CS 880: Complexity of Counting Problems April 17, 2012

Lecture 23: Towards Proving $\mathcal{U}_5$

Instructor: Jin-Yi Cai Scribe: Aaron Gorenstein

Today we will begin proving $\mathcal{U}_5$, which is on page 24 in the paper. Our goal is to prove this main theorem:

Theorem 1 (Condition $\mathcal{U}_5$) For all $r \in [N-1]$ and $i \in [0:2m-1]$, $D_i^{[r]}$ is either 0 or a power of ω_N.

Recall $\mathcal{U}_1$–$\mathcal{U}_4$ (page 23). Matrix $\mathbf{A}$ is purified, and there is a sequence of diagonal matrices $\mathbf{D}$ indexed according to the degree of the vertex mod N, where N is some fixed even number. With these, $\mathbf{C}$ is the bipartisation of the M-discrete unitary matrix $\mathbf{F} \in \mathbb{C}^{n\times n}$ (note that $\mathbf{C}$ and $\mathbf{F}$ uniquely determine each other). And importantly, recall that $D_i^{[0]} = 1$ for some i, and that $D^{[0]}$ is all integers.

We currently know that

$$D_i^{[r]} \in \mathbb{Q}(\omega_N), \text{ and } \left|D_i^{[r]}\right| = 0 \text{ or } 1. \tag{1}$$

Our goal will be to show that $D_i^{[r]}$ are all powers of the same ω_n. We want this so that the entries can all be powers of the same base, so their product is a sum of their exponents. Then it becomes a polynomial evaluation problem.

Recall our current partition function:

$$Z = \sum_{\sigma: V\to[m]} \prod_{e=(u,v)} C_{\sigma(u),\sigma(v)} \prod_{v\in V} D_{\sigma(v)}^{[deg(v) \bmod N]}. \tag{2}$$

We already know that C is made of powers of ω_n, now we will make D also powers of ω_n. It is sufficient to instead show that $D_i^{[r]}$ is a root of unity.

1 Interlude from last lecture: Group Condition

Recall that

$$X_{ij} = \{\left|\langle F_{i,\star} \circ \overline{F_{j,\star}}, F_{a,\star} \circ \overline{F_{b,\star}}\rangle\right|\}. \tag{3}$$

We also define $S_{ij}(x) =$ the number of times x appears in X_{ij}. So we see that $\sum S_{ij}(x) = m^2$, and

$$\sum S_{ij}(x) \cdot x^{2p} = m^{2p+1}, \tag{4}$$

following from the idea that the matrix determinant must be 0. For $x \in X_{ij}$, as $p = 1, 2, \ldots, p$ need only go up to $|X_{ij}| - 1$.

In other words,

$$\begin{bmatrix} 1 & 1 & \ldots & 1 \\ x_1^2 & x_2^2 & \ldots & x_{|X_{ij}|}^2 \\ x_1^4 & x_2^4 & \ldots & \ldots \\ \vdots & \vdots & \vdots & \ddots \end{bmatrix} \begin{bmatrix} S_{ij}(x_1) \\ S_{ij}(x_2) \\ S_{ij}(x_3) \\ \vdots \end{bmatrix} \tag{5}$$

and recall that by definition all x are distinct and non-negative, so their squares are different. That means we have set up a Vandermonde system!

Such a system has a single solution, and we will ultimately guess it. We want to pick a value such that all of the equations are satisfied. We know that $0 \in X_{ij}$ and $m \in X_{ij}$. We get 0 by setting $a = i, b \neq j$ in equation (3) and noting that F is orthogonal. We get m by setting $a = i, b = j$, and with their conjugates we get a sum of 1 for the inner product, and there are m of them.

Let Z_{ij} be a function similar to S_{ij}, but we define it such that $Z_{ij}(0) = m^2 - m$ and $Z_{ij}(m) = m$. Every other parameter is set to 0 (if any exist!). Considering Z for S in our equation (4) defining the Vandermonde system, we see that it works! So we have correctly guessed the unique solution.

Aside The approach to concluding this is not unlike the proof showing log space is equal to co-log space. You guess, and realize that in guessing you've covered everything, and so you're done! This method is surprising: until the proof, most thought log space was not equal to co-log space!

We are not yet there with the group action. Consider $j = 0$, we can rewrite the right-hand-side of (3) as follows:

$$\sum_{a=0}^{m-1} |\langle F_{i,\star} \circ F_{b,\star}, F_{a,\star} \rangle|^2 . \tag{6}$$

We can view the inner product as expanding the left-hand-side vector on the Fourier basis of the right-hand-side. This is a generalization of Pythagoras's inequality. The summation is equal to $m \cdot \|F_{i,\star} \circ F_{b,\star}\|^2$. All of the vectors involved, though, become 1, so we get m^2.

So how can equation (6), a sum of m, m^2 be equal to m^2? The only way is if there is exactly one m! We now know it is the case that

$$\forall i \forall x \exists a \, |\langle F_{i,\star} \circ F_{b,\star}, F_{a,\star} \rangle| = m.$$

Now consider how all of the values in that vector or roots of unity of length 1. For them all to sum to 1, they *must* point in the same direction. So the two vectors we are inner-producting over differ, element-wise, by a fixed θ. In other words,

$$F_{a,\star} = e^{i\theta} \cdot (F_{i,\star} \circ F_{b,\star}). \tag{7}$$

Look at the first entry, and we can set it to 1. The equation (7) becomes $1 = \theta \cdot 1 \cdot 1$, so $\theta \equiv 0 \mod 2\pi$. Thus we have our group condition! Now we return to determining the composition of $D_i^{[r]}$.

