

Deterministic Lifting Theorems for One-Way Number-on-Forehead Communication

Guangxu Yang *

Jiapeng Zhang *

June 14, 2025

Abstract

Lifting theorems are one of the most powerful tools for proving communication complexity lower bounds, with numerous downstream applications in proof complexity, monotone circuit lower bounds, data structures, and combinatorial optimization. However, to the best of our knowledge, prior lifting theorems have primarily focused on the two-party communication.

In this paper, we propose a new lifting theorem that establishes connections between the *two-party* communication and the *Number-on-Forehead (NOF)* communication model. Specifically, we present a deterministic lifting theorem that translates one-way two-party communication lower bounds into one-way NOF lower bounds.

Our lifting theorem yields two applications. First, we obtain an optimal explicit separation between randomized and deterministic *one-way NOF communication*, even in the multi-player setting. This improves the prior square-root vs. constant separation for three players established by Kelley and Lyu (arXiv 2025). Second, we achieve *optimal separations* between one-round and two-round deterministic NOF communication, improving upon the previous separation of $\Omega\left(\frac{n^{1/(k-1)}}{k^k}\right)$ vs. $O(\log n)$ for k players, as shown by Viola and Wigderson (FOCS 2007).

On the technical side, we use the *generalized inner product function over large fields (GIP)* as the gadget. As a bonus result, we construct an explicit function that for any number of players k , at least $\Omega(n/2^k)$ bits of communication are required to solve it, even for randomized NOF protocols. This improves the previous best bound of $\Omega(n/4^k)$ for generalized inner product over the binary field, established by Babai, Nisan, and Szegedy (STOC 1989).

Beyond the lifting theorems, we also apply our techniques to the disjointness problem. In particular, we provide a new proof that the deterministic one-way three-party NOF communication complexity of set disjointness is $\Omega(n)$, further demonstrating the broader applicability of our methods.

1 Introduction

Lifting theorems are a generic method for translating lower bounds from weaker computational models to relatively stronger ones. A representative example of lifting theorems is the query-to-communication lifting theorems, which convert lower bounds in query complexity into communication complexity lower bounds, using a suitable base function composed with a gadget.

*Research supported by NSF CAREER award 2141536.

Thomas Lord Department of Computer Science, University of Southern California.

Email: {guangxuy, jiapengz}@usc.edu

There has been a long line of work developing query-to-communication lifting theorems, with diverse applications in various areas such as monotone circuit complexity, proof complexity, combinatorial optimization, and more [RM97, Zha09, GPW18, PR17, GPW20, CFK⁺19, LMM⁺22, YZ24, MYZ25]. Though these lifting theorems have achieved significant success, to the best of our knowledge, all existing lifting theorems have focused on two-party communication models (or on a slight generalization known as the Number-in-Hand model). No lifting theorems have yet been established for the more powerful models, such as the Number-on-Forehead (NOF) models.

Compared to two-party communication lower bounds, lower bounds in NOF models are known to have more connections to several major open problems. However, existing lower bound techniques for NOF models remain quite limited. Motivated by this, papers by Kumar, Meka, and Zuckerman [KMZ20] and Toniann Pitassi [Pit21] raised a natural question:

Can we develop lifting theorems in NOF models and derive interesting applications?

Though this problem is well-motivated, it remains wide open. Furthermore, we do not even have good candidates for conjectured statements for the lifting theorem in NOF models. In this paper, we propose a lifting theorem that converts two-party communication lower bounds into lower bounds in the NOF models. As a first step in this direction, we prove a deterministic lifting theorem that lifts one-way communication lower bounds in the two-party setting to one-way communication lower bounds in NOF protocols. Although the one-way NOF model may seem like a restricted variant of the general NOF model, since each player is allowed to speak only once in a fixed order, it still enables many surprising applications. Notably, it has been instrumental in proving strong lower bounds in areas such as circuit complexity [HG90, PRS97, Cha07, VW07], cryptography [CKGS98, BDFP17], and streaming algorithms [KMPV19, VW07]. Despite its restricted nature, proving lower bounds in the one-way NOF model remains a highly challenging and fundamental problem.

1.1 Our Contribution

In this paper, we propose a new form of lifting two-party communication problems into NOF communication problems.

Definition 1.1. For any two-party function $f : [q] \times [q] \rightarrow \{0, 1\}$ and a gadget function $g^k : [N]^k \rightarrow [q]$, the lifted problem over $(k + 1)$ players, denoted by, $f \circ g^k : [N] \times \cdots \times [N] \times [q] \rightarrow \{0, 1\}$, is defined as

$$f \circ g^k(x_1, \dots, x_k, z) = f(z, g^k(x_1, \dots, x_k)).$$

In the NOF setting, we assume that the $(k + 1)$ -th player knows the input (x_1, \dots, x_k) , while each of the remaining i -th players knows all inputs except x_i .

