = X_{u,v} = 2^{w_{u,v}} = 2^1 = 2$ for all $(u, v) \in L \times R = E$. Therefore,

$$\det A = \det \begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix} = 2 \cdot 2 - 2 \cdot 2 = 0.$$

This shows that the property from part (c) does not hold, completing the proof. $\square$

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

Suppose that G contains only one perfect matching of minimum weight. By part (c), $\det A \neq 0$. Suppose that we know the binary representation of $|\det A|$ is $\sum_{i=0}^{k} b_i 2^i$, where $b_i \in \{0,1\}$ for all $i \in \{0,\ldots,k\}$. Let i^* be the smallest $i \in \{0,\ldots,k\}$ such that $b_i = 1$. Then we can detect whether an edge $e \in E$ is in the minimum weight perfect matching using Algorithm 3, which uses a single call to an oracle for determinant computations.

let $A' \in \mathbb{R}^{n\times n}$ be s.t. $\forall u,v \in V$, $A'_{u,v}$ equals $2^{w_{u,v}}$ for all $(u,v) \in E \setminus \{e\}$ and 0 otherwise
$d' \leftarrow \det A'$
if $d' = 0$ **then**
    return *"e is in the minimum weight perfect matching"*
let the binary representation of $|d'|$ be $\sum_{j=0}^{k'} b'_j 2^j$, where $b'_j \in \{0,1\}$ for all $j \in \{0,\ldots,k'\}$
$j^* \leftarrow$ smallest $j \in \{0,\ldots,k'\}$ such that $b'_j = 1$
if $i^* = j^*$ **then**
    return *"e is not in the minimum weight perfect matching"*
else
    return *"e is in the minimum weight perfect matching"*

Algorithm 3: An algorithm for checking whether an edge $e \in E$ is in the minimum weight perfect matching of a bipartite graph $G = (V,E)$ that contains only one perfect matching of minimum weight, using a single call to an oracle for determinant computations.

Proof. Let M be the unique perfect matching of minimum weight w^* in G. Let G' be the graph obtained by removing e from G (while keeping its endpoints). Then $i^* = w^*$ by part (c) and by the definition of i^*.

If e is not contained in M, then M is a unique minimum weight perfect matching of G', so $d' = \det A' \neq 0$, and the minimum weight of a perfect matching of G' is w^*. Therefore, $j^* = w^* = i^*$ by part (c) and by the definition of j^*.

Now, suppose that e is contained in M. We have the following two cases:

- G' does not contain a perfect matching. Then the determinant of the (symbolic) Tutte matrix T' of G' is the zero multivariate polynomial. Note that $\det A'$ is the evaluation of $\det T'$ at values $2^{w_{u,v}}$ for $(u,v) \in E \setminus \{e\}$. Hence, $d' = \det A' = 0$.
- G' contains at least one perfect matching of minimum weight w'. Since any perfect matching of G' is also a perfect matching of G, then $w' > w^*$, or else there would be more than one perfect matching of minimum weight in G, a contradiction to the assumption. WLOG, assume that $\det A' \neq 0$. Let $\sigma_1, \ldots, \sigma_\ell$ be permutations of $[n]$ such that M_{σ_i} is a perfect matching of G' for each $i \in [\ell]$ and that $w' = w(M_{\sigma_1}) \leq w(M_{\sigma_2}) \leq \ldots \leq w(M_{\sigma_\ell})$. By (5),

$$\begin{aligned}\left|\det A'\right| &= 2^{w\left(M_{\sigma_1}\right)} \left|\operatorname{sign}\left(\sigma_1\right) + \sum_{i=2}^{\ell} \operatorname{sign}\left(\sigma_i\right) 2^{w\left(M_{\sigma_i}\right) - w\left(M_{\sigma_1}\right)}\right| \\ &= 2^{w'} \left|\operatorname{sign}\left(\sigma_1\right) + \sum_{i=2}^{\ell} \operatorname{sign}\left(\sigma_i\right) 2^{w\left(M_{\sigma_i}\right) - w\left(M_{\sigma_1}\right)}\right|.\end{aligned}$$

