CS 2429 - Foundations of Communication Complexity

Lecture #9: 10 November 2009

Lecturer: Matei David

Scribe Notes by: Matei David

1 Nondeterministic vs. Randomized NOF Protocols

Recall from last time:

Definition 1 (Lifted function)**.** *Let $m := n^\epsilon$ for a small constant ϵ determined later. Given a* base function $f : \{0,1\}^m \to \{-1,+1\}$*, and a* selection function $\phi : \{0,1\}^{kn} \to \binom{[n]}{m}$*, we define the* lifted function $\mathrm{Lift}\,(f,\phi) : \{0,1\}^{(k+1)n} \to \{-1,+1\}$ *by*

$$\mathrm{Lift}\,(f,\phi)\,(x,y_1,\ldots,y_k) := f(x|\phi(y_1,\ldots,y_k)).$$

We want to compute $\mathrm{Lift}\,(f,\phi)$ *using $(k+1)$-player NOF protocols, where player 0 has x on its forehead, and player $i > 0$ has y_i on its forehead.*

Fact 1. $\forall \phi, \qquad N(\mathrm{Lift}\,(\mathrm{OR},\phi)) \le \log n + 1$*, so* $\mathrm{Lift}\,(\mathrm{OR},\phi) \in \mathsf{NP}^{\mathrm{cc}}_k$*, for all k.*

Our goal is to show that: if $k = k(n) < \delta \cdot \log n$ for a fixed $\delta < 1$ and sufficiently large n, there exists an α such that for *some* ϕ, $R(\mathrm{Lift}\,(\mathrm{OR},\phi)) > n^\alpha$. As we have seen last time, to get the lower bound above it is enough to show that there exists a distribution λ such that $\mathrm{corr}_\lambda\left(\mathrm{Lift}\,(\mathrm{OR},\phi), \Pi^{n^\alpha}\right) < 1/3$.

By [4, 3], there exists a constant γ, a function $g : \{0,1\}^m \to \{-1,+1\}$, and a distribution μ on $\{0,1\}^m$, such that

- $\mathrm{corr}_\mu\,(\mathrm{OR}, g) \ge 5/6$
- and $\mathrm{corr}_\mu\,(g, \chi_S) = 0$ for all S with $|S| < \gamma \cdot \sqrt{m}$.

Furthermore, let λ be the distribution on $\{0,1\}^{(k+1)n}$ defined by

$$\lambda(x,y_1,\ldots,y_k) := \frac{2^m \mu(x|\phi(y_1,\ldots,y_k))}{2^{(k+1)n}}.$$

Fact 2.

$$\mathrm{corr}_\lambda\left(\mathrm{Lift}\,(\mathrm{OR},\phi), \mathrm{Lift}\,(g,\phi)\right) = \mathrm{corr}_\mu\,(\mathrm{OR}, g)\,.$$

We have seen that $d(f,g) = 1 - \mathrm{corr}\,(f,g)$ is a distance, so by the triangle inqeuality,

Fact 3.

$$\begin{aligned}\mathrm{corr}_\lambda\left(\mathrm{Lift}\left(\mathrm{OR},\phi\right),\Pi^c\right) &\le \mathrm{corr}_\lambda\left(\mathrm{Lift}\left(g,\phi\right),\Pi^c\right) + \left(1-\mathrm{corr}_\lambda\left(\mathrm{Lift}\left(\mathrm{OR},\phi\right),\mathrm{Lift}\left(g,\phi\right)\right)\right)\\ &= \mathrm{corr}_\lambda\left(\mathrm{Lift}\left(g,\phi\right),\Pi^c\right) + \left(1-\mathrm{corr}_\mu\left(\mathrm{OR},g\right)\right)\\ &\le \mathrm{corr}_\lambda\left(\mathrm{Lift}\left(g,\phi\right),\Pi^c\right) + 1/6.\end{aligned}$$

Thus, to obtain the upper bound on $\mathrm{corr}_\lambda\left(\mathrm{Lift}\left(\mathrm{OR},\phi\right),\Pi^c\right) < 1/3$, it is enough to obtain the upper bound $\mathrm{corr}_\lambda\left(\mathrm{Lift}\left(g,\phi\right),\Pi^c\right) < 1/6$. For the latter, we use the following connection between correlation and discrepancy, along with the regular discrepancy method of [1].

