CS 880: Complexity of Counting Problems 03/27/2012

Lecture 19: The Vanishing Lemma and Lemma 8.8

Instructor: Jin-Yi Cai Scribe: Hesam Dashti

Recall from the previous lecture that $\mathbf{D}^{[r]}_a = \sum_{b=0}^{N-1} \alpha_{a,b}\omega_N^{br}$, and also $\mathbf{D}^{[0]}_a = \sum_{b=0}^{N-1} \alpha_{a,b}$ with positive diagonal entries, such that

$$\mathbf{D}^{[0]} = \begin{pmatrix} \mathbf{D}^{[0]}_{(0,*)} & \\ & \mathbf{D}^{[0]}_{(1,*)} \end{pmatrix} = \begin{pmatrix} \mathbf{K}^{[0]}_{(0,*)} \otimes \mathbf{L}^{[0]}_{(0,*)} & \\ & \mathbf{K}^{[0]}_{(1,*)} \otimes \mathbf{L}^{[0]}_{(1,*)} \end{pmatrix}.$$

Since $\mathfrak{D} = \{\mathbf{D}^{[0]}, \ldots, \mathbf{D}^{[N-1]}\}$ satisfy the $\mathcal{T}_3$ properties, then we have:

$$\mathbf{D}^{[r]}_a = \overline{\mathbf{D}^{[N-r]}_a}.$$

In other words, $\mathbf{D}^{[0]}$ is consists of an upper half and a lower half and there are blocks of a constant times the identity matrix in some size (section 8.4). Here we want to show the same is correct for $\mathbf{D}^{[r]}$.
$(Shape_6)$ $\exists\ \mathbf{K}^{[r]}_{(s+t)\times(s+t)}$ and $\mathbf{L}^{[r]}_{2h\times 2h}$ such that:

$$\mathbf{D}^{[r]} = \begin{pmatrix} \mathbf{D}^{[r]}_{(0,*)} & \\ & \mathbf{D}^{[r]}_{(1,*)} \end{pmatrix} = \begin{pmatrix} \mathbf{K}^{[r]}_{(0,*)} \otimes \mathbf{L}^{[r]}_{(0,*)} & \\ & \mathbf{K}^{[r]}_{(1,*)} \otimes \mathbf{L}^{[r]}_{(1,*)} \end{pmatrix}. \tag{1}$$

To prove this we need to assume (lemma 8.8) for any fixed $1 \le r \le N-1$

$$\text{Let } \mathbf{D}_{i,j} = \mathbf{D}^{[r]}_{(0,(i,j))} \quad \forall i \in [s] \text{ and } j \in [h]$$
$$\mathbf{D} = (\mathbf{D}_{i,j}),$$

with rank($\mathbf{D}$)≤ 1 and if $\mathbf{D}_{i,j} \neq 0$ and $\mathbf{D}_{i,j'} \neq 0$ then $|\mathbf{D}_{i,j}| = |\mathbf{D}_{i,j'}|$.
Having this assumption in our deposit, every non-zero $\mathbf{D}^{[r]}_{(0,*)}$ is of rank 1, therefore can be written as $\mathbf{D}_{i,*} = (\mathbf{D}_{(i,b)}/\mathbf{D}_{(a,b)})$ for any $i \in [s]$. Therefore the obvious choice for the corresponding $\mathbf{K}^{[r]}$ and $\mathbf{L}^{[r]}$ are as follows

$$\mathbf{K}^{[r]}_{(0,i)} = \mathbf{D}_{i,b} \text{ and } \mathbf{L}^{[r]}_{(0,j)} = \frac{\mathbf{D}_{a,j}}{\mathbf{D}_{a,b}} \quad \forall i \in [s], j \in [h].$$

Hence,

$$\mathbf{D}^{[r]}_{(0,(i,j))} = \mathbf{D}_{i,j} = \mathbf{K}^{[r]}_{(0,i)} \cdot \mathbf{L}^{[r]}_{(0,j)}, \quad \forall i \in [s] \text{ and } j \in [h].$$

One can follow the same process for $\mathbf{D}^{[r]}_{(1,*)}$ and show equation 1 is correct.
To prove the above assumption (lemma 8.8), one needs to to consider the vanishing lemma (8.4.1) as follows.