We observe that many well-known problems in the NOF model can be expressed as lifted problems of the form $f \circ g$. Examples include *Generalized Inner Product* [RY20], *Set Disjointness* [RY20], *Pointer Jumping* [VW07, Cha07], *Shifting* [PRS97], and the *Exactly-N* problem [CFL83]. As a quick example, consider the *Exactly-N* problem: Alice, Bob, and Charlie are given integers x , y , and z , and the goal is to determine whether $x + y + z = N$. We can express this as a composition $\text{EQ} \circ g$ by defining $g(x, y) := N - x - y$, and $\text{EQ}(z, s) = 1$ if and only if $z = s$. Then, the condition $x + y + z = N$ holds if and only if $f(z, g(x, y)) = 1$.

In this paper, we primarily use the generalized inner production function as the gadget g .

Definition 1.2. Let q be a prime and $k, r > 0$. We define the function $\text{GIP}_{q,r}^k : (\mathbb{F}_q^r)^k \rightarrow \mathbb{F}_q$ by

$$\text{GIP}_{q,r}^k(x_1, \dots, x_k) = \sum_{j \in [r]} \prod_{i \in [k]} x_{i,j},$$

where \mathbb{F}_q is a prime field, and all arithmetic operations are over \mathbb{F}_q . When q, r, k are clear from context, we write $\text{GIP}(x_1, \dots, x_k)$ for simplicity.

Using the generalized inner product function, we show that for any two-party function f , the one-way communication lower bound of f , denoted $\text{OCC}(f)$, can be lifted to a one-way NOF lower bound of $f \circ \text{GIP}$, denoted $\text{OCC}^{\text{NOF}}(f \circ \text{GIP})$.

Theorem 1.3. Let q be a prime and $k, r \geq 2^{k+1}$. For any Boolean function $f : [q] \times [q] \rightarrow \{0, 1\}$, we have

$$\text{OCC}^{\text{NOF}}(f \circ \text{GIP}_{q,r}^k) = \Theta(\text{OCC}(f)).$$

Although we only prove the theorem for one-way communication, we conjecture that it also holds for general NOF communication.

1.1.1 Applications of Our Main Theorem

We now discuss some applications of our main theorem.

Deterministic vs. randomized separation. One of the central goals in communication complexity is understanding the power of randomized communication. Separations between deterministic and randomized communication complexity in NOF have received a good amount of attention in recent years [BDPW10, KLM24, JLL⁺25, KL25]. Beame, David, Pitassi, and Woelfel [BDPW10] showed the existence of a three-party function $f : [N]^3 \rightarrow \{0, 1\}$ with randomized NOF complexity $O(1)$ and deterministic NOF complexity $\Omega(\log N)$. However, their result was non-explicit, relying on a counting argument.

For explicit constructions, the *Exactly- N* function introduced by [CFL83] has long been considered a strong candidate for such separations. While its randomized three-party complexity is $O(1)$, a deterministic lower bound was not known until the recent breakthrough by Jaber, Liu, Lovett, Ostuni, and Sawhney [JLL⁺25], who showed an $\Omega((\log N)^{\Omega(1)})$ lower bound. For other explicit constructions, Kelley and Lyu [KL25] established an $\Omega(\sqrt{\log N})$ vs. $O(1)$ separation.

Though these advances are very impressive, two key challenges remain. First, for existing approaches including [KLM24, JLL⁺25, KL25], it is still unknown how to break the square-root barrier. That is, it remains unclear how to achieve an $\Omega(\log N)$ vs. $O(1)$ optimal separation, even in the one-way setting. Second, proving deterministic lower bounds for more than three players remains difficult. For instance, the result of [JLL⁺25] yields only an $\Omega(\log \log \log \log N)$ vs. $O(1)$ separation for four players.

In this paper, we suggest a lifting-based approach. In the two-party setting, the equality function is a well-known example demonstrating a separation between deterministic and randomized communication complexity. As an application of Theorem 1.3, we obtain a NOF separation by lifting the equality function..

Theorem 1.4. For any $k \geq 2$ and $r \geq 2^{k+1}$, the deterministic one-way NOF complexity of $\text{EQ} \circ \text{GIP}_{q,r}^k$ is $\Omega(\log q)$, while its randomized one-way NOF complexity is $O(1)$.

Note that for any constant k , we have $\log q = \Theta(\log q^r) = \Theta(\log N)$. Therefore, our construction yields an $\Omega(\log N)$ vs. $O(1)$ optimal separation for a constant number of players in the one-way NOF setting.

