Lecture 15: CS 880: Complexity of Counting Problems

Instructor: Jin-Yi Cai Scribe: Chen Zeng

Let $\mathbf{C}$ be the bipartisation of $\mathbf{F} \in \mathbb{C}^{m \times m}$ where $\mathbf{C} = \left(\begin{smallmatrix} 0 & \mathbf{F} \\ \mathbf{F}^T & 0 \end{smallmatrix}\right)$. Let $\mathfrak{D} = \{\mathbf{D}^0, \ldots, \mathbf{D}^{[N-1]}\}$ be a sequence of N $2m \times 2m$ diagonal matrices. We use EVALP$(\mathbf{C}, \mathfrak{D})$ to denote the following problem: The input is a triple (G, w, i), where $G = (V, E)$ is an undirected graph with $w \in V$, and $i \in [2m]$; The output is:

$$Z_{\mathbf{C},\mathfrak{D}}(G, w, i) = \sum_{\xi: V \to [2m], \xi(w) = i} wt_{\mathbf{C},\mathfrak{D}}(\xi) \tag{1}$$

where

$$wt_{\mathbf{C},\mathfrak{D}}(\xi) = (\prod_{(u,v) \in E} \mathbf{C}_{\xi(u),\xi(v)})(\prod_{v \in V} D_{\xi(v)}^{[deg(v) mod N]}) \tag{2}$$

The difference between EVALP$(\mathbf{C}, \mathfrak{D})$ and EVAL$(\mathbf{C}, \mathfrak{D})$ is that EVALP$(\mathbf{C}, \mathfrak{D})$ fixes the value of a vertex w by i. We want to prove EVALP$(\mathbf{C}, \mathfrak{D}) \equiv$ EVAL$(\mathbf{C}, \mathfrak{D})$. It is easy to see that EVAL$(\mathbf{C}, \mathfrak{D}) \leq$ EVALP$(\mathbf{C}, \mathfrak{D})$. Thus, we only need to prove the other direction. First, we define the notion of a *discrete unitary matrix*.

Definition 1. *Let* $\mathbf{F} \in \mathbb{C}^{m \times m}$ *be a matrix. We say* $\mathbf{F}$ *is* M-discrete unitary *for some positive integer* M *if*

1. *Every entry* $F_{i,j}$ *is a root of unity, and* $M = lcm\{$ *the order of* $F_{i,j} : i, j \in [m]\}$
2. $F_{1,i} = F_{i,1} = 1$ *for all* $i \in [m]$
3. *For any* $i, j \in [m], i \neq j$, $\langle \mathbf{F}_{i,*}, \mathbf{F}_{j,*} \rangle = 0$ *and* $\langle \mathbf{F}_{*,i}, \mathbf{F}_{*,j} \rangle = 0$

We can prove Lemma 1 by assuming the following *pinning* condition on the pair $(\mathbf{C}, \mathfrak{D})$:

1. Every entry of $\mathbf{F}$ is a power of w_N where $w_N = e^{2\pi i/N}$ for some positive integer N.
2. $\mathbf{F}$ is a discrete unitary matrix.
3. $\mathbf{D}^{[0]}$ is the $2m \times 2m$ identity matrix.

Lemma 1. *If* $(\mathbf{C}, \mathfrak{D})$ *satisfies the pinning condition, then* EVALP$(\mathbf{C}, \mathfrak{D}) \equiv$ EVAL$(\mathbf{C}, \mathfrak{D})$.

To prove Lemma 1, we define the following equivalence relation over $[2m]$:

$$i \sim j \text{ if for any undirected graph } G = (V, E) \text{ and } w \in V,\ Z_{\mathbf{C},\mathfrak{D}}(G, w, i) = Z_{\mathbf{C},\mathfrak{D}}(G, w, j) \tag{3}$$

Suppose this equivalence relation divides $[2m]$ into s equivalence classes $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_s$ for some positive integer s. If $s = 1$, Lemma 1 is trivially true. If $s \geq 2$, for any $t \neq t' \in [s]$, there exists a $P_{t,t'} = (G, w)$, where G is an undirected graph and w is a vertex, such that for any $j \in \mathcal{A}_t$, $j' \in \mathcal{A}_{t'}$

$$Z_{\mathbf{C},\mathfrak{D}}(G, w, j) \neq Z_{\mathbf{C},\mathfrak{D}}(G, w, j')$$

