For a symmetric, bipartite matrix $A \in \mathbb{C}^{m \times m}$, we want to prove the following theorem:

**Theorem 1.** If $\text{EVAL}(A)$ is not $\#P$-hard, then there exists an $m \times m$ purified bipartite matrix $A'$ such that $\text{EVAL}(A) \equiv \text{EVAL}(A')$.

Recall the definition of the purified bipartite matrix:

**Definition 1.** Let $A \in \mathbb{C}^{m \times m}$ be a symmetric, connected and bipartite matrix. $A$ is called a purified bipartite matrix if there exists positive rational numbers $\mu_1, \ldots, \mu_m$, and an integer $1 \leq k < m$ such that

$$A = \begin{pmatrix} 0 & B \\ B^T & 0 \end{pmatrix}$$

where $B$ is $k \times (m - k)$, and of the following form:

$$B = \begin{pmatrix} \mu_1 \\ \mu_2 \\ \vdots \\ \mu_k \end{pmatrix} \begin{pmatrix} \zeta_{1,1} & \zeta_{1,2} & \cdots & \zeta_{1,m-k} \\ \zeta_{2,1} & \zeta_{2,2} & \cdots & \zeta_{2,m-k} \\ \vdots & \vdots & \ddots & \vdots \\ \zeta_{k,1} & \zeta_{k,2} & \cdots & \zeta_{k,m-k} \end{pmatrix} \begin{pmatrix} \mu_{k+1} \\ \mu_{k+2} \\ \vdots \\ \mu_m \end{pmatrix}$$

where every $\zeta_{i,j}$ is a root of unity.

We shall prove Theorem 1 by constructing the matrix $B$. First, we need to define the notion of a generating set.

**Definition 2.** Let $A = \{a_j\}_{j \in [n]}$ be a set of $n$ non-zero algebraic numbers, for some $n \geq 1$. Then we say $\{g_1, \ldots, g_d\}$, for some integer $d \geq 0$, is a generating set of $A$ if

1. Every $g_i$ is a non-zero algebraic number in $\mathbb{Q}(A)$.
2. For all $(k_1, \ldots, k_d) \in \mathbb{Z}^d$ such that $(k_1, \ldots, k_d) \neq 0$, then $g_1^{k_1} \cdots g_d^{k_d}$ is not a root of unity.
3. For every $a \in A$, there exists a unique $(k_1, \ldots, k_d) \in \mathbb{Z}^d$ such that $a/g_1^{k_1} \cdots g_d^{k_d}$ is a root of unity.

We shall utilize the following lemma to construct the matrix $B$.

**Lemma 1.** Let $A$ be a set of non-zero algebraic numbers, then it has a generating set.
Let $\mathcal{A}$ denote the set of all non-zero entries $A_{i,j}$ from $\mathcal{A}$, by Lemma 1, $\mathcal{A}$ has a generating set $\mathcal{G} = \{g_1, \ldots, g_d\}$. By Definition 2, for each $A_{i,j}$ there exists a unique tuple $(k_1, \ldots, k_d) \in \mathbb{Z}^d$ such that $A_{i,j}/g_1^{k_1} \cdots g_d^{k_d}$ is a root of unity, and we shall denote it by $\zeta_{i,j}$. Next, we construct the matrix $B = (B_{i,j})_{m \times m} \in \mathbb{C}^{m \times m}$ as follows: Let $p_1 < \cdots < p_d$ denote the $d$ smallest primes. Then,

$$B_{i,j} = \begin{cases} 0 & \text{if } A_{i,j} = 0 \\ p_1^{k_1} \cdots p_d^{k_d} \cdot \zeta_{i,j} & \text{if } A_{i,j} = g_1^{k_1} \cdots g_d^{k_d} \cdot \zeta_{i,j} \end{cases}$$ (1)