One-round vs. two-round deterministic separation. Understanding the power of interaction is one of the central objectives in communication complexity [PS82, DGS84, NW91, VW07, MYZ25]. As another application of our lifting theorem, we obtain an explicit optimal separation between one-round and two-round deterministic NOF communication. Papadimitriou and Sipser [PS82] initiated the study of how restricting two-party communication protocols to r rounds affects their complexity. Several researchers subsequently explored this fundamental question. Notably, Duris, Galil, and Schnitger [DGS84] established an exponential separation between r and $r + 1$ rounds in the two-party setting, a result later improved by Nisan and Wigderson [NW91]. However, for NOF settings involving more than two parties ($k > 2$), the only known result is by Viola and Wigderson [VW07], they give $\Omega\left(\frac{n^{1/(k-1)}}{k^k}\right)$ vs $O(\log n)$ separation between one-round and two-round deterministic NOF communication via the tree pointer jumping problem. We improve this bound to $\Omega\left(\frac{n}{2^k}\right)$ vs $O(\log n)$.

The following *index problem* is a well-known example that separates one-round and two-round deterministic communication in the two-party setting.

Definition 1.5. *In the index problem, Alice receives a binary string $x \in \{0, 1\}^n$, and Bob receives an index $i \in [n]$. The goal is to compute x_i .*

It is well known that the one-round communication complexity of the index problem is $\Omega(n)$, while in the two-round setting, it suffices for Bob to send his input using only $\log n$ bits. We now lift the index problem to the NOF setting.

To fit our lifting framework, we first slightly modify the input of the index problem. We define the modified index function $\text{Ind} : [q] \times [q] \rightarrow \{0, 1\}$ as follows: for every input (x, y) , let i_y be the integer represented by the first $\log \log q$ bits of y , and define $\text{Ind}(x, y) = x_{i_y}$. Using previous analysis, we know that the one-round communication complexity of Ind is $\Omega(\log q)$ and the two-round cost is $O(\log \log q)$.

By applying our lifting theorem (Theorem 1.3) again, we obtain the following:

Theorem 1.6. *For $k \geq 2$ and $r = 2^{k+1}$, the deterministic one-way NOF communication complexity of $\text{Ind} \circ \text{GIP}_{q,r}^k$ is $\Omega(\log q)$, while its two-round NOF communication complexity is $O(\log \log q)$.*

Disjointness lower bounds. Beyond the lifting theorem, we also apply our technique to obtain a new proof that the deterministic one-way three-party NOF communication cost of set disjointness is at least $\Omega(n)$.

Theorem 1.7. *The deterministic one-way three-party NOF complexity of set disjointness is $\Omega(n)$.*

To the best of our knowledge, the only known proof of Theorem 1.7 relies on the discrepancy method [RY15]. However, the discrepancy method can only establish an $\Omega(\sqrt{n})$ lower bound in the randomized *one-way NOF* protocols for set disjointness. In contrast, our approach is based on lifting, which has the potential for proving $\Omega(n)$ lower bounds in the randomized setting.

2 Preliminaries

Communication complexity. We begin by recalling some standard definitions in communication complexity. In the two-party communication model, Alice and Bob receive inputs $x \in X$ and $y \in Y$, respectively. Their goal is to compute a function $f : X \times Y \rightarrow \{0, 1\}$. For any two-party function f , we also use $M(f)$ to denote the *communication matrix* corresponding to f ; that is, $M(f)$ is an $X \times Y$ matrix where each entry at position (x, y) is $f(x, y)$.

Definition 2.1 (One-way communication complexity). *Alice sends a single message $\Pi(x)$ to Bob, and Bob outputs $f(x, y)$ based on y and the received message. The deterministic communication complexity is the maximum length of the message $|\Pi(x)|$ over all possible inputs, denoted by $\text{OCC}(f)$.*

We use the following lemma by Feder, Kushilevitz, Naor, and Nisan [FKNN95] to characterize the one-way deterministic communication complexity of any two-party function.

Lemma 2.2. *Let $f : [q] \times [q] \rightarrow \{0, 1\}$. Then f has one-way deterministic communication complexity C if and only if $M(f)$ contains a set of 2^C distinct rows. That is, there exists a subset $Z \subseteq [q]$ of size $|Z| = 2^C$ such that for any distinct $z_0, z_1 \in Z$, there exists $v \in [q]$ with $f(z_0, v) \neq f(z_1, v)$.*

Definition 2.3 (One-way NOF). *In the k -party one-way NOF, k players collaborate to compute a function $f : X_1 \times \dots \times X_k \rightarrow \{0, 1\}$. The inputs are distributed such that each player i knows all inputs except for x_i .*

In the one-way communication setting, the players communicate in a fixed order, from the first player to the last. Each player sends a single message, and the last player outputs the value of $f(x_1, \dots, x_k)$.

The deterministic communication complexity is defined as the maximum total length of all messages over all possible inputs, and is denoted by $\text{OCC}^{\text{NOF}}(f)$. The notion of cylinder intersections plays a central role in studying the communication complexity of NOF problems.

