# 26. Multiparty Communication – NOF model

*Lecturer: Prahladh Harsha* *Scribe: Fahad Panolan*

Today, we discuss multiparty communication complexity where the goal is for $k$ parties to evaluate a function defined of on $k$ inputs and these inputs are distributed among $k$ players. We have already seen one instance of multiparty communication – the NIH (number-in-hand) model wherein the input is partitioned among the $k$ players. Today, we will focus on a different model - the NOF (number-on-forehead) model and discuss lower bound techniques for this model. In the NOF model, the input is *not* partitioned among the $k$ players as in the NIH model, but there is considerable overlap in the distribution of inputs. The references for today's lecture include Sections 6.1–6.4 of Kushilevitz-Nisan's book [KN97].

## 26.1 The multiparty model

Let $f$ be a Boolean function defined on $k$ inputs.

$$f : X_1 \times X_2 \times \cdots \times X_k \to \{0, 1\}.$$

We will typically consider domains $X_i$ of the form $\{0, 1\}^n$. The Input $(x_1, x_2, \ldots, x_k)$ is distributed among the $k$ players $A_1, \ldots, A_k$ and they need to compute $f(x_1, x_2, \ldots, x_k)$ by communicating amongst themselves. We will restrict ourselves to the broadcast (also called blackboard) model of communication, i.e any message sent by any player is seen by all players. No two (or less than $k$) players can have a private conversation amongst themselves. This is modeled as follows: each player writes it's message on a black board which is seen by all players. Hence, the name blackboard model. The communication cost is the total number of bits written in the black board.

There are two commonly considered models depending on how the $k$ inputs is distributed among the $k$ players. The obvious generalization of the two-party model is to partition the inputs among the players, this is the number-in-hand (NIH) model. That is, in NIH model, player $A_i$ gets input $x_i$. Observe that the lower bounds in the two-party case naturally extend to the NIH model. In fact, one expects even better lower models as the number of player grows. As observed in the earlier lectures, this aspect of the NIH model is useful for proving lower bound for streaming algorithms. A different and non-obvious generalization of the two party case is the number-in-forehead (NOF) model. In the NOF model, player $A_i$ gets as input $(x_1, x_2, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k)$, i.e player $A_i$ knows all parts of the input except co-ordinate $x_i$. In some sense, $x_i$ is printed on the forehead of player $A_i$, a player can see what is written on other players' foreheads but not his own forehead. The NOF model abstracts situations in which the input is distributed among various parties and there is overlap of information amongst the $k$ players. Observe that in the two party case, the NOF and NIH model are equivalent. We will use the notation $\mathrm{D}^k(f), \mathrm{R}^k(f)$ to denote the deterministic and randomized communication cost of the $k$-party protocol to compute $f$ (the model NOF or NIH will be clear from context).

Due to the overlap, most of the lower bound techiques for the two-party case do not extend to the NOF model unlike the NIH model. In fact, the only known lower bound technique in the NOF model is the discrepancy bound. In general, the NOF model is not as well understood as the two-party case and lower bounds seem to be harder to obtain in this case.

Overlap of information in NOF model helps to reduce communication cost. Consider the function $\mathsf{EQ}_n^k$, which is equal to 1 iff all the $k$ inputs are equal (ie., $x_1 = x_2 = \cdots = x_k$). We know that $\mathrm{D}(\mathsf{EQ}_n^2) = n + 1$ for the two party case. On the other hand, for $k \geq 3$, $\mathrm{D}^k(\mathsf{EQ}_n^k) \leq 2$: Player 1 writes 1 if $x_2 = x_3 = \cdots = x_n$ and player 2 writes 1 if $x_1 = x_3$.

Recall that in the two party communication, any determnistic protocol can be thought of as binary tree where the internal nodes are labeled by the two players and the leaves by the outputs and the depth of the tree is the cost of the protocol. The multiparty deterministic protocol (in both the NIH and NOF models) can be similarly be thought as binary trees where each internal node is labeled by one of the $k$ players and the leaves are labeled with 0 or 1. As before, The cost of the protocol is the depth of the tree. In NIH model, if an internal node is labeled by player $i$, then one of the two edges (which is labeled 0 or 1) is selected based on a function depending only on $x_i$ whereas in the NOF model this function is defined on $(x_1, x_2, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$, ie., all but the $i^{th}$ part of the input.