Fact 4 ([5])**.**

$$\mathrm{corr}_\lambda\left(F,\Pi^c\right) \le 2^c \cdot \mathrm{disc}_\lambda(F).$$

Fact 5 ([1])**.** *For every function $f : \{0,1\}^{(k+1)n} \to \mathbb{R}$ and for every cylinder intersection $T \subseteq \{0,1\}^{(k+1)n}$,*

$$\left(\mathop{\mathrm{E}}_{x,\bar{y}}\left[f(x,\bar{y})\cdot 1_T(x,\bar{y})\right]\right)^{2^k} \le \mathop{\mathrm{E}}_{\bar{y}^0,\bar{y}^1}\left[\left|\mathop{\mathrm{E}}_{x}\left[\prod_{u\in\{0,1\}^k} f\left(x,\bar{y}^u\right)\right]\right|\right],$$

where we write $\bar{y}^u$ for $(y_1^{u_1}, y_2^{u_2}, \ldots, y_k^{u_k})$.

Putting these facts together, we get:

Claim 6.

$$\left(\mathrm{corr}_\lambda\left(\mathrm{Lift}\left(g,\phi\right),\Pi^c\right)\right)^{2^k} \le 2^{(c+m)2^k}\cdot \mathop{\mathrm{E}}_{\bar{y}^0,\bar{y}^1}\left[\left|\mathop{\mathrm{E}}_{x}\left[\prod_{u\in\{0,1\}^k}(\mu\cdot g)(x|\phi(\bar{y}^u))\right]\right|\right].$$

Proof of Claim 6.

$$\begin{aligned}\mathrm{corr}_\lambda\left(\mathrm{Lift}\left(g,\phi\right),\Pi^c\right) &\le 2^c\cdot\mathrm{disc}_\lambda\left(\mathrm{Lift}\left(g,\phi\right)\right) && \text{(by Fact 4)}\\ &= 2^c\cdot\left|\mathop{\mathrm{E}}_{(x,\bar{y})\sim\lambda}\left[\left(\mathrm{Lift}\left(g,\phi\right)\cdot 1_T\right)(x,\bar{y})\right]\right|,\end{aligned}$$

where T is the cylinder intersection witnessing the discrepancy of $\mathrm{Lift}\left(g,\phi\right)$ under λ,

$$\begin{aligned}&= 2^c\cdot\left|\sum_{x,\bar{y}}\left(\lambda\cdot\mathrm{Lift}\left(g,\phi\right)\cdot 1_T\right)(x,\bar{y})\right|\\ &= 2^c\cdot\left|\sum_{x,\bar{y}}\frac{(\mu\cdot g)(x|\phi(\bar{y}))}{2^{(k+1)\cdot n-m}}\cdot 1_T(x,\bar{y})\right|,\end{aligned}$$

where we have used the definitions of λ and $\mathrm{Lift}\left(g,\phi\right)$,

$$= 2^{c+m}\cdot\left|\mathop{\mathrm{E}}_{x,\bar{y}}\left[(\mu\cdot g)(x|\phi(\bar{y}))\cdot 1_T(x,\bar{y})\right]\right|.$$

We are now in a position to apply the version of the [1] argument given as Fact 5, obtaining:

$$\left(\mathrm{corr}_\lambda\left(\mathrm{Lift}\left(g,\phi\right),\Pi^c\right)\right)^{2^k} \le 2^{(c+m)\cdot 2^k} \mathop{\mathrm{E}}_{\bar{y}^0,\bar{y}^1}\left[\left|\mathop{\mathrm{E}}_{x}\left[\prod_{u\in\{0,1\}^k}(\mu\cdot g)(x|\phi(\bar{y}))\right]\right|\right].\square$$

We also use the following notation:

Definition 2. *Let $\mathcal{S}=(S_1,\ldots,S_z)$ be a multiset of m-element subsets of $[n]$. Let the* range of $\mathcal{S}$, *denoted by $\bigcup\mathcal{S}$, be the set of indices from $[n]$ that appear in at least one set in $\mathcal{S}$. Let the* boundary of $\mathcal{S}$, *denoted by $\partial\mathcal{S}$, be the set of indices from $[n]$ that appear in exactly one set in the collection $\mathcal{S}$.*

For $\bar{y}^0=(y_1^0,\ldots,y_k^0),\bar{y}^1=(y_1^1,\ldots,y_k^1)\in\{0,1\}^{kn}$, and for $u\in\{0,1\}^k$, define $S_u(\bar{y}^0,\bar{y}^1,\phi):=\phi(y_1^{u_1},\ldots,y_k^{u_k})$. Let $\mathcal{S}(\bar{y}^0,\bar{y}^1,\phi)$ be the multiset $\left(S_u:u\in\{0,1\}^k\right)$. We define the number of conflicts in $\mathcal{S}$ *to be $q(\mathcal{S}):=m\cdot 2^k-|\bigcup\mathcal{S}|$. We write S_u for $S_u(\bar{y}^0,\bar{y}^1,\phi)$ and $\mathcal{S}$ for $\mathcal{S}(\bar{y}^0,\bar{y}^1,\phi)$.*