Definition 2.4. *A set $S \subseteq X_1 \times \dots \times X_k$ is called a cylinder if there exists an index $i \in [k]$ such that membership in S does not depend on the value of x_i . A set S is called a cylinder intersection if it can be written as $S = S_1 \cap \dots \cap S_k$, where each S_i is a cylinder.*

3 A Lifting Theorem for One-Way NOF Model

We first recall the definition of $\text{GIP}_{q,r}^k : (\mathbb{F}_q^r)^k \rightarrow \mathbb{F}_q$ over a large field by,

$$\text{GIP}_{q,r}^k(x_1, \dots, x_k) = \sum_{j \in [r]} \prod_{i \in [k]} x_{i,j}.$$

To simplify notations, we also use $[N]$ to denote \mathbb{F}_q^r . Our main theorem aims to show that

$$\text{OCC}^{\text{NOF}}(f \circ \text{GIP}_{q,r}^k) = \Theta(\text{OCC}(f)),$$

for any two-party communication problem $f : [q] \times [q] \rightarrow \{0, 1\}$ and $r \geq 2^{k+1}$. The upper bound, i.e., $\text{OCC}^{\text{NOF}}(f \circ \text{GIP}_{q,r}^k) = O(\text{OCC}(f))$, is straightforward. Hence, we focus on the lower bound.

Proof of Theorem 1.3. For any two-party function f , by Lemma 2.2, let $Z \subseteq [q]$ be the set of the distinct rows of $M(f)$ of size $|Z| = 2^{\text{OCC}(f)}$. Our goal is to prove that

$$\text{OCC}^{\text{NOF}}(f \circ \text{GIP}) = \Omega(\log |Z|).$$

We omit the subscripts of q, r, k here as they are fixed throughout the proof. Let Π be any one-way NOF protocol. We show that if the communication complexity of Π is $o(\log |Z|)$, then there exist messages (π_1, \dots, π_k) , as well as distinct rows $z_0^*, z_1^* \in Z$ and inputs $(x_1^*, \dots, x_k^*) \in [N]^k$, such that

- The first k players output (π_1, \dots, π_k) for both inputs $(x_1^*, \dots, x_k^*, z_0^*)$ and $(x_1^*, \dots, x_k^*, z_1^*)$.
- $(f \circ \text{GIP})(x_1^*, \dots, x_k^*, z_0^*) \neq (f \circ \text{GIP})(x_1^*, \dots, x_k^*, z_1^*)$.

The items above imply that Π cannot distinguish inputs $(x_1^*, \dots, x_k^*, z_0^*)$ and $(x_1^*, \dots, x_k^*, z_1^*)$. Therefore, it is not a deterministic protocol for computing $f \circ \text{GIP}$.

Let Π be any one-way protocol with communication bits less than $(\log |Z|)/3$. By the pigeonhole principle, there exists a message tuple (π_1, \dots, π_k) such that the following set A has size at least

$$|A| \geq \frac{N^k \cdot |Z|}{|Z|^{1/3}} = N^k \cdot |Z|^{2/3} \geq 2N^k \cdot \sqrt{|Z|}.$$

Here, the set A is defined as

$$A = \{(x_1, \dots, x_k, z) \in [N]^k \times Z : \text{the first } k \text{ players output } (\pi_1, \dots, \pi_k) \text{ on input } (x_1, \dots, x_k, z)\}.$$

Now we focus on finding indistinguishable pairs (x^*, y^*, z_0^*) and (x^*, y^*, z_1^*) from the set A . The following largeness lemma is a crucial component of our proof.

Lemma 3.1. *Let $A \subseteq [N]^k \times Z$ be a set of size $|A| \geq 2N^k \cdot \sqrt{|Z|}$. Then for uniformly sampled distinct $z, z' \in Z$, we have that,*

$$\mathbb{E}_{z, z'} [|\{(x_1, \dots, x_k) : (x_1, \dots, x_k, z) \in A\} \cap \{(x_1, \dots, x_k) : (x_1, \dots, x_k, z') \in A\}|] \geq \frac{N^k}{|Z|} \geq \frac{q^{kr}}{q} = q^{kr-1}.$$

We postpone to proof of Lemma 3.1 to Section 3.1. Now we fix any distinct z, z' such that

$$|\{(x_1, \dots, x_k) : (x_1, \dots, x_k, z) \in A\} \cap \{(x_1, \dots, x_k) : (x_1, \dots, x_k, z') \in A\}| \geq q^{kr-1}$$

as our desired z_0^* and z_1^* . Since z_0^* and z_1^* are distinct rows of Z , there exists a $v \in [q]$ such that $f(z_0^*, v) \neq f(z_1^*, v)$. Our goal now reduces to finding a tuple (x_1^*, \dots, x_k^*) in the intersection, i.e.,

$$(x_1^*, \dots, x_k^*, z_0^*), (x_1^*, \dots, x_k^*, z_1^*) \in A$$

such that $\text{GIP}(x_1^*, \dots, x_k^*) = v$.