In the 2-party case, a protocol partitions the input space into rectangles. In the NIH model, rectangles are replaced with cubes while in the case of NOF model rectagles are replaced with more complicated objects, called "cylinder intersections"

### 26.1.1 Cylinder intersections

**Definition 26.1** (cylinder, cylinder intersection)**.** *$S \subseteq X_1 \times X_2 \times \cdots \times X_k$ is a cylinder in axis i if*

$$(x_1, x_2, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_k) \in S \implies \forall x_i' \in X_i, (x_1, x_2, \ldots, x_{i-1}, x_i', x_{i+1}, \ldots, x_k).$$

*A subset $S$ is called a cylinder intersection if it can be represented as an intersection of cylinders (in any axis), i.e, $S = \cap_{i=1}^k S_i$ where $S_i$ is a cylinder in axis $i$*[1].

It is easy to check that the set of inputs that reach a particular leaf in a deterministic NOF protocol from a cylinder intersection. Sometimes cylinder intersections are specified via the equivalent star formulation.

**Definition 26.2** (star property)**.** *A star in $X_1 \times X_2 \times \cdots \times X_k$ is a set of $k$ points of the form $(x_1', x_2, \ldots, x_k)$, $(x_1, x_2', \ldots, x_k), \cdots, (x_1, x_2, \ldots, x_k')$ where for each $i$, $x_i, x_i' \in X_i$. The point $(x_1, x_2, \ldots, x_k)$ is called the center of the star (note that center does not necessarily belongs to star).*

*A set $S$ satisfies the* star property *if*

$$\forall i, x_i, x_i' \in X_i, \left((x_1', x_2, \ldots, x_k), (x_1, x_2', \ldots, x_k), \ldots, (x_1, x_2, \ldots, x_k') \in S \implies (x_1, x_2, \ldots, x_k) \in S.\right).$$

*I.e, for every star $S$ contains, $S$ also contains its center.*

[1]Here, we have used the fact that intersections of cylinders in the same axis is a cylinder (in the same axis).

**Lemma 26.3.** *A set $S$ is a cylinder intersection iff $S$ satisfies the star property.*

*Proof.* $(\Rightarrow)$ : Let $S$ be a cylinder intersection. i.e, $S = \cap_{i=1}^{k} S_i$ where $S_i$ is a cylinder in axis $i$. Assume $S$ contains a star $(x'_1, x_2, \ldots, x_k), (x_1, x'_2, \ldots, x_k), \ldots, (x_1, x_2, \ldots, x'_k)$.

$$\begin{aligned}
&\Rightarrow \quad \forall i, \quad (x_1, x_2, \ldots, x'_i, \ldots, x_k) \in S_i \\
&\Rightarrow \quad \forall i, \quad (x_1, x_2, \ldots, x_i, \ldots, x_k) \in S_i \qquad (\because S_i \text{ is a cylinder in axis } i) \\
&\Rightarrow \quad (x_1, x_2, \ldots, x_i, \ldots, x_k) \in S
\end{aligned}$$

$(\Leftarrow)$ : Asuume $S$ satisfies star property. Define the set

$$S_i = \{(x_1, x_2, \ldots, x_i, \ldots, x_k) | \exists x'_i \in X_i, (x_1, x_2, \ldots, x'_i, \ldots, x_k) \in S\}.$$

By definition $S_i$ is a cylinder in axis $i$. We will show that if $S$ satisfies star property then $S = \cap_i S_i$. $S \subseteq \cap_i S_i$ is true from the definition of $S_i$. Consider a point $(x_1, x_2, \ldots, x_i, \ldots, x_k) \subseteq \cap_i S_i$. Then $\forall i, \exists x'_i$ such that $(x_1, x_2, \ldots, x'_i, \ldots, x_k) \in S$ (from the definition of $S_i$). This set of $k$ points is a star in $S$, which implies $(x_1, x_2, \ldots, x_i, \ldots, x_k)$ is also in $S$ $\square$

**Cylinder intersection property** A deterministic multiparty communication (NOF model) protocol of cost $C$ partitons the input space into cylinder intersections and since the depth of the tree is at most $C$, there are at most $2^C$ disjoint cylinder intersections in this partition.

