# 27. Multiparty communication complexity of disjointness

*Lecturer: Jaikumar Radhakrishnan* *Scribe: Swagato Sanyal*

In this lecture we shall derive a lower bound on multiparty communication complexity of the Disjointness problem, in the "Number on forehead" model introduced in the last lecture. Recall that earlier we proved lower bound of the complexity of the same problem in "Number in hand" model.

## 27.1 Multiparty Set Disjointness Problem

We have a universe $[n]$ and we have $k$ subsets of the universe $b_1, \ldots, b_k$, each given as a bit vector of size $n$. In such a bit vector, the $i$-th entry is 1 *iff* the element $i$ is a member of that set. There are $k$ players, and $b_i$ is the input to $i$-th player. According to our model, each player $i$ has access to every $b_j$ such that $j \neq i$. The goal is to decide whether the intersection of $b_1, \ldots, b_k$ is non-empty.

$$\mathsf{DISJ}_{\mathsf{n},\mathsf{k}}(b_1, \ldots, b_k) = \begin{cases} 1 & (\text{if } \cap_{i=1}^{k} b_i = \varphi) \\ 0 & (\text{otherwise}) \end{cases}$$

In this lecture we shall prove the following theorem by Sherstov:

**Theorem 27.1.** $R_{1/3}(\mathsf{DISJ}_{\mathsf{n},\mathsf{k}}) = \Omega\left(\frac{n}{4^k}\right)^{\frac{1}{4}}$.

We will move to the $-1, +1$ world from the $0, 1$ world. Thus $-1$ and $+1$ will stand for 1 and 0 respectively. For proving the above theorem we shall use the following claim without proof. $\mathsf{AND}_\mathsf{n}$ is the $n$ variable logical AND function.

**Claim 27.2.** *There exists a constant $\delta_0 > 0$ such that any polynomial that $1/3$-approximates $\mathsf{AND}_\mathsf{n}$ has degree at least $\delta_0\sqrt{n}$.*

For any function $g$, let $deg_\delta(g)$ denote the degree of a polynomial with least degree which $\delta$-approximates $g$. The broad idea of the proof is showing that if there is a cheap communication protocol for multiparty disjointness, then there is a low degree polynomial that closely approximates $\mathsf{AND}_\mathsf{n}$.
For some $r$, define a function $F : \{0,1\}^{nrk} \longrightarrow \{0,1\}$ as follows. Think of the input as $n$ matrices, each of dimension $r \times k$. Treat each matrix as an input to $\mathsf{DISJ}_{\mathsf{r},\mathsf{k}}$. Apply the function $\mathsf{DISJ}_{\mathsf{r},\mathsf{k}}$ to each matrix to get one bit for each of them. Finally define $F$ to be the logical AND of those bits. Note that $F$ is actually disjointness with $k$ players and a larger universe. Let $deg_\delta(\mathsf{AND}_\mathsf{n}) = d_\delta$. We will prove the following theorem:

**Theorem 27.3.**

$$\forall \varepsilon, \delta \geq 0, 2^{R_\varepsilon(F)} \geq (\delta - 2\varepsilon)\left(\frac{d_\delta\sqrt{r}}{2^k en}\right)^{d_\delta}.$$