To prove that, a crucial fact is that for any fixed z , the set $\{(x_1, \dots, x_k) : (x_1, \dots, x_k, z) \in A\}$ forms a cylinder intersection. Therefore, the intersection

$$\{(x_1, \dots, x_k) : (x_1, \dots, x_k, z_0^*) \in A\} \cap \{(x_1, \dots, x_k) : (x_1, \dots, x_k, z_1^*) \in A\}$$

is also a cylinder intersection of size at least q^{kr-1} . We now invoke the following disperser property of the generalized inner product function over cylinder intersection.

Lemma 3.2. For $r \geq 2^{k+1}$. Let $S \subseteq (\mathbb{F}_q^r)^k$ be any cylinder intersection of size $|S| \geq q^{r \cdot k - 1}$. Then for every $v \in \mathbb{F}_q$, we have that

$$\Pr_{(x_1, \dots, x_k) \in S} [\text{GIP}(x_1, \dots, x_k) = v] \geq \frac{1}{q} - q \cdot (2k/q)^4$$

We postpone the proof to Section 3.2. Assuming Lemma 3.2, we can choose the desired (x_1^*, \dots, x_k^*) such that $\text{GIP}(x_1^*, \dots, x_k^*) = v$. We then conclude the proof. \square

3.1 Proof of Lemma 3.1

Recall that $A \subseteq [N]^k \times Z$ is a set of size $|A| \geq 2N^2 \cdot \sqrt{|Z|}$, we aim to prove that

$$\mathbb{E}_{z, z'} [|\{(x_1, \dots, x_k) : (x_1, \dots, x_k, z) \in A\} \cap \{(x_1, \dots, x_k) : (x_1, \dots, x_k, z') \in A\}|] \geq \frac{N^k}{|Z|}.$$

We consider a bipartite graph $G = (L \cup R, E)$ defined by $L = Z$, $R = [N]^k$ and $E = \{(z, (x_1, \dots, x_k)) : (x_1, \dots, x_k, z) \in A\}$, and prove the following lemma.

Lemma 3.3. Let $G = (L \cup R, E)$ be a bipartite graph with $|E| \geq 2 \cdot \sqrt{|L|} \cdot |R|$. Then for uniformly chosen distinct $\ell, \ell' \in L$, we have that

$$\mathbb{E}[|N(\ell) \cap N(\ell')|] \geq \frac{|R|}{|L|}.$$

where $N(\ell) \subseteq R$ denote the neighborhoods of ℓ in R .

Proof. Let $\mathbf{1}(\ell, r) := \mathbf{1}\{(\ell, r) \in E\}$ denote the indicator function for whether the edge (ℓ, r) exists in E . Then we have

$$\mathbb{E}[|N(\ell) \cap N(\ell')|] = \mathbb{E}\left[\sum_{r \in R} \mathbf{1}(\ell, r) \cdot \mathbf{1}(\ell', r)\right] = \sum_{r \in R} \mathbb{E}[\mathbf{1}(\ell, r) \cdot \mathbf{1}(\ell', r)].$$

Let $\deg(r) := \sum_{\ell \in L} \mathbf{1}(\ell, r)$ be the degree of vertex $r \in R$. Then,

$$\sum_{r \in R} \mathbb{E}[\mathbf{1}(\ell, r) \cdot \mathbf{1}(\ell', r)] = \frac{2}{|L|(|L| - 1)} \cdot \sum_{r \in R} \sum_{\ell \neq \ell' \in L} \mathbf{1}(\ell, r) \cdot \mathbf{1}(\ell', r) = \frac{2}{|L|(|L| - 1)} \cdot \sum_{r \in R} \binom{\deg(r)}{2}.$$

Now observe that

$$\sum_{r \in R} \binom{\deg(r)}{2} \geq \frac{1}{2} \cdot \sum_{r \in R} (\deg(r) - 1)^2 \geq \frac{1}{2|R|} \left(\sum_{r \in R} (\deg(r) - 1) \right)^2 = \frac{(|E| - |R|)^2}{2|R|}.$$

The second inequality follows from the Cauchy-Schwarz inequality; the equality uses the identity $\sum_{r \in R} \deg(r) = |E|$. Therefore,

$$\mathbb{E}[|N(\ell) \cap N(\ell')|] \geq \frac{2}{|L|(|L| - 1)} \cdot \frac{(|E| - |R|)^2}{2|R|} \geq \frac{2}{|L|(|L| - 1)} \cdot \frac{(2\sqrt{|L|} - 1)^2 \cdot |R|^2}{2|R|} = \frac{(2\sqrt{|L|} - 1)^2 \cdot |R|}{|L|(|L| - 1)}$$

where the second inequality uses the assumption that $|E| \geq 2\sqrt{|L|} \cdot |R|$. Finally, we conclude the proof since $(2\sqrt{|L|} - 1)^2 \geq |L| - 1$. \square