## 26.2 Randomized multiparty protocols

A (public coins) randomized multiparty protocol is, as in the 2-party case, a distribution over deterministic protocols. Thus, a public coins multiparty protocol of cost $C$ can be modeled as a distribution over protocol trees where each tree partitions the input space into at most $2^C$ disjoint cylinder intersections. Yao's characterization of randomized communication cost in terms of distributional communication cost also extends to the multiparty setting.

**Theorem 26.4** (Yao's Theorem)**.** $\mathrm{R}_\varepsilon^k(f) = \max_\mu \mathrm{D}_\varepsilon^{\mu,k}(f)$.

Here, $\mathrm{D}_\varepsilon^{\mu,k}(f)$ denotes the communication cost of the best deterministic $k$-party protocol that makes error on at most $\varepsilon$ fraction of the inputs according to the distribution $\mu$.

### 26.2.1 Discrepancy Lower Bound for NOF model

Recall that the discrepancy of a set $S$ is defined as

$$\begin{aligned}
\mathrm{disc}_\mu(f; S) &= \left| \Pr_{x \sim \mu}\left[f(x) = 1 \wedge x \in S\right] - \Pr_{x \sim \mu}\left[f(x) = 0 \wedge x \in S\right] \right| \\
&= \left| \sum_{x \in S} \mu(x) \cdot (-1)^{f(x)} \right|.
\end{aligned}$$

We will denote $\mu(x) \cdot (-1)^{f(x)}$ by $\psi(x) = \psi_{f,\mu}(x)$. Thus, $\mathrm{disc}_\mu(f; S) = |\sum_{x \in S} \psi(x)|$.

The only lower bound techinque from the 2-party case that generalizes to the multiparty case is the discrepency method.Analogous to the theorem in two party communication complexity we have the following theorem

**Theorem 26.5.**

$$\mathrm{D}^{\mu,k}_{\frac{1}{2}-\varepsilon}(f) \geq \log\left(\frac{2\varepsilon}{\mathrm{disc}^k_\mu(f)}\right),$$

*where* $\mathrm{disc}^k_\mu(f) = \max_S \mathrm{disc}_\mu(f;S)$ *where the maximum is taken over all* $k$*-cylinder intersections* $S$*.*

Proof of this theorem is very similer to the proof in the case of 2-party case. Here cylinder intersections replaces rectangles.

The discrepancy bound proved in Lecture 24 for the 2-party case has a natural multiparty generalization.

**Lemma 26.6.** *Let* $f : X_1 \times, \ldots, \times X_k \to \{0,1\}$ *and* $\mu$ *be a distribution on input space. Then*

$$\left(\frac{\mathrm{disc}^k_\mu(f)}{|X_1|\cdot\cdots\cdot|X_k|}\right)^{2^{k-1}} \leq \mathop{\mathbb{E}}_{\substack{x_1^0\in X_1\\ x_1^1\in X_1}} \mathop{\mathbb{E}}_{\substack{x_2^0\in X_2\\ x_2^1\in X_2}} \cdots \mathop{\mathbb{E}}_{\substack{x_{k-1}^0\in X_{k-1}\\ x_{k-1}^1\in X_{k-1}}} \left| \mathop{\mathbb{E}}_{x_k\in X_k} \prod_{z\in\{0,1\}^{k-1}} \psi(x_1^{z_1}, x_2^{z_2}, \ldots, x_{k-1}^{z_{k-1}}, x_k)\right|.$$

Proof is similer to the proof of discrepancy bound lemma in the 2-part case. Here we need to apply Cauchy-Schwartz inequality $k-1$ times.