The crux of the argument is that, while for every ϕ, $\mathrm{Lift}\left(\mathrm{OR},\phi\right)\in\mathsf{NP}^{\mathrm{cc}}_k$, when ϕ is a *random selection function*, $\mathrm{Lift}\left(\mathrm{OR},\phi\right)\notin\mathsf{BPP}^{\mathrm{cc}}_k$. Formally, we claim that:

$$\mathop{\mathrm{E}}_{\phi}\left[\mathrm{corr}_\lambda\left(\mathrm{Lift}\left(g,\phi\right),\Pi^c\right)\right]<1/6.$$

To prove this, we first expand the bound above as follows:

$$\begin{aligned}
\left(\mathop{\mathrm{E}}_{\phi}\left[\mathrm{corr}_\lambda\left(\mathrm{Lift}\left(g,\phi\right),\Pi^c\right)\right]\right)^{2^k} &\le \mathop{\mathrm{E}}_{\phi}\left[\left(\mathrm{corr}_\lambda\left(\mathrm{Lift}\left(g,\phi\right),\Pi^c\right)\right)^{2^k}\right]\\
&\le \mathop{\mathrm{E}}_{\phi}\left[2^{(c+m)\cdot 2^k}\mathop{\mathrm{E}}_{\bar{y}^0,\bar{y}^1}\left[\left|\mathop{\mathrm{E}}_{x}\left[\prod_{u\in\{0,1\}^k}(\mu\cdot g)(x|\phi(\bar{y}^u))\right]\right|\right]\right]\\
&= 2^{(c+m)\cdot 2^k}\cdot\mathop{\mathrm{E}}_{\phi,\bar{y}^0,\bar{y}^1}\left[\left|\mathop{\mathrm{E}}_{x}\left[\prod_{u\in\{0,1\}^k}(\mu g)(x|S_u)\right]\right|\right]\\
&= 2^{(c+m)\cdot 2^k}\cdot\sum_{q\ge 0}\Pr\left[q(\mathcal{S})=q\right]\cdot\mathrm{E}\left[\left|\mathop{\mathrm{E}}_{x}\left[\prod_{u}(\mu g)(x|S_u)\right]\right|\,\middle|\,q(\mathcal{S})=q\right]
\end{aligned}$$

Above, both the probability and the outter expected value are taken over the choice of a uniformly random selection function ϕ, and uniformly random input vectors $\bar{y}^0$ and $\bar{y}^1$.

We analyze the sum in three steps.

First, we claim that when the number of conflicts in $\mathcal{S}$ is small enough, some set S_v has such a small intersection with the other sets S_u, that the second property in the definition of g (the fact that it is orthogonal to all Fourier characters of all sets) kicks in and allows us to conclude that the contribution of those terms to the sum is 0.

Lemma 7. *For every $\bar{y}^0,\bar{y}^1$ and ϕ, if $q(\mathcal{S}(\bar{y}^0,\bar{y}^1,\phi))<\gamma\cdot\sqrt{m}\cdot 2^k/2$, then*

$$\mathop{\mathrm{E}}_{x}\left[\prod_{u\in\{0,1\}^k}(\mu g)(x|S_u(\bar{y}^0,\bar{y}^1,\phi))\right]=0.$$

Proof of Lemma 7. Let $r(\mathcal{S}) = |\bigcup \mathcal{S}|$ be the size of the range of $\mathcal{S}$, and let $b(\mathcal{S}) = |\partial\mathcal{S}|$ be the size of the boundary of $\mathcal{S}$. Note that $r(\mathcal{S}) - b(\mathcal{S}) \leq q(\mathcal{S})$ because every $j \in \cup\mathcal{S} \setminus \partial\mathcal{S}$ occurs in at least 2 sets in $\mathcal{S}$, thus contributes at least 1 to $q(\mathcal{S})$. Furthermore, $r(\mathcal{S}) + q(\mathcal{S}) = m \cdot 2^k$. Then, $\sum_{u\in\{0,1\}^k} |S_u \cap \partial\mathcal{S}| = b(\mathcal{S}) \geq r(\mathcal{S}) - q(\mathcal{S}) = m \cdot 2^k - 2 \cdot q(\mathcal{S}) > (m - \gamma\sqrt{m})2^k$. By the pigeonhole principle, there exists v such that $|S_v \cap \partial\mathcal{S}| > m - \gamma\sqrt{m}$. We can write

$$\mathop{\mathrm{E}}_{x}\left[\prod_{u\in\{0,1\}^k}(\mu\cdot g)(x|S_u)\right] = \mathop{\mathrm{E}}_{x|S_v}\left[(\mu\cdot g)(x|S_v)\cdot \mathop{\mathrm{E}}_{x|[n]\setminus S_v}\left[\prod_{u\neq v}(\mu\cdot g)(x|S_u)\right]\right].$$