3.2 Proof of Lemma 3.2

We prove Lemma 3.2 in this section. Let $r \geq 2^{k+1}$ and $S \subseteq (\mathbb{F}_q^r)^k$ be any cylinder intersection of size $|S| \geq q^{r \cdot k - 1}$. We aim to prove that for every $v \in \mathbb{F}_q$,

$$\Pr_{(x_1, \dots, x_k) \in S} [\text{GIP}(x_1, \dots, x_k) = v] \geq \frac{1}{q} - q \cdot (2k/q)^4$$

Proof. Let $\mathbf{1} : \mathbb{F}_q \rightarrow \{0, 1\}$ be the indicator function, i.e., $\mathbf{1}(z) = 1$ if $z = 0$ and $\mathbf{1}(z) = 0$ otherwise. We write its Fourier transform as

$$\mathbf{1}(z) = \frac{1}{q} \sum_{\alpha \in \mathbb{F}_q} \chi_\alpha(z),$$

where χ_α are the additive characters of \mathbb{F}_q . Then,

$$\begin{aligned} \Pr_{(x_1, \dots, x_k) \in S} [\text{GIP}(x_1, \dots, x_k) = v] &= \frac{1}{|S|} \sum_{(x_1, \dots, x_k) \in S} \mathbf{1}(\text{GIP}(x_1, \dots, x_k) - v) \\ &= \frac{1}{|S|} \sum_{(x_1, \dots, x_k) \in S} \frac{1}{q} \cdot \sum_{\alpha \in \mathbb{F}_q} \chi_\alpha(\text{GIP}(x_1, \dots, x_k) - v) \\ &= \frac{1}{q} + \frac{1}{q \cdot |S|} \sum_{\alpha \neq 0} \chi_\alpha(-v) \sum_{(x_1, \dots, x_k) \in S} \chi_\alpha(\text{GIP}(x_1, \dots, x_k)). \end{aligned}$$

The last equality follows by the fact that $\chi_\alpha(0) = 1$ and $\chi_\alpha(a + b) = \chi_\alpha(a) \cdot \chi_\alpha(b)$. We first analyze the upper bound of

$$\left| \sum_{(x_1, \dots, x_k) \in S} \chi_\alpha(\text{GIP}(x_1, \dots, x_k)) \right|$$

for every α . Recall the definition of GIP, we rewrite it as below D_α .

$$D_\alpha := \left| \sum_{(x_1, \dots, x_k) \in S} \chi_\alpha \left(\sum_{j \in [r]} \prod_{i \in [k]} x_{i,j} \right) \right| = \left| \sum_{(x_1, \dots, x_k) \in (\mathbb{F}_q^r)^k} \prod_i \mathbf{1}_{S_i}(x_1, \dots, x_k) \cdot \chi_\alpha \left(\sum_j \prod_i x_{i,j} \right) \right|$$

Let $\gamma_\alpha = D_\alpha / q^{r \cdot k} = |\mathbb{E}_{(x_1, \dots, x_k)} [\prod_i \mathbf{1}_{S_i}(x_1, \dots, x_k) \cdot \chi_\alpha(\sum_j \prod_i x_{i,j})]|$. By the fact that $(\mathbb{E}[X])^2 \leq \mathbb{E}[X^2]$, we have that

$$\begin{aligned} \gamma_\alpha^2 &\leq \mathbb{E}_{x_1, \dots, x_{k-1}} \left[\mathbf{1}_{S_k}(x_1, \dots, x_{k-1})^2 \mathbb{E}_{x_k, x'_k} \left[\prod_{i \leq k-1} \mathbf{1}_{S_i}(x_1, \dots, x_k) \mathbf{1}_{S_i}(x_1, \dots, x'_k) \chi_\alpha \left(\sum_j x_{k,j} x'_{k,j} \prod_{i \leq k-1} x_{i,j} \right) \right] \right] \\ &\leq \mathbb{E}_{x_k, x'_k} \mathbb{E}_{x_1, \dots, x_{k-1}} \left[\prod_{i \in [k-1]} (\mathbf{1}_{S_i}(x_1, \dots, x_k) \cdot \mathbf{1}_{S_i}(x_1, \dots, x'_k)) \chi_\alpha \left(\sum_j x_{k,j} \cdot x'_{k,j} \prod_{i \in [k-1]} x_{i,j} \right) \right] \end{aligned}$$

By applying the this argument $(k-1)$ times, we have that

$$\gamma_\alpha^{2^{k-1}} \leq \mathbb{E}_{(x_2, \dots, x_k), (x'_2, \dots, x'_k)} \left[\mathbb{E}_{x_1} \left[\chi_\alpha \left(\sum_j x_{1,j} \cdot \prod_{i \geq 1} x_{i,j} x'_{i,j} \right) \right] \right]$$

Recall that for any character χ_α , it holds that $\sum_{z \in \mathbb{F}_q} \chi_\alpha(z) = 0$. Hence, for any $(x_2, \dots, x_k), (x'_2, \dots, x'_k)$, if there is a $j \in [r]$ such that $\prod_{i>1} x_{i,j} x'_{i,j} \neq 0$, we have that

$$\mathbb{E}_{x_1} \left[\chi_\alpha \left(\sum_j x_{1,j} \cdot \prod_{i>1} x_{i,j} x'_{i,j} \right) \right] = 0$$