For any subset $S \subseteq [s]$, we define:

$$Z_{\mathbf{C},\mathfrak{D}}(G, w, S) = \sum_{\xi: V \to [2m], \xi(w) \in \cup_{t \in S} A_t} wt_{\mathbf{C},\mathfrak{D}}(\xi)$$

We will prove the following claim:

Claim 1. *If $S \subseteq [s]$ and $|S| \geq 2$, then there exists a partition $\{S_1, \ldots, S_k\}$ of S for some $k > 1$ such that*

$$\text{EVAL}(\mathbf{C}, \mathfrak{D}, S_d) \leq \text{EVAL}(\mathbf{C}, \mathfrak{D}, S) \ \textit{for all } d \in [k]$$

Proof. Let $t \neq t'$ be two different integers in S, and $P_{t,t'} = (G^*, w^*)$ where $G^* = (V^*, E^*)$. It defines the following equivalence relation over S: For $a, b \in S$,

$$a \sim^* b \text{ if } Z_{\mathbf{C},\mathfrak{D}}(G^*, w^*, i) = Z_{\mathbf{C},\mathfrak{D}}(G^*, w^*, j) \text{ where } i \in \mathcal{A}_a \text{ and } j \in \mathcal{A}_b$$

This gives us equivalence classes $\{S_1, \ldots, S_k\}$, also a partition of S, which is independent of the choice of i (j) as long as $i \in A_a (j \in A_b)$. The reason is that by (3), for any $i_1, i_2 \in A_a$, $Z_{\mathbf{C},\mathfrak{D}}(G^*, w^*, i_1) = Z_{\mathbf{C},\mathfrak{D}}(G^*, w^*, i_2)$.

By our definition of $P_{t,t'}$, t and t' belong to different classes. Thus, $k \geq 2$. For each $d \in [k]$, let

$$Y_d = Z_{\mathbf{C},\mathfrak{D}}(G^*, w^*, i), \ \text{ where } i \in \mathcal{A}_a \text{ and } a \in S_d \tag{4}$$

Our definition of Y_d is independent of both a and i. That is because for any $a_1, a_2 \in \mathcal{S}_d$, and any $i_1 \in A_{a_1}$ and $i_2 \in A_{a_2}$, $Z_{\mathbf{C},\mathfrak{D}}(G^*, w^*, i_1) = Z_{\mathbf{C},\mathfrak{D}}(G^*, w^*, i_2)$.

Let G be an undirected graph and w be a vertex. For each integer $p \in [0 : k-1]$, we construct a graph $G^{[p]} = (V^{[p]}, E^{[p]})$ as follows: $G^{[p]}$ contains one copy of the undirected graph G and p independent copies of G^*. For each integer $i \in [p]$, we add two vertices x_i and y_i, and then we connect edges as shown in Figure 1: one edge between $(w^*_{[i]}, x_i)$ and (y_i, w); $N-1$ edges between (x_i, w) and $(w^*_{[i]}, y_i)$. Therefore, $Z_{\mathcal{C},\mathfrak{D}}(G^{|p|}, w, S)$ is equal to

$$\sum_{\substack{i \in \cup_{a \in S} A_a \\ i_1, \ldots, i_p \in [2m]}} Z_{\mathcal{C},\mathfrak{D}}(G^*, w^*, i_j) (\prod_{j=1}^{p} Z_{\mathcal{C},\mathfrak{D}}(G^*, w^*, i_j)) \prod_{j=1}^{p} (\sum_{x \in [2m]} C_{i_j,x} \overline{C_{i,x}} \sum_{y \in [2m]} \overline{C_{i_j,y}} C_{i,y}) \tag{5}$$

