CS 880: Complexity of Counting Problems 04/12/2012

Lecture 22: Step 2.4

Instructor: Jin-Yi Cai Scribe: Hesam Dashti

In step 2.3 we considered a pair ($\mathbf{C}$, $\mathfrak{D}$) and showed that this pair satisfies all the properties of $Shape_1$ to $Shape_6$. In this pair

$$\mathbf{C} = \begin{pmatrix} 0 & F \\ F^T & 0 \end{pmatrix},$$

where

$$F = \begin{pmatrix} \mu_1\mathbf{I} & & \\ & \ddots & \\ & & \mu_s\mathbf{I} \end{pmatrix} \begin{pmatrix} \mathbf{H} & \cdots & \\ \vdots & \ddots & \\ & & \mathbf{H} \end{pmatrix} \begin{pmatrix} \nu_1\mathbf{I} & & \\ & \ddots & \\ & & \nu_s\mathbf{I} \end{pmatrix},$$

or in other words, if $M = (\mu_i\nu_j)$, then $F = M \otimes \mathbf{H}$. The vector weights

$$\mathfrak{D} = \{\mathbf{D}^{[0]}, \dots \mathbf{D}^{[n-1]}\},$$

with

$$\mathbf{D}^{[r]} = K^{[r]} \otimes L^{[r]}.$$

Let us start this section with Lemma 8.10 as follows,
Lemma 8.10: EVAL($\mathbf{C}$, $\mathfrak{D}$)≡EVAL($\mathbf{C}''$, $\mathfrak{L}$), where

$$\mathbf{C}'' = \begin{pmatrix} 0 & \mathbf{H} \\ \mathbf{H}^T & 0 \end{pmatrix} \text{ and } \mathfrak{L} = \{L^{[0]}, \dots, L^{[N-1]}\}.$$

Proof. To prove this lemma, we need to define another pair ($\mathbf{C}'$, $\mathfrak{K}$), where

$$\mathbf{C}' = \begin{pmatrix} 0 & M \\ M^T & 0 \end{pmatrix} \text{ and } \mathfrak{K} = \{K^{[0]}, \dots, K^{[N-1]}\}.$$

Let $G = (V, E)$ be a connected undirected graph and $u^* \in V$. We saw that (lemma 2.2 and 2.3)

$$Z_{\mathbf{C},\mathfrak{D}}(G) = Z^{\rightarrow}_{\mathbf{C},\mathfrak{D}}(G, u^*) + Z^{\leftarrow}_{\mathbf{C},\mathfrak{D}}(G, u^*). \tag{1}$$

where,

$$Z^{\rightarrow}_{\mathbf{C},\mathfrak{D}}(G, u^*) = Z^{\rightarrow}_{\mathbf{C}',\mathfrak{K}}(G, u^*) + Z^{\rightarrow}_{\mathbf{C}'',\mathfrak{L}}(G, u^*).$$
$$Z^{\leftarrow}_{\mathbf{C},\mathfrak{D}}(G, u^*) = Z^{\leftarrow}_{\mathbf{C}',\mathfrak{K}}(G, u^*) + Z^{\leftarrow}_{\mathbf{C}'',\mathfrak{L}}(G, u^*).$$

We divide the equality (1) equality into inner and outer parts and consider each part separately. First, we show that the outer part is polynomially computable as follows:

For simplicity we ignore $\mathfrak{D}$ and also only consider $Z_{\overrightarrow{\mathbf{C}'},\mathfrak{R}}(G,u^*)$. The same is correct for $Z_{\overleftarrow{\mathbf{C}'},\mathfrak{R}}(G,u^*)$. The graph G is bipartite (otherwise these terms are zero) so can be written as $G(U\cup V,E)$ where every node in U is connected to some nodes in V. Let $u^*\in U$ and Ξ be a set of assignments such that