*Proof.* Let $S = \cap_{i=}^k S_i$ be the cylinder intersection such that $\mathrm{disc}^k_\mu(f) = \mathrm{disc}_\mu(f;S)$. Define $k$ random variables $\alpha_1, \ldots, \alpha_k : X_1 \times \cdots \times X_k \to \{\pm 1\}$ based on the $k$ cylinders $S_i$'s as follows.

$$\alpha_i(x) = \begin{cases} 1 & \text{if } x \in S_i, \\ \pm 1 & \text{with equal probability if } x \notin S_i. \end{cases}$$

Observe that $\alpha_i$ is independent of $x_i$, i.e., $\alpha_i(x_1, \ldots, x_k) = \alpha_i(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k) = \alpha_i(x_{-i})$. It follows from the definitions that $\mathrm{disc}^k_\mu(f) = \left|\mathbb{E}\left[\sum_{x\in\prod_{i=1}^k X_i} \psi(x)\cdot\prod_{i=1}^k \alpha_i(x)\right]\right|$ where the expectation is over the random $\alpha_i$. We now choose the functions $\alpha_i$'s such that

$$\mathrm{disc}^k_\mu(f) \leq \left|\left[\sum_{x\in\prod_{i=1}^k X_i} \psi(x)\cdot\prod_{i=1}^k \alpha_i(x)\right]\right|.$$

Rewriting the summation in terms of an expectation, we have

$$\left(\frac{\mathrm{disc}^k_\mu(f)}{|X_1|\cdot\cdots\cdot|X_k|}\right) \leq \left|\mathop{\mathbb{E}}_{x_1\in X_1}\cdots\mathop{\mathbb{E}}_{x_k\in X_k}\left[\psi(x_1,\ldots,x_k)\cdot\prod_{i=1}^k \alpha_i(x_1,\ldots,x_k)\right]\right|.$$

Applying Jenson's inequality $k-1$ times and observing that $\alpha_i$ is independent of $x_i$ and