## 27.2 Proof of Theorem 27.3

Let $\Pi$ be a $\varepsilon$-error randomized protocol for $F$. Let $\mu_{r,k}^{+1}$ and $\mu_{r,k}^{-1}$ be two distributions (to be fixed later) on $\{0,1\}^{rk}$ supported on negative and positive instances of $\mathsf{DISJ_{r,k}}$ respectively. Let $\mu = \frac{\mu_{r,k}^{+1}+\mu_{r,k}^{-1}}{2}$. We obtain a randomized process for computing $\mathsf{AND_n}$ from $\Pi$ as follows: Given $n$ bits $z_1, \cdots, z_n$ (by bits we mean $+1, -1$ values), we draw $\mathsf{DISJ_{r,k}}$ instances $X_1, \cdots, X_n$ from probablity distributions $\mu_{r,k}^{z_1}, \ldots, \mu_{r,k}^{z_n}$ respectively. Clearly $\Pi(X_1, \cdots, X_n) = AND(X_1, \cdots, X_n)$ with probability at least $1-\varepsilon$. Let $P(z_1, \ldots, z_n)$ be the expected value computed by the randomized process on inputs $z_1, \cdots, z_n$ (the expectation is over the random choices that the process makes). Let $\sum_{S\subseteq[n]} \gamma_S . \prod_{i\in S} z_i$ be the Fourier expansion of $P(z_1, \cdots, z_n)$. For each $S \subseteq [n]$, $\gamma_S$ is $E_{z_1\sim U\{0,1\},\cdots,z_n\sim U\{0,1\}}[P(z_1, \ldots, z_n)\Pi_{i\in S} z_i]$. Let $\Pi(X)$ be the expected output of $\Pi$ on $X$. Check that,

$$\gamma_S = E_{X_1\sim\mu,\cdots,X_n\sim\mu}[\Pi(X_1, \cdots, X_n) \prod_{i\in S} \mathsf{DISJ_{r,k}}(X_i)] \tag{27.2.1}$$

In the last lecture we saw that in NOF model, each leaf of the protocol tree of any deterministic protocol corresponds to intersection of $k$ cylinders. The $i$-th cylinder is a set of inputs, where the membership does not depend on the $i$-th input. For every cylinder intersection $\mathcal{K}$, let $\mathcal{K}()$ denote the indicator function of membership in $\mathcal{K}$. Let $\mathcal{C}$ be the set of all cylinder intersections of a deterministic protocol $\Psi$. Then $\Psi$ can be written as:

$$\Psi(X) = \sum_{\mathcal{K}\in\mathcal{C}} a_{\mathcal{K}}\mathcal{K}(X)$$

where $X$ is the input to the protocol, and $a_{\mathcal{K}}$ is the output (i.e. a $+1/-1$ value) of $\Psi$ when $X$ belongs to the cyliner intersection $\mathcal{K}$. Since a randomized protocol's output is a probability distribution over outputs of some deterministic protocols, we can write

$$\Pi(X) = \sum_{\mathcal{K}\in\mathcal{C}} a_{\mathcal{K}}\mathcal{K}(X)$$

where $\Pi(X)$ is the expected output of $\Pi$ on $X$, and $a_{\mathcal{K}}$ is the expected output of $\Pi$ when $X$ is in $\mathcal{K}$. Both expectations are over internal randomizations of $\Pi$. $a_{\mathcal{K}}$ is a real between $-1$ and $+1$, and $\sum_{\mathcal{K}} |a_{\mathcal{K}}| \leq 2^c$, where $c$ is the communication complexity of $\Pi$. Thus from 27.2.1 we have

$$\gamma_S = \sum_{\mathcal{K}\in\mathcal{C}} a_{\mathcal{X}} E_{X_1\sim\mu,\cdots,X_n\sim\mu}[\mathcal{X}(X_1, \cdots, X_n) \prod_{i\in S} \mathsf{DISJ_{r,k}}(X_i)]$$

Now we will analyze how well does the polynomial $\sum_{S\subseteq[n],|S|<d_\delta} \gamma_S . \Pi_{i\in S} z_i$ approximate $P(z_1, \cdots, z_n)$. Let the error on input $z_1, \cdots, z_n$ resulted because of dropping all monomials with degree greater than $d_\delta$ be $\varepsilon'(z_1, \cdots, z_n)$. Then,

$$\varepsilon'(z_1, \cdots, z_n) = \sum_{\mathcal{X}\in\mathcal{C}} \sum_{S\subseteq[n],|S|\geq d_\delta} a_{\mathcal{X}} E_{X_1\sim\mu,\cdots,X_n\sim\mu}[\mathcal{X}(X_1, \cdots, X_n) \prod_{i\in S} \mathsf{DISJ_{r,k}}(X_i)] \prod_{i\in S} z_i$$