Therefore,

$$\gamma_\alpha^{2^{k-1}} \leq \Pr_{(x_2, \dots, x_k, x'_2, \dots, x'_k)} \left[\forall j \in [r], \prod_{i>1} x_{i,j} x'_{i,j} = 0 \right] \leq (2k/q)^r$$

It implies that

$$D_\alpha = q^{r \cdot k} \cdot \gamma_\alpha \leq q^{r \cdot k} \cdot (2k/q)^{r/2^{k-1}}$$

Recall that $|S| \geq q^{r \cdot k - 1}$ and $r \geq 2^{k+1}$, then we have that

$$\begin{aligned} \Pr_{(x_1, \dots, x_k) \in S} [\text{GIP}(x_1, \dots, x_k) = v] &= \frac{1}{q} + \frac{1}{q \cdot |S|} \sum_{\alpha \neq 0} \chi_\alpha(-v) \sum_{(x_1, \dots, x_k) \in S} \chi_\alpha(\text{GIP}(x_1, \dots, x_k)) \\ &\geq \frac{1}{q} - \frac{1}{|S|} \left| \sum_{(x_1, \dots, x_k) \in S} \chi_\alpha(\text{GIP}(x_1, \dots, x_k)) \right| \\ &\geq \frac{1}{q} - \frac{q^{r \cdot k} \cdot (2k/q)^{r/2^{k-1}}}{|S|} \geq \frac{1}{q} - q \cdot (2k/q)^4 \end{aligned}$$

The first inequality is by the triangle inequality and $|\chi_\alpha(-v)| = 1$. The claim then follows. \square

A bonus result of Lemma 3.2 is that we construct a k -party NOF problem that requires $\Omega(n/2^k)$ randomized communication cost.

Corollary 3.4. *For every $n > 0$ and $k \leq \log n - 5 \log \log n$. Let q be a $n/2^{k+1}$ -bit length prime number, and let $r = 2^{k+1}$. Define $G : (\mathbb{F}_q^r)^k \rightarrow \{0, 1\}$ be a function defined by*

$$G(x_1, \dots, x_k) = \text{GIP}(x_1, \dots, x_k) \pmod 2$$

Then G is a function with input length n , and has a randomized NOF lower bounds $\Omega(n/2^{k+1})$

4 A One-Way NOF Lower Bound of Set Disjointness

In this section, we present a new proof of the $\Omega(n)$ deterministic one-way communication lower bound for the three-party NOF model. The proof follows a similar structure to that of Theorem 1.3. However, the key difference is that we no longer have a large gadget with disperser properties. Instead, we incorporate the density increment argument by Yang and Zhang [YZ22, YZ23].

We first recall that in the two-party communication, for inputs x, y , $\text{DISJ}_2(x, y) = 1$ if and only if x and y are disjoint, i.e., $\bigwedge_{i=1}^n (\bar{x}_i \vee \bar{y}_i)$.

Definition 4.1. *Let $x, y, z \in \{0, 1\}^n$. The three-party set disjointness DISJ_3 is defined as*

$$\text{DISJ}_3(x, y, z) := \text{DISJ}_2(z, x \wedge y) = \bigwedge_{i=1}^n (\bar{z}_i \vee \bar{x}_i \vee \bar{y}_i).$$

We now show that the deterministic one-way NOF communication complexity of DISJ_3 is $\Omega(n)$.

Proof of Theorem 1.7. For any protocol Π with communication complexity $o(n)$, we aim to show that there is a message pair (π_A^*, π_B^*) , a pair of distinct inputs z_0^*, z_1^* , and a pair (x^*, y^*) , such that:

- $\Pi_A(y^*, z_0^*) = \Pi_A(y^*, z_1^*) = \pi_A^*$.
- $\Pi_B(x^*, z_0^*, \pi_A^*) = \Pi_B(x^*, z_1^*, \pi_A^*) = \pi_B^*$.
- $\text{DISJ}_3(z_0^*, x^*, y^*) \neq \text{DISJ}_3(z_1^*, x^*, y^*)$.

Define the set $D_0 := \{(x, y) \in \{0, 1\}^n \times \{0, 1\}^n : \bigwedge_{i=1}^n (\bar{x}_i \vee \bar{y}_i) = 1\}$, i.e., the set of all pairs of disjoint sets. By an averaging argument, there exists a transcript (π_A^*, π_B^*) such that the set

$$A := \{(z, x, y) \in \{0, 1\}^n \times \{0, 1\}^n \times \{0, 1\}^n : \Pi_A(y, z) = \pi_A^*, \Pi_B(x, z, \pi_A^*) = \pi_B^*, \text{ and } (x, y) \in D_0\}$$

has size at least

$$|A| \geq 2^n \cdot |D_0| \cdot 2^{-o(n)}.$$

Similar to Lemma 3.3, we now prove the following largeness lemma.