$$\forall\xi\in\Xi,\xi:U\to[s]\text{ and }V\to[t].$$

Then we will have

$$\begin{aligned} Z_{\overrightarrow{\mathbf{C}'},\mathfrak{R}}(G,u^*) &= \sum_{\xi\in\Xi}\left(\prod_{uv\in E}\mu_{\xi(u)}\cdot\nu_{\xi(v)}\right)\left(\prod_{u\in U}K^{[deg(u)]}_{(0,\xi(u))}\right)\left(\prod_{v\in V}K^{[deg(v)]}_{(1,\xi(v))}\right)\\ &= \prod_{u\in U}\left(\sum_{i\in[s]}(\mu_i)^{[deg(u)]}\cdot K^{[deg(u)]}_{(0,i)}\right)\times\prod_{v\in V}\left(\sum_{j\in[t]}(\nu_j)^{[deg(v)]}\cdot K^{[deg(v)]}_{(1,j)}\right), \end{aligned}$$

which is polynomially computable.
Next, let us consider the inner part. Recall that from the third pinning lemma-corollary 8.2 that $Z_{\overrightarrow{\mathbf{C}},\mathfrak{D}}(G,u^*)$ and $Z_{\overleftarrow{\mathbf{C}},\mathfrak{D}}(G,u^*)$ are reducible to $Z_{\mathbf{C},\mathfrak{D}}(G)$. Therefore the inner part is reducible to $Z_{\mathbf{C}'',\mathfrak{L}}(G)$ which is the right hand side of the lemma and we are done with the proof.
The only exception is when one of the outer part terms is equal to zero. This exception is considered in Lemma 8.8 and we do not through it here. □

Now we have almost enough tools to prove the theorems 5.3 and 5.4. The next lemma to prove is lemma 9.1 as follows,
Lemma 9.1 Let $((M,N),\ \mathbf{C},\ \mathfrak{D})$ be a tuple that satisfies $(\mathcal{U}_1)$-$(\mathcal{U}_4)$ with $\mathbf{F}\in\mathbb{C}^{m\times m}$ as the upper-right block of $\mathbf{C}$. Then either EVAL($\mathbf{C}$, $\mathfrak{D}$) is #-P hard or $\mathbf{F}$ satisfies the following group conditions $(\mathcal{GC})$:

1. (row-$\mathcal{GC}$): $\forall i,j\in[0:m-1],\exists k\in[0:m-1]$ such that $\mathbf{F}_{k,*}=\mathbf{F}_{i,*}\circ\mathbf{F}_{j,*}$
2. (col-$\mathcal{GC}$): $\forall i,j\in[0:m-1],\exists k\in[0:m-1]$ such that $\mathbf{F}_{*,k}=\mathbf{F}_{*,i}\circ\mathbf{F}_{*,j}$

We need to develop some preliminaries before proving the lemma. Let $G=(V,E)$ be an undirected graph and replace every $uv\in E$ by a gadget $G^{[p]}$ for every integer $p\geq 1$ (Figure 5 of the paper (here Figure 1)).

According to the structure of this gadget and also since $\mathfrak{D}$ satisfies $(\mathcal{U}_3)$ then

$$Z_{\mathbf{C},\mathfrak{D}}(G^{[p]})=Z_{\mathbf{C}}(G^{[p]}).\tag{2}$$

On the other hand the graph $G^{[p]}$ is symmetric, therefore we would be able to construct a symmetric matrix $A^{[p]}$ such that

$$Z_{A^{[p]}}(G)=Z_{\mathbf{C}}(G^{[p]}).\tag{3}$$

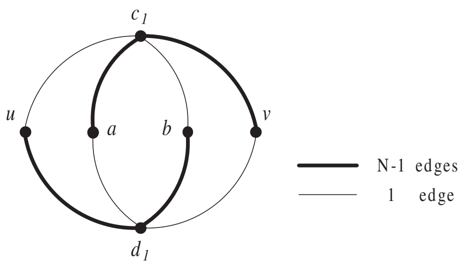

Figure 1: The gadget $G^{[1]}$. It is clear that the degree of every vertex in G is N