(8.4.1) The Vanishing Lemma

For a positive integer k and $1 \leq i \leq k$, let $\{x_{i,n}\}_{n\geq 1}$ be k infinite sequences of non-zero real numbers. In addition, let $\{x_{0,n}\}_{n\geq 1}$ be a squence with $\{x_{0,n}\}_{n\geq 1} = 1$. The following is correct for all $0 \leq i < k$

$$\lim_{n\to\infty} \frac{x_{i+1,n}}{x_{i,n}} = 0.$$

Part A Let a_i and b_i be complex coefficients of $x_{i,n}$. Suppose

$$\begin{aligned}
&\exists 1 \leq l \leq k, \text{such that } a_i = b_i, \quad \forall 0 \leq i < l. \\
&a_0 = b_0 = 1 \\
&\mathrm{Im}(a_l) = \mathrm{Im}(b_l).
\end{aligned}$$

For *infinity many n*, $|\sum_{i=0}^{k} a_i x_{i,n}| = |\sum_{i=0}^{k} b_i x_{i,n}|$, then $a_l = b_l$.

Part B Let $a_i \in \mathbb{C}$, for $0 \leq i < k$. For *infinity many n*, $|\sum_{i=0}^{k} a_i x_{i,n}| = 0$ then $a_i = 0$, for all $0 \leq i \leq k$.

We note that in both parts $x_{i,n}$ are real and cannot be extended to the complex numbers. This is only allowed to choose the coefficients from $\mathbb{C}$.

Proof. The proof of Part A starts with multiplying the equation with the conjugate terms:

$$\left(\sum_{i=0}^{k} a_i x_{i,n}\right)\left(\sum_{j=0}^{k} \overline{a_j} x_{j,n}\right) = \left(\sum_{i=0}^{k} b_i x_{i,n}\right)\left(\sum_{j=0}^{k} \overline{b_j} x_{j,n}\right)$$

Next consider the following conditions:

1. $\max\{i,j\} < l$. Recall that in this case $a_i = b_i$, then $a_i \overline{a_j} x_{i,n} x_{j,n} = b_i \overline{b_j} x_{i,n} x_{j,n}$ and the equality is satisfied.

2. $(\max\{i,j\} > l)$ or $(\max\{i,j\} = l$ and $\min i,j > 0)$. As $n \to \infty$ then both side of the equality become of order $\mathrm{o}(|x_{l,n}|)$ and cancel each other, hence the equality is satisfied.

3. $\max\{i,j\} = l$ and $\min\{i,j\} = 0$. After canceling the identical terms and sending n to infinity $n \to \infty$ the equation becomes

$$(a_l + \overline{a_l}) x_{l,n} + o(|x_{l,n}|) = (b_l + \overline{b_l}) x_{l,n} + o(|x_{l,n}|).$$

   After dividing the equation by $x_{l,n}$ the remaining terms show $\mathrm{Re}(a_l)$=$\mathrm{Re}(b_l)$. Recall $\mathrm{Im}(a_l)$=$\mathrm{Im}(b_l)$, therefore a_l=b_l and the equation is satisfied.

Note that the equality of the imaginary parts plays an important role in the proof and the lemma is not correct without this condition. A supporting example is

$$a_1 = 3 + \sqrt{3}i, \quad a_2 = 3(\frac{1}{2} + \frac{\sqrt{3}}{2}i), \quad \text{and } b_1 = b_2 = 3.$$

Then $|1 + a_1x + a_2x^2| = |1 + b_1x + b_2x^2|$ for all real x, particularly when $x \to 0$.

To prove Part B, one needs to consider that $\{x_{i,n}\}$ is non-zero. Since $x_{0,n} = 1$, then $a_0 = 0$. Next, for simplicity, let's normalize the sequence by $x_{1,n}$, then the sum becomes

$$|\sum_{i=1}^{k} a_i x_{i,n}/x_{1,n}| = |a_1 + a_2x_{2,n}/x_{1,n} + \ldots| = 0.$$

therefore a_1=0. By induction it is clear that $a_i = 0$.