Since $\det A' \neq 0$ and since weights are non-negative integers, then

$$\left|\operatorname{sign}(\sigma_1) + \sum_{i=2}^{\ell} \operatorname{sign}(\sigma_i)\, 2^{w\left(M_{\sigma_i}\right) - w\left(M_{\sigma_1}\right)}\right| \tag{7}$$

is at least 1. Suppose that the binary representation of (7) is $\sum_{i=0}^{k'} \beta_i 2^i$, where $\beta_i \in \{0, 1\}$ for all $i \in \{0, \ldots, k'\}$, and there exists $i \in \{0, \ldots, k'\}$ with $\beta_i = 1$. Hence,

$$\left|\det A'\right| = 2^{w'} \left(\sum_{i=0}^{k'} \beta_i 2^i\right) = \sum_{i=0}^{k'} \beta_i 2^{w'+i}.$$

By the uniqueness of binary representations, we have $j^* \geq w' > w^* = i^*$.

In other words, we have shown that an edge $e \in E$ is not contained in the (unique) minimum weight perfect matching of G if and only if $\det A' \neq 0$ and $i^* = j^*$ (as defined in Algorithm 3). This justifies Algorithm 3, completing the proof. $\square$

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

Proof. We claim that, with high probability, Algorithm 4 finds a perfect matching in a bipartite graph G, given an oracle for determinant computations, such that all calls to the oracle are simultaneous. Note that we can obtain the index of the lowest one in the binary representation of a positive integer $x \in \mathbb{N}$ (i.e., the smallest $i \in \{0, \ldots, k\}$ such that $b_i = 1$ if the binary representation of x is $\sum_{i=0}^{k} b_i 2^i$, where $b_i \in \{0, 1\}$ for all $i \in \{0, \ldots, k\}$) by successively dividing x by 2 until the resulting integer is odd.

let $A \in \mathbb{R}^{n\times n}$ be such that $\forall u, v \in V$, $A_{u,v}$ equals $2^{w_{u,v}}$ if $(u, v) \in E$ and 0 otherwise
$\mathcal{T} \leftarrow \{$task to compute $\det A$ and save the result to variable $d^*\}$
foreach $(u, v) \in E$ **do**
    pick $w_{u,v} \in [n^3]$ uniformly at random
foreach $e = (u, v) \in E$ **do**
    let $A^{(e)} \in \mathbb{R}^{n\times n}$ be obtained by setting the (u, v)-entry of A to 0
    $\mathcal{T} \leftarrow \mathcal{T} \cup \{$task to compute $\det A^{(e)}$ and save the result to variable $d_e\}$
run tasks in $\mathcal{T}$ in parallel, obtaining variables d^* and d_e for $e \in E$
$w^* \leftarrow$ index of the lowest one in the binary representation in $|d^*|$
foreach $e \in E$ *with* $d_e \neq 0$ **do**
    $w_e \leftarrow$ index of the lowest one in the binary representation of $|d_e|$
$M \leftarrow \{e \in E : d_e = 0$ or $w_e \neq w^*\}$
return M

Algorithm 4: A randomized algorithm for finding a perfect matching in a bipartite graph $G = (V, E)$, given an oracle for determinant computations, such that all calls to the oracle are simultaneous.

By part (e), if G has only one perfect matching of minimum weight, then an edge $e \in E$ is contained in this (unique) minimum weight perfect matching if and only if $d_e = \det A^{(e)} \neq 0$ or $w_e \neq w^*$ (where w_e and w^* are defined as in Algorithm 4). Hence, if G has only one perfect matching of minimum weight, then M is this (unique) perfect matching, so Algorithm 4 returns a perfect matching. By Problem 2 part (b),

$$\begin{aligned}\mathbb{P}[\text{Algorithm 4 is correct}] &\geq \mathbb{P}[G \text{ has only one perfect matching of minimum weight}] \\ &\geq 1 - \frac{|E|}{|n^3|} \geq 1 - \frac{n^2}{n^3} = 1 - \frac{1}{n} = 1 - o(1).\end{aligned}$$

This completes the proof. $\square$