From the equations (2) and (3)

$$Z_{\mathbf{C},\mathfrak{D}}(G^{[p]}) = Z_{A^{[p]}}(G) \quad \forall G.$$

Therefore, $Z_{A^{[p]}}(G) \leq Z_{\mathbf{C},\mathfrak{D}}(G^{[p]})$ and when $Z_{\mathbf{C},\mathfrak{D}}(G^{[p]})$ is not #-P hard therefore $Z_{A^{[p]}}(G)$ won't be.
Let us consider the structure of $A^{[p]}$. The $(i,j)^{th}$ entry of $A^{[p]}$ is of the form

$$\begin{aligned} A^{[p]}_{i,j} &= \sum_{a=0}^{2m-1}\sum_{b=0}^{2m-1}\left(\sum_{c=0}^{2m-1}\mathbf{C}_{i,c}\overline{\mathbf{C}_{a,c}}\mathbf{C}_{b,c}\overline{\mathbf{C}_{j,c}}\right)^{p}\left(\sum_{d=0}^{2m-1}\overline{\mathbf{C}_{i,d}}\mathbf{C}_{a,d}\overline{\mathbf{C}_{b,d}}\mathbf{C}_{j,d}\right)^{p} \\ &= \sum_{a=0}^{2m-1}\sum_{b=0}^{2m-1}\left|\sum_{c=0}^{2m-1}\mathbf{C}_{i,c}\overline{\mathbf{C}_{a,c}}\mathbf{C}_{b,c}\overline{\mathbf{C}_{j,c}}\right|^{2p}. \end{aligned}$$

Then

$$A^{[p]} = \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \geq 0,$$

and for $i,j \in [0:m-1]$

$$A^{[p]}_{i,j} = \sum_{a=0}^{m-1}\sum_{b=0}^{m-1} | < \mathbf{F}_{i,*} \circ \overline{\mathbf{F}_{j,*}}, \mathbf{F}_{a,*} \circ \overline{\mathbf{F}_{b,*}} > |^{2p} \tag{4}$$

$$A^{[p]}_{i+m,j+m} = \sum_{a=0}^{m-1}\sum_{b=0}^{m-1} | < \mathbf{F}_{*,i} \circ \overline{\mathbf{F}_{*,j}}, \mathbf{F}_{*,a} \circ \overline{\mathbf{F}_{*,b}} > |^{2p}. \tag{5}$$

Next let us consider two cases when $i = j$ and $i \neq j$ and compute $A^{[p]}_{i,j}$:

$$A^{[p]}_{i,i} = \sum_{a=0}^{m-1}\sum_{b=0}^{m-1} | < 1, \mathbf{F}_{a,*} \circ \overline{\mathbf{F}_{b,*}} > |^{2p} = \sum_{a=0}^{m-1}\sum_{b=0}^{m-1} | < \mathbf{F}_{a,*}, \mathbf{F}_{b,*} > |^{2p}.$$

and since $\mathbf{F}$ is unitary matrix we will get $A^{[p]}_{i,j} = m \cdot m^2$. On the other hand

$$A^{[p]}_{i,j} = A^{[p]}_{j,i} \quad i \neq j.$$

Since $A^{[p]}$ is not #-P hard, therefore by Bulatov-Grohe we should have

$$\begin{vmatrix} A^{[p]}_{i,i} & A^{[p]}_{i,j} \\ A^{[p]}_{j,i} & A^{[p]}_{j,j} \end{vmatrix} = 0.$$

Combining this by the symmetric property of $A^{[p]}$ we can conclude that

$$\forall i,j \quad A^{[p]}_{i,j} = m^{2p+1}.$$

Having these properties we show that $\mathbf{F}$ satisfies the $\mathcal{GC}$. For $i,j \in [0:m-1]$, let

$$X_{i,j} = \left\{ | < \mathbf{F}_{i,*} \circ \overline{\mathbf{F}_{j,*}}, \mathbf{F}_{a,*} \circ \overline{\mathbf{F}_{b,*}} > | \right\} \quad \forall a,b \in [0:m-1]. \tag{6}$$

Some properties of $X_{i,j}$:

1. $X_{i,j}$ is finite for every i,j.
2. $|X_{i,j}| \leq m^2$.
3. $\forall x \in X_{i,j}, 0 \leq x \leq m$.