$(\alpha_i(x))^2 = 1$, we have

$$
\begin{aligned}
&\left(\frac{\mathrm{disc}_\mu^k(f)}{|X_1|\cdot\dots\cdot|X_k|}\right)^{2^{k-1}} \\
\leq\;& \left(\mathop{\mathbb{E}}_{x_k}\mathop{\mathbb{E}}_{x_{k-1}}\cdots\mathop{\mathbb{E}}_{x_2}\mathop{\mathbb{E}}_{x_1}\left[\psi(x_1,\dots,x_k)\cdot\prod_{i=1}^{k}\alpha_i(x_1,\dots,x_k)\right]\right)^{2^{k-1}} \\
\leq\;& \mathop{\mathbb{E}}_{x_k}\left(\mathop{\mathbb{E}}_{x_{k-1}}\cdots\mathop{\mathbb{E}}_{x_1}\left[\psi(x_1,\dots,x_k)\cdot\prod_{i=1}^{k}\alpha_i(x_1,\dots,x_k)\right]\right)^{2^{k-1}} \\
\leq\;& \mathop{\mathbb{E}}_{x_k}\left(\mathop{\mathbb{E}}_{x_{k-1}}\left(\mathop{\mathbb{E}}_{x_{k-2}}\cdots\mathop{\mathbb{E}}_{x_1}\left[\psi(x_1,\dots,x_k)\cdot\prod_{i=1}^{k}\alpha_i(x_1,\dots,x_k)\right]\right)^{2^{k-2}}\right)^{2} \\
\leq\;& \mathop{\mathbb{E}}_{x_k}\left(\mathop{\mathbb{E}}_{x_{k-1}}\left(\mathop{\mathbb{E}}_{x_{k-2}}\left(\mathop{\mathbb{E}}_{x_{k-3}}\cdots\mathop{\mathbb{E}}_{x_1}\left[\psi(x_1,\dots,x_k)\cdot\prod_{i=1}^{k}\alpha_i(x_1,\dots,x_k)\right]\right)^{2^{k-3}}\right)^{2}\right)^{2} \\
&\vdots \\
\leq\;& \mathop{\mathbb{E}}_{x_k}\left(\mathop{\mathbb{E}}_{x_{k-1}}\left(\cdots\left(\mathop{\mathbb{E}}_{x_2}\left(\mathop{\mathbb{E}}_{x_1}\left[\psi(x_1,\dots,x_k)\cdot\prod_{i=1}^{k}\alpha_i(x_1,\dots,x_k)\right]\right)^{2}\right)^{2}\cdots\right)^{2}\right)^{2} \\
=\;& \mathop{\mathbb{E}}_{x_k}\mathop{\mathbb{E}}_{x_{k-1}^0,x_{k-1}^1}\cdots\mathop{\mathbb{E}}_{x_1^0,x_1^1}\left[\prod_{z\in\{0,1\}^{k-1}}\left(\psi\left(x_1^{z_1},\dots,x_{k-1}^{z_{k-1}},x_k\right)\cdot\prod_{i=1}^{k}\alpha_i\left(x_1^{z_1},\dots,x_{k-1}^{z_{k-1}},x_k\right)\right)\right] \\
=\;& \mathop{\mathbb{E}}_{x_1^0,x_1^1}\cdots\mathop{\mathbb{E}}_{x_{k-1}^0,x_{k-1}^1}\left[\mathop{\mathbb{E}}_{x_k}\left[\prod_{z\in\{0,1\}^{k-1}}\psi\left(x_1^{z_1},\dots,x_{k-1}^{z_{k-1}},x_k\right)\right]\cdot\left(\prod_{z\in\{0,1\}^{k-1}}\alpha_k\left(x_1^{z_1},\dots,x_{k-1}^{z_{k-1}}\right)\right)\right] \\
\leq\;& \mathop{\mathbb{E}}_{x_1^0,x_1^1}\cdots\mathop{\mathbb{E}}_{x_{k-1}^0,x_{k-1}^1}\left|\mathop{\mathbb{E}}_{x_k}\left[\prod_{z\in\{0,1\}^{k-1}}\psi\left(x_1^{z_1},\dots,x_{k-1}^{z_{k-1}},x_k\right)\right]\right|
\end{aligned}
$$

Thus, proved.

$\square$

## 26.3 Generalized Inner Product

We will now consider a generalization of the inner product function to $k$ inputs and study its communication complexity in the NOF model. Recall, that $\mathsf{IP}(x_1, x_2)$ is the parity of the number of co-ordinates for which both $x_1$ and $x_2$ are 1. Generalized Inner Product (denoted by $\mathsf{GIP}$) is a natural extension of this to $k$ inputs: it is the parity of the number of co-ordinates in which all the $k$ inputs are 1. More precisely, if we consider the $k$ inputs

$(x_1, \ldots, x_k) \in \{0,1\}^{nk}$ as a $k \times n$ matrix whose rows are $x_1, x_2, \ldots, x_k$, then $\mathsf{GIP}_n^k$ is defined as

$$\mathsf{GIP}_n^k(x_1, x_2, \ldots, x_k) = \begin{cases} 1 & \text{if \# of all } 1s \text{ columns are odd} \\ 0 & \text{otherwise.} \end{cases}$$

It will be useful that $\mathsf{GIP}_n^k$ is given by the following expression.

$$\mathsf{GIP}_n^k(x_1, x_2, \ldots, x_k) = \sum_{j=1}^{n} \prod_{i=1}^{k} x_{ij} \pmod 2.$$

We begin with a surprising upper bound due to Grolmusz [Gro94] that improves with the number of players.

**Theorem 26.7** ($\mathsf{GIP}$ – upper bound [Gro94])**.** $\mathrm{D}^k(\mathsf{GIP}_n^k) = O\left(\frac{kn}{2^k}\right)$.

*Proof.* The input is considered as a $k \times n$ matrix. To begin with, the $k$ players divide the columns of matrix into blocks of size atmost $2^{k-1} - 1$. If we compute $\mathsf{GIP}$ for every block and then summ the results (mod 2), we get the required answer. Hence the communication cost will be $\frac{n}{2^{k-1}-1}$ times the cost for one block. Now consider the following protocol for a block.