□

Here we have enough tools to prove lemma 8.8.

Lemma 1. *If we are not dealing with* EVAL$(\mathbf{C}, \mathfrak{D})$*#P-hard, then rank*$(\mathbf{D})$ *is at most 1, and if* $\mathbf{D}_{i,j} \neq 0$ *and* $\mathbf{D}_{i,j'} \neq 0$ *then* $|\mathbf{D}_{i,j}| = |\mathbf{D}_{i,j'}|$ $\forall i \in [s]$ *and* $j, j' \in [h]$.

Proof. To proof this lemma consider an undirected graph $G = (V, E)$ where we substitute every edge in $uv \in E$, by the gadget shown in the following figure (Figure 4 of the paper).

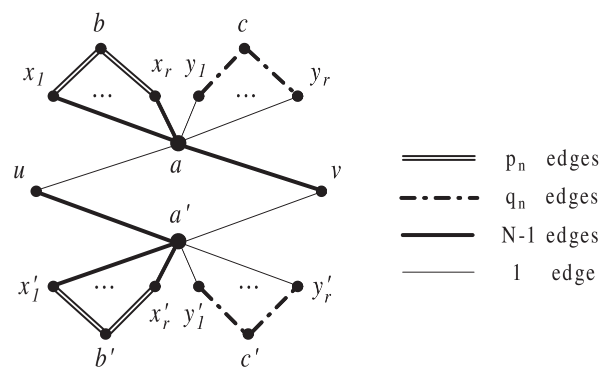

Figure 1: The gadget for constructing $G^{[n]}$. Note that the node a is connected to $2r$ nodes in top and the nodes u and v in bottom. These nodes are connected to the conjugate of a as well. Hence swapping u and v does not change the gadget; a symmetric graph.

Some properties of the graph G:
The node b in this graph is connected to $x_{1:r}$ via the function $p_n = n^2N + 1 \equiv 1(N)$ and the node c is connected to $y_{1:r}$ via $g_n = Nn - 1 \equiv -1(N)$ $(\forall r \geq 1)$. One observation could be comparing these functions as $n \to \infty$, which yields to $p_n > q_n$. Later we will use the fact that

$deg(b) \equiv r(N)$ and $deg(c) \equiv -r(N)$, which means they are conjugate of each other. When we pass this graph to our partition function Z, one needs to consider all the assignments to u and v and moreover computes the collaborations of the virtual vertices. By taking advantage of the symmetry of G, we can construct a matrix $\mathbf{R}$ such that

$$Z_{\mathbf{R}^{[n]},\mathfrak{D}^*}(G) = Z_{\mathbf{C},\mathfrak{D}}(G^{[n]})$$
$$\Rightarrow \mathsf{EVAL}(\mathbf{R}^{[n]},\mathfrak{D}^*) \leq \mathsf{EVAL}(\mathbf{C},\mathfrak{D}) \quad \text{so } \mathsf{EVAL}(\mathbf{R}^{[n]},\mathfrak{D}^*) \text{ is not \#P-hard.}$$

Note that the matrix $\mathbf{R}$ has the same dimension as $\mathbf{C}$ but with opposite shape, therefore

$$\mathbf{R}^{[0]} = \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}.$$

Because of the shape of $\mathbf{R}$ we have

$$\mathbf{R}^{[n]}_{(0,u),(1,v)} = \mathbf{R}^{[n]}_{(1,u),(0,v)} = 0, \quad \forall u \in I, v \in J.$$

The entries of $\mathbf{R}$ are as follows:

$$\mathbf{R}^{[n]}_{(1,u),(1,v)} = \left(\sum_{a,b,c \in I_{[s]\times[h]}} (\mathbf{I})^r (\mathbf{II})^r F_{a,u} F^{N-1}_{a,v} \mathbf{D}^{[0]}_{(0,a)} \mathbf{D}^{[r]}_{(0,b)} \mathbf{D}^{[N-r]}_{(0,c)} \right)$$
$$\times \left(\sum_{a,b,c \in I_{[s]\times[h]}} (\mathbf{I})^r (\mathbf{II})^r F^{N-1}_{a,u} F_{a,v} \mathbf{D}^{[0]}_{(0,a)} \mathbf{D}^{[r]}_{(0,b)} \mathbf{D}^{[N-r]}_{(0,c)} \right), \forall u,v \in J_{[t]\times[h]}$$