Let $T = S_v \setminus \partial\mathcal{S}$. So $|T| \leq \gamma\sqrt{m}$. Let $h := \mathrm{E}_{x|[n]\setminus S_v}\left[\prod_{u\neq v}(\mu\cdot g)(x|S_u)\right]$. Since h depends only on $x|T$, by Property (ii) of g and μ, $\mathrm{E}_{x|S_v}\left[(\mu\cdot g)(x|S_v)\cdot h(x|T)\right] = 0$. □

Second, we claim a general bound for every q. This does not depend on g at all, only on the fact that μ is a probability distribution.

Lemma 8. *For every $\bar{y}^0, \bar{y}^1$ and ϕ:*

$$\mathop{\mathrm{E}}_{x}\left[\prod_{u\in\{0,1\}^k}\mu(x|S_u(\bar{y}^0,\bar{y}^1,\phi))\right] \leq \frac{2^{q(\mathcal{S}(\bar{y}^0,\bar{y}^1,\phi))}}{2^{m\cdot 2^k}}.$$

Third, we have the point where the random choice of ϕ comes into play:

Lemma 9. *For every $q > 0$ and uniformly chosen $\bar{y}^0, \bar{y}^1, \phi$:*

$$\Pr_{\bar{y}^0,\bar{y}^1,\phi}\left[q(\mathcal{S}(\bar{y}^0,\bar{y}^1,\phi)) = q\right] \leq \left(\frac{m^3\cdot 2^{2k}}{q\cdot n}\right)^q.$$

Proof sketch of Lemma 9. Assume that for every $1 \leq i \leq k$, $y_i^0 \neq y_i^1$. Then, all 2^k points $\bar{y}^u$ where ϕ is evaluated are distinct. In this case, the multiset $\mathcal{S}$ consists of 2^k random m-element subsets of $[n]$.

If these were chose *with* replacement (i.e., for each set: pick m elements of $[n]$ with replacement), the probability of obtaining q conflicts in $\mathcal{S}$ is at most:

$$\binom{m\cdot 2^k}{q}\cdot\left(\frac{m\cdot 2^k}{n}\right)^q \leq \left(\frac{e\cdot m^2\cdot 2^{2k}}{qn}\right)^q$$

To see this: the binomial coefficient is the number of ways to get q conflicts out of the total 2^k (sets) times m (elements per set) draws; the range of the elements picked so far is always at most $m \cdot 2^k$; so the probability for each conflict is at most $m \cdot 2^k/n$.

Of course, the sets are in fact picked *without* replacement, but a similar bound holds.

This takes care of the case when $y_i^0 \neq y_i^1$ for all i. If any of these are equal, the 2^k points where ϕ is evaluated are no longer distinct. However, by a union bound, this happens with probability at most $k/2^n$.

Adding these two terms we get the bound stated in the Lemma. □

By standard algebraic manipulations, we get

$$\left(\mathop{\mathrm{E}}_{\phi}\left[\mathrm{corr}_{\lambda}\left(\mathrm{Lift}\left(g,\phi\right),\Pi^{c}\right)\right]\right)^{2^{k}} \leq 2^{c\cdot 2^{k}} \sum_{q\geq\gamma\sqrt{m}2^{k}/2} \left(\frac{4}{\gamma}\cdot n^{\frac{5\epsilon}{2}-(1-\delta)}\right)^{q},$$

where we have used $k < \delta\cdot\log n$ and $m = n^{\epsilon}$. Setting $\epsilon := \frac{1-\delta}{5}$,

$$\leq 2^{c\cdot 2^{k}+1-\frac{\gamma\sqrt{m}2^{k}}{2}}$$

For $\alpha := \epsilon/4$ and $c := n^{\alpha}$,

$$\leq 2^{2^{k}(n^{\alpha}-(\gamma/2)\cdot n^{\varepsilon/2})}.$$

Therefore, for all large enough n, there is some ϕ such that $\mathrm{corr}_{\lambda}\left(\mathrm{Lift}\left(g,\phi\right),\Pi^{c}\right) < 1/6$. As discussed before, this implies $\mathrm{Lift}\left(\mathrm{OR},\phi\right) \notin \mathsf{BPP}_{k}^{\mathrm{cc}}$.