Step 1 : Player 1 announces a vector $\alpha \in \{0,1\}^k$ which is not of the columns in the block as follows. Note that Player 1 needs to do this despite not knowing the first row. Consider player 1's restricted view of the block – a matrix with $k-1$ rows. Since, there are at most $2^{k-1} - 1$ columns in this matrix and and each column is a vector of $k-1$ bits, there is at least one vector of length $k-1$ which is not a column in the matrix formed by the $k-1$ rows in the block. Player 1 then extends this $k-1$ vector by putting 1 in the first co-ordinate to obtain a vector that is not of the columns in the block.

Step 2 : Now all players know a column $\alpha$ which is not in the block. If $\alpha = (1, \ldots, 1)$ then ouput 0. Otherwise $\alpha$ contains atleast one 0. Without loss of generality, assume $\alpha$ is in the form $(0, \ldots, 0, 1, \ldots, 1)$ , i.e, $l$ 0's followed by $k-l$ 1's (if this is not the case we re-permute the rows). Let $y_i$ be the number of column vectors of the form $(0, \ldots, 0, 1, \ldots, 1)$, i.e, $i$ 0's followed by $k-i$ 1's. Let $z_i$ be the number of columns of the form $(0, \ldots, 0, \star, 1, \ldots, 1)$, i.e, $i-1$ 0's followed by a $\star$ and $k-i$ 1's. Note that $z_i = y_{i-1} + y_i$ and $y_l = 0$ (because $\alpha (= y_l)$ is not a column in the block). Furthermore, Player $i$ knows the value of $z_i$. For each $i \in [l]$, Player $i$ announce $z_i \mod 2$. Given this, the players can now compute $y_0$.

Cost of the protocol is $O\left(\frac{kn}{2^k}\right)$, because $\mathsf{GIP}$ for a block have a cost of at most $2k$ bits. $\square$

We will now show a lower bound, due to Babai, Nisan and Szegedy [BNS92], which was proved prior to Grolmusz's result. This lower bound was later improved to $\Omega(n/2^k)$ by Chung and Tetali [CT93].

**Theorem 26.8** ($\mathsf{GIP}$ – lower bound [BNS92])**.** $R^k_{\frac{1}{2}-\varepsilon}(\mathsf{GIP}_n^k) \geq D^{\mathsf{unif},k}_{\frac{1}{2}-\varepsilon}(\mathsf{GIP}_n^k) = \Omega\left(\frac{n}{4^k} - \log\left(\frac{1}{\varepsilon}\right)\right)$

*Proof.* Let $\mu$ represent uniform distribution over inputs.
Let $\psi(x_1,\ldots,x_k) = (-1)^{\mathsf{GIP}^k_n(x_1,\ldots,x_k)}\mu(x_1,\ldots,x_k)$.
Due to discrepancy bound lemma 26.6,