Where

$$\mathbf{I} : \sum_{x \in J} F^{N-1}_{(a,x)} F^{p_n}_{(b,x)} \mathbf{D}^{[0]}_{(1,x)} = \mu^{N-1}_{a_1} \mu^{p_n}_{b_1} \sum_{x \in J} \nu^{N-1}_{x_1} \nu^{p_n}_{x_1} \mathbf{H}^{N-1}_{a_2,x_2} \mathbf{H}^{p_n}_{b2,x2} \mathbf{D}^{[0]}_{(1,(x_1,1))}$$

Note that $\mathbf{H}_{a_2,x_2}$ are roots of unity so we can get the conjufate $\mathbf{H}^{N-1}_{a_2,x_2} = \overline{\mathbf{H}_{a_2,x_2}}$. And also $p_n \equiv 1(N)$ then $\mathbf{H}^{p_n}_{b2,x2} = \mathbf{H}_{b2,x2}$. Therefore

$$\mathbf{I} = \mu^{N-1}_{a_1} \mu^{p_n}_{b_1} \sum_{x_1 \in [t]} \nu^{N-1+p_n}_{x_1} \mathbf{D}^{[0]}_{(1,(x_1,1))} < \mathbf{H}_{a_2,*}, \mathbf{H}_{b_2,*} >$$

$$< \mathbf{H}_{a_2,*}, \mathbf{H}_{b_2,*} > = \begin{cases} h & a_2 = b_2 \\ 0 & \text{O/W} \end{cases}$$

$$\text{Let } L = h \cdot \sum_{x_1 \in [t]} \nu^{N-1+p_n}_{x_1} \mathbf{D}^{[0]}_{(1,(x_1,1))}$$

$$\mathbf{I} = \mu^{N-1}_{a_1} \mu^{p_n}_{b_1} L, \text{ where } L \text{ is independent of } u,v,a,b,c, \text{ and also } L > 0.$$

And the the $\mathbf{II}$ term can be written as

$$\mathbf{II} : \sum_{y \in J} F_{a,y} F^{q_n}_{c,y} \mathbf{D}^{[0]}_{(1,y)} = L' \mu_{a_1} \mu^{q_n}_{c_1} \quad \forall a_1 = c_1.$$

The L' term is defined like L as a sum on h, ν, and D and is a positive term.
Next, to simplify $\mathbf{R}$, we need to define some notations and keep in mind that (from $Shape_3$) $\mathbf{D}^{N-r}_{(0,c)} = \overline{\mathbf{D}^{[r]}_{(0,c)}} = \overline{\mathbf{D}_{c1,c2}}$. In addition, from the $\mathbf{H}$'s dot products in the definitions of $\mathbf{I}$ and $\mathbf{II}$, we only consider $\mathbf{R}$ entries in which $u_1 = v_1 = 1$, hence we can denote $\mathbf{R}_{u,v} = \mathbf{R}_{(1,(1,u)),(1,(1,v))}$.
Let $P_n = rp_n$, $Q_n = rq_n$, and

$$Z = \sum_{a_1 \in [s]} (L \cdot \mu_{a_1}^{N-1})^r (L' \cdot \mu_{a_1})^r \mu_{a_1}^N \mathbf{D}^{[0]}_{(0,(a_1,1))}.$$

Therefore (note that $\nu = 1$):

$$R_{u,v} = Z^2 \left(\sum_{b,c \in [s]} \mu_b^P \mu_c^Q \sum_{a \in [h]} \mathbf{D}_{b,a} \overline{\mathbf{D}_{c,a}} \mathbf{H}_{a,u} \overline{\mathbf{H}_{a,v}} \right) \left(\sum_{b',c' \in [s]} \mu_{b'}^P \mu_{c'}^Q \sum_{a \in [h]} \mathbf{D}_{b',a} \overline{\mathbf{D}_{c',a} \mathbf{H}_{a,u}} \mathbf{H}_{a,v} \right).$$