By the *pinning* condition, if $i_j \neq i$, then

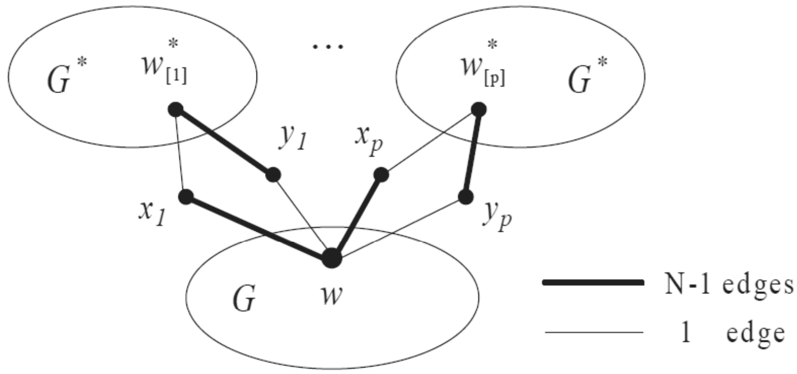

Figure 1: Graph $G^{[p]}$

$$\sum_{x\in[2m]} C_{i_j,x}\overline{C_{i,x}} = \langle \mathbf{F}_{i_j,*}, \mathbf{F}_{i,*}\rangle = 0$$

By our construction of Figure 1, $\deg(x_i) = \deg(y_i) = N$, and thus, the changes to the degrees of w and $w^*_{[i]}$ are all multiples of N. Also by the *pinning* condition, $\mathbf{D}^{[0]}$ is the identity matrix, and thus, there are no new vertex weight contributions from $\mathfrak{D}$. Therefore,

$$Z_{\mathcal{C},\mathfrak{D}}(G^{|p|}, w, S) = m^{2p} \sum_{i\in\cup_{a\in S}A_a} Z_{\mathcal{C},\mathfrak{D}}(G, w, i)(Z_{\mathcal{C},\mathfrak{D}}(G^*, w^*, i))^p = m^{2p} \sum_{d\in[k]} (Y_d)^p Z_{\mathcal{C},\mathfrak{D}}(G, w, S_d)$$

By our definition of Y_d in (4), $Y_d \neq Y_d'$ unless $d = d'$, and thus, this is a Vandermonde system with row indexed by p and column indexed by d. Because both k and the size of the graph G^* are constants that are independent of G, this claim then follows. $\square$

Then, the proof of Lemma 1 is similar to the first pinning lemma in the last lecture, and we omit the details here.

Next, we turn to the following problem: assume $\mathbf{A}$ is connected and bipartite, obtain the conditions on $\mathbf{A}$ such that $Z_{\mathbf{A}}$ is not #P-hard. Our roadmap to solve that problem consists of the following steps: first, we define a *purification* of a matrix $\mathbf{A}$.

Definition 2. *Let $\mathbf{A} \in \mathbb{C}^{m\times m}$ be a symmetric, connected and bipartite matrix. $\mathbf{A}$ is called a* purified bipartite matrix *if there exists positive rational numbers $\mu_1, \dots, \mu_m$, and an integer $1 \leq k < m$ such that*

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

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

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

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

If $\mathbf{A}$ is a purified, bipartite and connected matrix, we can prove the following theorem:

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

Now let $\mathbf{A} \in \mathbb{C}^{m\times m}$ be a purified bipartite matrix. We will prove that EVAL($\mathbf{A}$) is either #P-hard or can be reduced to EVAL($\mathbf{C}, \mathfrak{D}$) in polynomial time for some $\mathbf{C}$ and $\mathfrak{D}$, and the matrix $\mathbf{C}$ is the bipartisation of a *discrete unitary matrix*. Then we can prove the following theorem.

Theorem 2. *Let $\mathbf{A} \in \mathbb{C}^{m\times m}$ be a purified bipartite matrix. Then either*

1. *EVAL($\mathbf{A}$) is tractable or*
2. *EVAL($\mathbf{A}$) is #P-hard or*
3. *There exists a triple $(\mathcal{C}, \mathfrak{D}, (M, N))$ satisfying the following conditions:*

- *M and N are positive integers that satisfy $2|N$ and $M|N$, and $\mathfrak{D}$ is a sequence of N $2n \times 2n$ diagonal matrices over $\mathbb{C}$, and $\mathbf{C} \in \mathbb{C}^{2n\times 2n}$ for some $n \geq 1$.*
- *$\mathbf{C} = \begin{pmatrix} 0 & \mathbf{F} \\ \mathbf{F}^T & 0 \end{pmatrix}$ where $\mathbf{F} \in \mathbb{C}^{n\times n}$ is M-discrete unitary.*
- *$\mathbf{D}^0 = I$. For all $r \in [N-1]$, if there exists an integer $i \in [n]([n+1:2n])$ such that $\mathbf{D}_i^{[r]} \neq 0$, then there exists another integer $i' \in [n]([n+1:2n])$ such that $\mathbf{D}_{i'}^{[r]} = 1$.*
- *For all $r \in [N-1]$ and all $i \in [2n]$, $\mathbf{D}_i^{[r]} \in \mathbb{Q}(w_N)$ and $|\mathbf{D}_i^{|r|}| \in \{0, 1\}$.*