$$\leq \sum_{\mathcal{X}\in\mathcal{C}} \sum_{S\subseteq[n],|S|\geq d_\delta} a_{\mathcal{X}} E_{X_1\sim\mu,\cdots,X_n\sim\mu}[\mathcal{X}(X_1,\cdots,X_n)\prod_{i\in S}\mathsf{DISJ}_{\mathsf{r},\mathsf{k}}(X_i)]$$

$$\leq \sum_{\mathcal{X}\in\mathcal{C}} |a_{\mathcal{X}}| \sum_{S\subseteq[n],|S|\geq d_\delta} |E_{X_1\sim\mu,\cdots,X_n\sim\mu}[\mathcal{X}(X_1,\cdots,X_n)\prod_{i\in S}\mathsf{DISJ}_{\mathsf{r},\mathsf{k}}(X_i)]|$$

To bound this sum, we use a lemma which we will prove in the next lecture. Let $\alpha(s) = \left(\frac{2^{k-1}}{\sqrt{r}}\right)^s$.

**Lemma 27.4.** *There exist distributions $\mu_{r,k}^{+1}$ and $\mu_{r,k}^{-1}$, such that for all $S \subseteq [n]$ with $|S| = s$,*

$$|E_{X_1\sim\mu,\cdots,X_n\sim\mu}[\mathcal{X}(X_1,\cdots,X_n)\Pi_{i\in S}\mathsf{DISJ}_{\mathsf{r},\mathsf{k}}(X_i)]| \leq \alpha(s).$$

For the choice of $\mu_{r,k}^{+1}$ and $\mu_{r,k}^{-1}$ given by the lemma, this gives us

$$\varepsilon'(z_1,\cdots,z_n) \leq \sum_{\mathcal{X}} |a_{\mathcal{X}}| \sum_{s=d}^{n} \alpha(s).\binom{n}{s}$$

$$\leq \sum_{\mathcal{X}} |a_{\mathcal{X}}| \sum_{s=d}^{n} \left(\frac{2^{k-1}.en}{\sqrt{r}s}\right)^s$$

$$\leq \sum_{\mathcal{X}} |a_{\mathcal{X}}| \sum_{s=d}^{n} \left(\frac{2^{k-1}.en}{\sqrt{r}d}\right)^s$$

If $\frac{2^{k-1}.en}{\sqrt{r}d} < 1$ the sum is geometrically decreasing, and hence bounded above by $2^c\left(\frac{2^k.en}{\sqrt{r}d}\right)^d$. If $\frac{2^{k-1}.en}{\sqrt{r}d} \geq 1$, the quantity $2^c\left(\frac{2^k.en}{\sqrt{r}d}\right)^d$ is at least 1 and hence bounds the error from above. We know that the randomized process approximates AND within error $\varepsilon$. So the expected output of the randomized process (denoted by $P()$) is within an additive error of $2\varepsilon$ of $\mathsf{AND}_\mathsf{n}$. Thus the above polynomial approximates AND within error $2\varepsilon + 2^c\left(\frac{2^k.en}{\sqrt{r}d}\right)^d$. But since the polynomial is of degree less than $d_\delta$, it should not approximate AND better than $\delta$. This gives us

$$2\varepsilon + 2^c\left(\frac{2^k.en}{\sqrt{r}d}\right)^d \geq \delta$$

$$\Rightarrow 2^c > (\delta - 2\varepsilon)\left(\frac{d_\delta\sqrt{r}}{2^k en}\right)^{d_\delta}$$

This proves Theorem 27.3.

## 27.3 Proof of Theorem 27.1

Putting $\delta = 1/3$ gives us $d_\delta \geq \delta_0\sqrt{n}$ (claim 27.2). Take $r = 4^k n$. From Theorem 27.1

$$2^{R_{1/9}(F)} = 2^{\Omega(\sqrt{n})}.$$

Note that $F$ is disjointness on inputs of size $N = 4^k n^2$. Thus,

$$2^{R_{1/9}(F)} = 2^{\left(\frac{N}{4^k}\right)^{1/4}}.$$

This proves Theorem 27.1 as we can improve the error from 1/3 to 1/9 by increasing communication by a constant factor.