$$\begin{aligned}
\left(\frac{\mathrm{disc}^k_\mu(\mathsf{GIP}^k_n)}{2^{nk}}\right)^{2^{k-1}} &\le \mathop{\mathbb{E}}_{\substack{x_1^0\in X_1\\ x_1^1\in X_1}} \mathop{\mathbb{E}}_{\substack{x_2^0\in X_2\\ x_2^1\in X_2}} \cdots \mathop{\mathbb{E}}_{\substack{x_{k-1}^0\in X_{k-1}\\ x_{k-1}^1\in X_{k-1}}} \left| \mathop{\mathbb{E}}_{x_k\in X_k} \prod_{z\in\{0,1\}^{k-1}} \psi(x_1^{z_1}x_2^{z_2}\ldots x_{k-1}^{z_{k-1}}x_k)\right| \\
&\le \frac{1}{(2^{nk})^{2^{k-1}}}\,\mathbb{E}\ldots\mathbb{E}\left|\mathop{\mathbb{E}}_{x_k\in X_k} \prod_{z\in\{0,1\}^{k-1}} (-1)^{\mathsf{GIP}^k_n(x_1^{z_1}x_2^{z_2}\ldots x_{k-1}^{z_{k-1}}x_k)}\right| \\
\textit{i.e,}\quad \left(\mathrm{disc}^k_\mu(\mathsf{GIP}^k_n)\right)^{2^{k-1}} &\le \mathbb{E}\ldots\mathbb{E}\left|\mathop{\mathbb{E}}_{x_k\in X_k}(-1)^{\sum_{z\in\{0,1\}^{k-1}}\sum_{j=1}^n\prod_{i=1}^{k-1}x_{ij}^{z_i}x_{kj}}\right| \\
&\le \mathbb{E}\ldots\mathbb{E}\left|\mathop{\mathbb{E}}_{x_k}\left[(-1)^T\right]\right| \\
\text{where}\qquad T &= \sum_{z\in\{0,1\}^{k-1}}\sum_{j=1}^n\prod_{i=1}^{k-1}x_{ij}^{z_i}x_{kj} \\
&= \sum_{j=1}^n x_{kj}\sum_{z\in\{0,1\}^{k-1}}\prod_{i=1}^{k-1}x_{ij}^{z_i} \\
&= \sum_{j=1}^n x_{kj}\prod_{i=1}^{k-1}(x_{ij}^0+x_{ij}^1) \\
\mathop{\mathbb{E}}_{x_k}\left[(-1)^T\right] &= \begin{cases} 0 & \text{if } \exists j \text{ such that } \prod_{i=1}^{k-1}(x_{ij}^0+x_{ij}^1)\neq 0 \pmod 2 \\ 1 & \text{otherwise}\end{cases}
\end{aligned}$$

$$\begin{aligned}
\Pr\left[\prod_{i=1}^{k-1}(x_{ij}^0+x_{ij}^1)\neq 0 \pmod 2 \text{ for a fixed } j\right] &= \frac{1}{2^{k-1}} \\
\Pr\left[\forall j\ \prod_{i=1}^{k-1}(x_{ij}^0+x_{ij}^1)= 0 \mod 2\right] &= \left(1-\frac{1}{2^{k-1}}\right)^n \\
\text{Therefore}\quad \left(\mathrm{disc}^k_\mu(\mathsf{GIP}^k_n)\right)^{2^{k-1}} &\le \left(1-\frac{1}{2^{k-1}}\right)^n \\
&\le e^{\frac{-n}{2^{k-1}}} \\
\text{Hence,}\quad \mathrm{disc}^k_\mu(\mathsf{GIP}^k_n) &\le e^{\frac{-n}{4^{k-1}}}
\end{aligned}$$

Hence $D^{\mathsf{unif},k}_{\frac{1}{2}-\varepsilon}(\mathsf{GIP}^k_n) = \Omega\left(\frac{n}{4^k}+\log\varepsilon\right)$ (due to Theorem 26.5).

Theorem 26.4 and Claim 26.8 implies $R^k_{\frac{1}{2}-\varepsilon}(\mathsf{GIP}^k_n) = \Omega\left(\frac{n}{4^k}+\log\varepsilon\right)$. $\square$

## References


[BNS92] László Babai, Noam Nisan, and Mario Szegedy. *Multiparty protocols, pseudorandom generators for logspace, and time-space trade-offs*. J. Computer and System Sciences, 45(2):204–232, 1992. (Preliminary version in *21st STOC*, 1989). doi:10.1016/0022-0000(92)90047-M.

[CT93] Fan R. K. Chung and Prasad Tetali. *Communication complexity and quasi randomness*. SIAM J. Discrete Math., 6(1):110–123, 1993. doi:10.1137/0406009.

[Gro94] Vince Grolmusz. *The BNS lower bound for multi-party protocols in nearly optimal*. Inf. Comput., 112(1):51–54, 1994. doi:10.1006/inco.1994.1051.

[KN97] Eyal Kushilevitz and Noam Nisan. *Communication Complexity*. Cambridge University Press, 1997. doi:10.2277/052102983X.