So far, we have shown the original problem EVAL($\mathbf{A}$) is either tractable; or #P-hard; or polynomial-time equivalence to a new problem EVAL($\mathbf{C}, \mathfrak{D}$).

Theorem 3. *Suppose $((M, N), \mathbf{C}, \mathfrak{D})$ satisfies $(\mu_1)-(\mu_4)$ and the integer $M > 1$, then either the problem EVAL$(\mathbf{C}, \mathfrak{D})$ is #P-hard or every entry of $\mathbf{D}^{[r]}$ is either 0 or a power of ω_n*

The next theorem shall explores the structures in $\mathbf{F}$ as well as the diagonal matrices in $\mathfrak{D}$. Before that, we defines the notion of a *Fourier decomposition.*

Definition 3. *Let $q > 1$ be a prime power, and $k \geq 1$ be an integer such that* $\gcd(k, q) = 1$. *We call the following $q \times q$ matrix $\mathcal{F}_{q,k}$ a (q, k)-*Fourier matrix *where the $(x, y)^{th}$ entry is:*

$$w_q^{kxy} = e^{2\pi i(kxy/q)}$$

Then we will prove Theorem 5.4 on page 24. That concludes the roadmap of our proof. Next, to prove Theorem 1, we first define a class of counting problems:

Definition 4. *Let* $\mathbf{A} \in \mathbb{C}^{m \times m}$ *be a fixed symmetric matrix with algebraic entries, then the input of the problem* COUNT*(*$\mathbf{A}$*) is a pair* (G, x) *where* $G = (V, E)$ *is an undirected graph, and* x *is a complex number. The output is:*

$$\#_{\mathbf{A}}(G, x) = |\{\textit{assignment}\ \xi : V \to [m] | wt_{\mathbf{A}}(\xi) = x\}|$$

Suppose $\mathbf{A}$ is a symmetric matrix with algebraic entries, we will show that EVAL($\mathbf{A}$) $\equiv$ COUNT($\mathbf{A}$).

Proof. Let $G = (V, E)$ and $n = |E|$, and

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

By combinatorics, $|X| = \binom{n+m^2-1}{m^2-1}$. By our assumption that m is a constant, $|X|$ is thus in polynomial in n. Recall the definition of $wt_{\mathbf{A}}(\xi)$ where:

$$wt_{\mathbf{A}}(\xi) = \prod_{(u,v) \in E} A_{\xi(u),\xi(v)}$$

Therefore, for any $x \notin X$, $\#_{\mathbf{A}}(G, x) = 0$, and thus,

$$Z_{\mathbf{A}}(G) = \sum_{x \in X} x \cdot \#_{\mathbf{A}}(G, x)$$

Therefore, EVAL($\mathbf{A}$) $\leq$ COUNT($\mathbf{A}$). For the other direction, we construct a graph by thickening: for any $p \in [|X|]$, a new undirected graph $G^{[p]}$ is generated from G by replacing every edge (u, v) of G with p parallel edges between u and v. Then for any assignment ξ, if its weight over G is x, then its weight over $G^{[p]}$ must be x^p. Hence, for every $p \in [|X|]$, and any undirected graph,

$$Z_{\mathbf{A}}(G^{[p]}) = \sum_{x \in X} x^p \cdot \#_{\mathbf{A}}(G, x)$$

which constitutes a Vandermonde system. By querying EVAL($\mathbf{A}$) for the graph $G^{[p]}$, we can solve it and get $\#_{\mathbf{A}}(G, x)$ for every non-zero $x \in X$. For $x = 0$, we observe that:

$$\sum_{x \in X} \#_{\mathbf{A}}(G, x) = m^{|V|}$$

Since $|X|$ is in polynomial in n, this gives a polynomial-time reduction, COUNT($\mathbf{A}$) $\leq$ EVAL($\mathbf{A}$). $\square$