Note that we normalize ν's and μ's based on ν_1 and μ_1 respectively:

$$\nu_1 = 1 > \ldots > \nu_{[t]} \text{ and } \mu_1 = 1 > \ldots > \mu_{[s]}.$$

Next we want to work on the magnitude of μ and stratify the sum based on these orders. Notice that $\mu_b^P \mu_c^Q \mu_{b'}^P \mu_{c'}^Q = (\mu_b \mu_{b'})^P (\mu_c \mu_{c'})^Q$. These terms are first ordered based on $\mu_b \mu_{b'}$ and then $\mu_c \mu_{c'}$ (recall that as $n \to \infty P > Q$). Therefore we define the order over a set $\mathcal{T}$,

$$\mathcal{T} = \left\{ T = \begin{pmatrix} b & c \\ b' & c' \end{pmatrix} | b, b', c, c' \in [s] \right\}.$$

Where

$T_1 \equiv_\mu T_2$ iff $(\mu_{b1}\mu_{b1'} = \mu_{b2}\mu_{b2'})$ and $(\mu_{c1}\mu_{c1'} = \mu_{c2}\mu_{c2'})$
$T_1 \leq_\mu T_2$ If either $(\mu_{b1}\mu_{b1'} < \mu_{b2}\mu_{b2'})$ or $(\mu_{b1}\mu_{b1'} = \mu_{b2}\mu_{b2'}$ and $\mu_{c1}\mu_{c1'} \leq \mu_{c2}\mu_{c2'})$

Based on this definition we can see

$$\begin{aligned}
\mathcal{T}_1 &= \left\{ T_1 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \right\} \\
\mathcal{T}_2 &= \left\{ T_1 = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, T_2 = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix} \right\} \\
&\ldots,
\end{aligned}$$

therefore we can divide $\mathcal{T}$ into classes $\mathcal{T}_1, \mathcal{T}_2, \ldots \mathcal{T}_d$, from the largest to the smallest order. Having this definition, we can rewrite the $\mathbf{R}$ as follows:

$$\mathbf{R}_{u,v} = Z^2 \sum_{i \in [d]} U_i^P W_i^Q \sum_{T \in \mathcal{T}_i} X_{u,v,T},$$

where

$$\begin{aligned}
U_i &= \mu_b \mu_{b'} \\
W_i &= \mu_c \mu_{c'} \\
X_{u,v,T} &= \left(\sum_{a \in [h]} \mathbf{D}_{b,a} \overline{\mathbf{D}_{c,a}} \mathbf{H}_{a,u} \overline{\mathbf{H}_{a,v}} \right) \left(\sum_{a \in [h]} \mathbf{D}_{b',a} \overline{\mathbf{D}_{c',a} \mathbf{H}_{a,u}} \mathbf{H}_{a,v} \right).
\end{aligned}$$

Therefore, when $u = v$ the $\mathbf{H}$ terms cancel each other out and one can get

$$\frac{\mathbf{R}_{u,u}}{Z^2} = |\sum_{b,c \in [s]} \sum_{a \in [h]} \mathbf{D}_{1,a} \overline{\mathbf{D}_{1,a}}|^2 U_1^P W_1^Q.$$

This means the coefficient of the leading term $U_1^P W_1^Q$ is $\|\mathbf{D}_{1,*}\|^4$. Next a question arises that whether $\mathbf{D}_{a,*} = 0$ or not? Consider the case where the equality is correct, then μ_1 must be 0 and we can start the process from μ_2. On the other hand, if $\mathbf{D}_{1,*} \neq 0$ and its coefficient is sufficiently big, then $\mu_2, \ldots$ do not matter. Hence, the other terms become zero for sufficiently large n.

Next we are going to use the vanishing lemma on the matrix $\mathbf{R}$ and show that all the non-zero terms of D must have the same norm.

(The proof will be continued). □