Note that this construction is in 1-to-1 correspondence: $B_{i,j}$ is well-defined by the uniqueness of $(k_1, \ldots, k_d) \in \mathbb{Z}^d$ and conversely by taking the prime factorization of $|B_{i,j}|$, and then recover $A_{i,j}$. We will prove that EV AL($\mathcal{A}$) $\equiv$ EV AL($\mathcal{B}$). By the last lemma from our last lecture, it suffices to prove COUNT($\mathcal{A}$) $\equiv$ COUNT($\mathcal{B}$). Recall the problem COUNT($\mathcal{A}$) is defined as follows:

**Definition 3.** Let $\mathcal{A} \in \mathbb{C}^{m \times m}$ be a fixed symmetric matrix with algebraic entries, then the input of the problem COUNT($\mathcal{A}$) is a pair $(G, x)$ where $G = (V, E)$ is an undirected graph, and $x$ is a complex number. The output is:

$$\#_\mathcal{A}(G, x) = |\{\text{assignment } \xi : V \rightarrow [m] | \text{wt}_\mathcal{A}(\xi) = x\}|$$

**Lemma 2.** COUNT($\mathcal{A}$) $\equiv$ COUNT($\mathcal{B}$)

**Proof.** We will only prove COUNT($\mathcal{A}$) $\leq$ COUNT($\mathcal{B}$) as the other direction is proved similarly. Let $(G, x)$ be an input of COUNT($\mathcal{A}$) where $G = (V, E)$, and $n = |E|$. Let

$$X = \{ \prod_{i,j \in [m]} A_{i,j}^{k_{i,j}} | k_{i,j} \in \mathbb{N} \text{ and } \sum_{i,j \in [m]} k_{i,j} = n \}$$

Recall that $X$ is polynomial in $n$, and for any $x \notin X$, $\#_\mathcal{A}(G, x) = 0$. For any $x \in X$, we can find a sequence of non-negative integers $\{k_{i,j}^*\}_{i,j \in [m]}$ in polynomial time such that $\sum_{i,j} k_{i,j}^* = n$ and

$$x = \prod_{i,j \in [m]} A_{i,j}^{k_{i,j}^*}$$ (2)

We define $y$ by

$$y = \prod_{i,j \in [m]} B_{i,j}^{k_{i,j}^*}$$ (3)

Thus, $x = 0$ iff $y = 0$, which happens iff when some $k_{i,j}^* > 0$ for some entry $A_{i,j} = 0$. To prove COUNT($\mathcal{A}$) $\leq$ COUNT($\mathcal{B}$), it suffices to prove the claim $\#_\mathcal{A}(G, x) = \#_\mathcal{B}(G, y)$. To prove that claim, we only need to show that for any assignment $\xi : V \rightarrow [m],

$$\text{wt}_\mathcal{A}(\xi) = x \iff \text{wt}_\mathcal{B}(\xi) = y$$

$^1$In this write-up, $\mathbb{N}$ is the set of non-negative integers.
We shall only prove $\wt_A(\xi) = x \Rightarrow \wt_B(\xi) = y$ as the other direction is proved similarly.

Let $\xi : V \to [m]$ be an assignment, for every $i, j \in [m]$, let $k_{i,j}$ be the number of edges $(u, v) \in E$ such that $(\xi(u), \xi(v)) = (i, j)$ or $(j, i)$, then

$$\wt_A(\xi) = \prod_{i,j \in [m]} A_{i,j}^{k_{i,j}} \quad (4)$$

and

$$\wt_B(\xi) = \prod_{i,j \in [m]} B_{i,j}^{k_{i,j}} \quad (5)$$

For $x = 0$, $\wt_A(\xi) = 0$ iff for some zero entry $A_{i,j} = 0$, $k_{i,j} > 0$. By our construction of $B$, $A_{i,j} = 0$ iff $B_{i,j} = 0$, and thus, $\wt_B(\xi) = 0$. Next, we assume both $x, y \neq 0$. Let $\mathcal{G} = \{g_1, \ldots, g_d\}$ be the generating set of the set of all non-zero entries in $A$. By Definition 2, there exists integers $e_{1,(ij)}, \ldots, e_{d,(ij)}$ such that:

$$A_{i,j} = \prod_{\ell=1}^d g_{\ell,(ij)} \cdot \zeta_{i,j} \quad (6)$$

and

$$B_{i,j} = \prod_{\ell=1}^d p_{\ell,(ij)} \cdot \zeta_{i,j} \quad (7)$$

for $A_{i,j} \neq 0$ where $\zeta_{i,j}$ is a root of unity. By (4) and (6),

$$\wt_A(\xi) = x \Rightarrow \prod_{\ell=1}^d g_{\ell}^{\sum_{i,j \in [m]} (k_{i,j} - k_{i,j}^\star) e_{\ell,(ij)}} \text{ is a root of unity}$$

By the second requirement of a generating set in Definition 2, for any $\ell \in [d]$

$$\sum_{i,j} (k_{i,j} - k_{i,j}^\star) e_{\ell,(ij)} = 0$$

which implies that

$$\prod_{i,j} (\zeta_{i,j})^{k_{i,j}} = \prod_{i,j} (\zeta_{i,j})^{k_{i,j}^\star}$$

By (3), (5) and (7), it follows that $\wt_B(\xi) = y$. \qed

Next, we construct the matrix $B'$ by $B'_{i,j} = |B_{i,j}|$, and we will show:

**Lemma 3.** $\text{EVAL}(B') \leq \text{EVAL}(B)$

**Proof.** It suffices to show $\text{COUNT}(B') \leq \text{COUNT}(B)$. Let

$$Y = \{ \prod_{i,j \in [m]} B_{i,j}^{k_{i,j}} | k_{i,j} \in \mathbb{N} \text{ and } \sum_{i,j \in [m]} k_{i,j} = n \}$$
\[ Y_x = \{ y | y \in Y \text{ and } |y| = x \}. \] Thus,
\[ \#B'(G, x) = \sum_{y \in Y_x} \#B(G, y) \]
the lemma then follows.

Next, we will prove Theorem 1.

\textit{Proof}. As both \( B \) and \( B' \) are connected and bipartite, there is always a permutation \( \prod \) of \([m]\) such that \( B_{\prod,\prod} \) is the bipartisation of a \( k \times (m - k) \) matrix \( F \) for some \( k \in [m] \):
\[ B_{\prod,\prod} = \left( \begin{smallmatrix} F & 0 \\ 0 & F' \end{smallmatrix} \right) \] and \( B'_{\prod,\prod} \) is the bipartisation of \( F' \) where \( F'_{i,j} = |F_{i,j}| \). Since permuting \( B \) does not affect the complexity of \( \text{EVAL}(B) \), then
\[ \text{EVAL}(B'_{\prod,\prod}) \leq \text{EVAL}(B_{\prod,\prod}) \equiv \text{EVAL}(B) \equiv \text{EVAL}(A) \]

If \( \text{EVAL}(B'_{\prod,\prod}) \) is \( \#P \)-hard, then \( \text{EVAL}(A) \) is also \( \#P \)-hard. If \( \text{EVAL}(B'_{\prod,\prod}) \) is not \( \#P \)-hard, then since every entry in \( B'_{\prod,\prod} \) is non-negative, by Bulatov and Grohe’s theorem, the rank of \( F' \) must be 1. Therefore, there exists non-negative rational numbers \( \mu_1, \ldots, \mu_k, \ldots, \mu_m \) such that \( F'_{i,j} = \mu_i \mu_{j+k} \) for all \( i \in [k] \) and \( j \in [m - k] \). Furthermore, for all \( i \in [m] \), \( \mu_i \) can not be 0 or else \( B'_{\prod,\prod} \) is not connected. Since every entry in \( B_{\prod,\prod} \) is the product of the corresponding entry in \( B'_{\prod,\prod} \) and some root of unity, \( B_{\prod,\prod} \) is also a purified bipartite matrix. The theorem then follows. \[\square\]