2 Proving Lemma 9.2

We begin by proving a sufficient condition for our main theorem:

Lemma 1 (Lemma 9.2) Showing $D_i^{[r]}$ is a root of unity is sufficient to show theorem 1.

Proof. Let $D = \omega_M^k$, such that $(k, M) = 1$ (here parens means the gcd). Now we know that $(M, N) = a \cdot N + b \cdot M$. With some arithmetic, we can conclude that $\frac{1}{\text{lcm}} = \frac{a}{M} + \frac{b}{N}$. The term lcm is the least common multiple of M and N.

Observe:

$$e^{2\pi i \frac{1}{\text{lcm}}} = \omega_{\text{lcm}(M,N)} = e^{2\pi i \frac{a}{M}} \cdot e^{2\pi i \frac{b}{N}} = \omega_M^a \cdot \omega_N^b.$$

This is a formal verification of the idea that, if you have a pie, and can modify some size-$\frac{1}{x}$ portion, or some size-$\frac{1}{y}$ portion, you can modify a $\frac{1}{xy}$ portion.

So we have $\omega_{\text{lcm}} \in \mathbb{Q}(D, \omega_N)$. With $D = \omega_M^k$, and k relatively prime (so $a'k + b'M = 1$), we see that

$$\omega_M = \omega'_M = \omega_M^{a'k+b'M}, \text{ but it is mod M, } = (\omega_M^k)^{a'}$$

We conclude that $\omega_{\text{lcm}} \in \mathbb{Q}(\omega_M, \omega_N) = \mathbb{Q}(\omega_{\text{lcm}})$. Here we invoke an external theorem, the fact that $[\mathbb{Q}(\omega_N) : \mathbb{Q}] = \phi(n)$. By ϕ we mean Euler's totient function. This statement basically means that the cyclotomic polynomial is irreducible, e.g.:

$$x^7 - 1 = (x - 1)(x^6 + x^5 + \ldots + x + 1), \tag{8}$$

or $\Phi_7(x)$, is irreducible.

More generally we define

$$\Phi_n(x) = \prod_{\substack{K=1\ldots N \\ \gcd(K,N)=1}} (x - \omega_N^K). \tag{9}$$

It is true that $\Phi_n(x) \in \mathbb{Q}[x]$ and the degree is the totient of n. If $n = p_1^{e_1} p_2^{e_2} \ldots$, its prime factorization, we can define the totient. Recall that the totient is $n \cdot \prod_{p|n}(1 - \frac{1}{p}) = p_1^{e_1}(1 - \frac{1}{p})p_2^{e_2} \ldots$. Note that if n is odd, it

has the same totient as $2n$, because it merely adds a 1 factor to the totient. If we have $2^{e_k>1}$, however, the value does change.

$$\mathbb{Q}(\omega_N) = \mathbb{Q}(\omega_M, \omega_N) = \mathbb{Q}(\omega_{\text{lcm}})$$

then

$$\mathbb{Q}(\omega_N) = \mathbb{Q}(\omega'_N) \implies N \mid N'$$

so we conclude

$$\phi(N) = \phi'(N).$$

Given the above, only these two cases are possible: if N is odd, then $N = N'$ or $N = 2N'$. The extra 2 factor is allowed, because the "first one" doesn't change ϕ. Otherwise, if N is even, $N = N'$, that's it. Recall that we designed N to be even. This is why! The two values must be equal, and we have finished our lemma. □

Now we need "just" to show that $D_i^{[r]}$ is *some* root of unity. To do so, we'll introduce a lemma without proof. For $K = \{i \in [0, m-1] | D_i \neq 0\}$, we fix some r, $D_i = D_{m+i}^{[r]}$. So we're really considering the second part of the bipartisation. Now, showing $D_i^{[r]}$ is a root of unity. If $|K| = 0$ we're done. If $|K| = 1$ recall there must be at least one 1, so that element must be 1, and we're done. We assume, then, that $|K| \geq 2$. We define a vector $z = (D_0^N, D_1^N, \ldots, D_{m-1}^N)$.

Lemma 2 If $\exists k \in K$ s.t. $Z_k (= D_k^N)$ is *not* a root of unity, then there exists a sequence $\{P_n\}$ such that when $n \to \infty$ (note $Z_k^{P_n} : k \in K$) approaches to all 1, but never equal to it. But there is a time when all the values are "really close".

For example, with a vector of length 3, after $n^3 + 1$ steps, 2 of the elements in the vector must be close to 1. This is a multidimensional version of the box principle of Dirichlet, which is described as follows. Say we want to minimize $\left|\alpha - \frac{n}{m}\right|$ where $m < M$ for some fixed α, M. An easy answer is $\frac{1}{m}$. Some more thought gives us $\frac{1}{2m}$. The box principle says that we can always get $\leq \frac{c}{M^{3/2}}$, for a universal constant c. Hint: consider $1 \cdot \alpha, 2 \cdot \alpha, 3 \cdot \alpha$, etc. The multidimensional version says that you can get within $\frac{c}{M^{1+\frac{1}{k}}}$.

Now consider page 71 of the paper, figure 6. That is an edge gadget, and we've seen similar applications before. We will create:

$$A_{u,v}^{[p]} = \text{ by Bulatov-Grohe } = L_p \cdot \left(\sum_{k \in K} D_k^{pN} F_{u,k} \overline{F_{v,k}}\right)\left(\sum_{k \in K} D_k^{pN} \overline{F_{u,k}} F_{v,k}\right) \forall u, v \in [0 \ldots m-1] \tag{10}$$

We will pick up around the argument form the middle of page 72 to the end. Remember in particular the sentence before the word "Assume": it describes the proof by contradiction we will show next time.