Now if $s_{i,j}(x)$ denotes number of pairs (a,b) such that $| < \mathbf{F}_{i,*} \circ \overline{\mathbf{F}_{j,*}}, \mathbf{F}_{a,*} \circ \overline{\mathbf{F}_{b,*}} > | = x$, then we can have

$$A^{[p]}_{i,j} = \sum_{x \in X_{i,j}} s_{i,j}(x) \cdot x^{2p} = m^{2p+1}.$$

Notice that $s_{i,j}$ does not depend on p and

$$\sum_{x \in X_{i,j}} s_{i,j} = m^2.$$

Notice that in these equations if we have $(a,b) = (i,j)$ and (i',j) with $i' \neq i$, then we will get $m \in X_{i,j}$ and $0 \in X_{i,j}$. We can consider the equation of $A^{[p]}_{i,j}$ -for a fixed (i,j)- as a system of equations, we may be able to find a solution for the unknowns $s_{i,j}$. The unknown matrix is a Vandermonde matrix of dimension $|X_{i,j}| \times |X_{i,j}|$ of $((x^2)^p)$, with row index $p = 1, \dots |X_{i,j}| - 1$ and column index $x \in X_{i,j}$.
Since this is a Vandermonde matrix, it is a full rank matrix and has a unique solution. We also found that m and 0 are in $s_{i,j}$. By plugging in these values we will get

$$\begin{cases} s_{i,j}(m) = m, \\ s_{i,j}(0) = m^2 - m, \\ s_{i,j}(x) = 0 \quad \text{for all other cases,} \end{cases}$$

is a solution of the linear system. Therefore

$$\forall i,j,a,b \in [0:m-1], | < \mathbf{F}_{i,*} \circ \overline{\mathbf{F}_{j,*}}, \mathbf{F}_{a,*} \circ \overline{\mathbf{F}_{b,*}} > | = 0 \text{ or } m. \tag{7}$$

Next, we use this property to prove that $\mathbf{F}$ indeed satisfies the $\mathcal{GC}$.
Recall the definition of $A_{i,j}^{[p]}$ (equation (4)) and set $j = 0$. In this case we will get

$$\sum_{b=0}^{m-1}\sum_{a=0}^{m-1} | < \mathbf{F}_{i,*} \circ \overline{\mathbf{F}_{0,*}}, \mathbf{F}_{a,*} \circ \overline{\mathbf{F}_{b,*}} > |^2$$

Since $\mathbf{F}_{0,*} = 1$,

$$\sum_{b=0}^{m-1}\sum_{a=0}^{m-1} | < \mathbf{F}_{i,*} \circ \mathbf{F}_{b,*}, \mathbf{F}_{a,*} > |^2.$$

Note that this is similar to the Fourier trnasform where the basis are orthogonal and $\|\mathbf{F}_{a,*}\|^2 = m$.

$$\Rightarrow \sum_{b=0}^{m-1}\sum_{a=0}^{m-1} | < \mathbf{F}_{i,*} \circ \mathbf{F}_{b,*}, \mathbf{F}_{a,*} > |^2 = m \cdot \|\mathbf{F}_{i,*} \circ \mathbf{F}_{b,*}\|^2.$$

Since $\|\mathbf{F}_{i,*} \circ \mathbf{F}_{b,*}\|^2$ is a root of unity and equal to m,
$\Rightarrow m \cdot \|\mathbf{F}_{i,*} \circ \mathbf{F}_{b,*}\|^2 = m^2$.

Here we can conclude that

$$\forall i, \forall b, \exists a \text{ such that } | < \mathbf{F}_{i,*} \circ \mathbf{F}_{b,*}, \mathbf{F}_{a,*} > | = m.$$

Let us consider this equality, all of these vectors are roots of unity and their inner products is equal to m. Therefore all of the vectors have the same angle θ such that

$$\mathbf{F}_{a,*} = e^{i\theta} \cdot (\mathbf{F}_{i,*} \circ \mathbf{F}_{b,*}).$$

To finish $\mathbf{F}$ satisfies the row-$\mathcal{GC}$, we plug in $(* = 0)$ to find the θ:

$$\mathbf{F}_{a,0} = e^{i\theta} \cdot (\mathbf{F}_{i,0} \circ \mathbf{F}_{b,0}).$$
$$\mathbf{F}_{*,0} = 1.$$
$$\Rightarrow 1 = e^{i\theta} \cdot (1 \circ 1).$$
$$\Rightarrow \theta = 0.$$
$$\Rightarrow \mathbf{F}_{a,*} = \mathbf{F}_{i,*} \circ \mathbf{F}_{b,*}.$$

The proof for col$-\mathcal{GC}$ is exactly the same. Therefore $\mathbf{F}$ satisfies the group conditions.