2 Deterministic vs. Randomized NOF Protocols

Here, we give a brief overview of the following related class separation:

Theorem 10 ([2])**.** $\mathsf{P}_{k}^{\mathrm{cc}} \neq \mathsf{RP}_{k}^{\mathrm{cc}}$ *for* $k \leq n^{O(1)}$.

Consider the class of functions $\mathcal{G} = \left\{g : \{0,1\}^{kn} \to \{0,1\}^{m}\right\}\left\{g : \{0,1\}^{kn} \to \{0,1\}^{m} \;\middle|\; \right\}$ for some $m \leq n$. For every $g \in \mathcal{G}$, consider the *graph function* $f^{g} : \{0,1\}^{(k+1)n} \to \{0,1\}$ defined by $f^{g}(x,\bar{y}) = 1$ if and only if $x = g(\bar{y})\circ 0^{n-m}$. Observe that, for every $\bar{y}$ input to players $1,\ldots,k$, there is a unique value for the x input of player 0 such that $f(x,\bar{y}) = 1$.

Lemma 11. *For every* g, $f^{g} \in \mathsf{coRP}_{k}^{\mathrm{cc}}$.

Proof. Consider the following protocol: player 0, seeing $\bar{y}$, computes $x^{*} = g(\bar{y})\circ 0^{n-m}$; then, players 0 and 1 run an equality testing protocol with inputs x^{*} and x, respectively. This costs $O\left(\log n\right)$ in the private coin model, and it has only false-positives error. □

Our goal is now to show that for *some* g, $f^{g} \notin \mathsf{P}_{k}^{\mathrm{cc}}$. We do this using a counting argument. The key property which allows us to give the upper bound needed in the counting argument is the following "normal form" property.

Lemma 12. *Let* g *be a function in* $\mathcal{G}$*, and let* π *be a deterministic protocol for* f^{g} *with cost* c*. Then, there exists another deterministic protocol* π' *for* f^{g}*, which works as follows:*

- *player 0 first sends* c *bits;*
- *players 1 through* k *simultaneously send 1 bit each;*
- *the output of* π' *is 1 iff all "check" bits send in the second stage are 1.*

Proof sketch. We describe π'. Player 0, seeing $\bar{y}$, computes the unique value $x^* = g(\bar{y}) \circ 0^{n-m}$ for which $f^g(x^*, \bar{y}) = 1$. Then, player 0 communicates the entire transcript τ of π on input $(x^*, \bar{y})$. Now each other player $i > 0$ checks inductively that τ is consistent with its own view on the real input $(x, \bar{y})$ to π'. That is, for every bit τ_j that would have been communicated by player i in π, player i checks that τ_j is the value it would have communicated seeing the previous communication $\tau_1, \ldots, \tau_{j-1}$ and the real input $(x, y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_k)$. It is easy to see that all players 1 through k agree with τ iff $x = x^*$, and hence, iff $f^g(x, \bar{y}) = 1$. □

Observe that π' has slightly higher cost π: $c + k$ vs. c. However, the interaction between the players is much more limited in π' than in π, and this allows us to describe a protocol of the type of π' very efficiently. The crux of the counting argument is that, when $c \simeq n/2$, $m \simeq n/2$, and $k \leq n^{O(1)}$, there are *more* functions $g \in \mathcal{G}$ than there are deterministic protocols of cost c for graph functions f^g. Hence, for all large enough n, *some* graph function f^g has complexity more than c, placing it outside $\mathsf{P}^{\mathrm{cc}}_k$.

References

[1] L. Babai, N. Nisan, and M. Szegedy, *Multiparty protocols, pseudorandom generators for logspace, and time-space trade-offs*, J. Comput. Syst. Sci., 45 (1992), pp. 204–232. 2, 3

[2] P. Beame, M. David, T. Pitassi, and P. Woelfel, *Separating deterministic from nondeterministic nof multiparty communication complexity*, in 34th International Colloquium on Automata, Languages and Programming (ICALP), Springer, 2007, pp. 134–145. 5

[3] N. Nisan and M. Szegedy, *On the degree of boolean functions as real polynomials*, Computational Complexity, 4 (1994), pp. 301–313. 1

[4] A. Sherstov, *The pattern matrix method for lower bounds on quantum communication*, in 40th Annual Symposium on the Theory of Computing (STOC), ACM Press, 2008, pp. 85–94. 1

[5] E. Viola and A. Wigderson, *Norms, XOR lemmas, and lower bounds for GF(2) polynomials and multiparty protocols*, Theory of Computing, 4 (2008), pp. 137–168. 2