Lemma 4.2. *Let $G = (L, R, E)$ be a bipartite graph with $L = \{0, 1\}^n$. Suppose the number of edges satisfies $|E| \geq 2^n \cdot |R| \cdot 2^{-\delta \cdot n}$ for some $\delta < 0.1$. Then there exist vertices $\ell, \ell' \in \{0, 1\}^n$ with Hamming distance $d_H(\ell, \ell') \geq 0.1n$ such that*

$$|N(\ell) \cap N(\ell')| \geq |R| \cdot 2^{-2\delta n - 2},$$

where $N(\ell) \subseteq R$ denotes the neighborhood of ℓ in R , and $d_H(\ell, \ell')$ denotes the Hamming distance.

Proof. Since $|E| \geq 2^n \cdot |R| \cdot 2^{-\delta n}$, using similar ideas from Lemma 3.3, we have that

$$\mathbb{E}_{\ell, \ell'} [|N(\ell) \cap N(\ell')|] = \sum_{r \in R} \mathbb{E}_{\ell, \ell'} [\mathbf{1}(\ell, r) \cdot \mathbf{1}(\ell', r)] \geq \frac{2}{|L|(|L| - 1)} \cdot \frac{(|E| - |R|)^2}{2|R|} \geq |R| \cdot 2^{-2\delta n - 1},$$

where $\mathbf{1}(\ell, r)$ denotes the indicator that $(\ell, r) \in E$. We split the expectation based on the Hamming distance between ℓ and ℓ' . Specifically, we write $\mathbb{E}_{\ell, \ell'} [|N(\ell) \cap N(\ell')|]$ as

$$\mathbb{E} [|N(\ell) \cap N(\ell')| \cdot \mathbf{1}(d_H(\ell, \ell') < 0.1n)] + \mathbb{E} [|N(\ell) \cap N(\ell')| \cdot \mathbf{1}(d_H(\ell, \ell') \geq 0.1n)].$$

For the first term, we upper bound it by:

$$\Pr_{\ell, \ell'} [d_H(\ell, \ell') < 0.1n] \leq 2^{-n} \cdot \sum_{i=0}^{0.1n} \binom{n}{i} \leq 2^{-n} \cdot \left(\frac{e}{0.1}\right)^{0.1n} \leq 2^{-n/2}.$$

Hence, we have

$$\mathbb{E} [|N(\ell) \cap N(\ell')| \cdot \mathbf{1}(d_H(\ell, \ell') < 0.1n)] \leq \mathbb{E} [|R| \cdot \mathbf{1}(d_H(\ell, \ell') < 0.1n)] \leq |R| \cdot 2^{-n/2}.$$

Therefore, the contribution from the second term is at least

$$\mathbb{E} [|N(\ell) \cap N(\ell')| \cdot \mathbf{1}(d_H(\ell, \ell') \geq 0.1n)] \geq |R| \cdot 2^{-2\delta n - 1} - |R| \cdot 2^{-n/2} \geq |R| \cdot 2^{-2\delta n - 2},$$

where the last inequality holds for small constant $\delta < 0.1$. This completes the proof. \square

By applying Lemma 4.2 with $L = \{0, 1\}^n$, $R = D_0$, and $E = A$, we obtain a pair of distinct strings $z_0^*, z_1^* \in \{0, 1\}^n$ with Hamming distance $d_H(z_0^*, z_1^*) \geq 0.1 \cdot n$ such that the following set

$$R := \{(x, y) : \Pi_A(y, z_0^*) = \pi_A^*, \Pi_B(x, z_0^*, \pi_A^*) = \pi_B^*\} \cap \{(x, y) : \Pi_A(y, z_1^*) = \pi_A^*, \Pi_B(x, z_1^*, \pi_A^*) = \pi_B^*\}$$

has large intersection with the set D_0 , specifically,

$$|R \cap D_0| \geq |D_0| \cdot 2^{-o(n)}.$$

Notice that for fixed (π_A^*, π_B^*) and z_0^*, z_1^* , the set R is a rectangle. Unlike the proof of the lifting theorem (Theorem 1.3, we can no longer apply a disperser property on the set $R \cap D_0$ as there is no large gadget. Instead, we take the approach by [YZ22, YZ23]. For each $\ell \in [n]$, define the set

$$D_\ell := \{(x, y) \in \{0, 1\}^n \times \{0, 1\}^n : x \wedge y = e_\ell\},$$

where e_ℓ is the unit vector with a 1 at coordinate ℓ and 0 elsewhere. Yang and Zhang proved the following pseudorandomness lemma.

Lemma 4.3 (Theorem 1.1 of [YZ23]). *Let $R \subseteq \{0, 1\}^n \times \{0, 1\}^n$ be any rectangle. If*

$$|R \cap D_0| \geq |D_0| \cdot 2^{-c},$$

then there exists a set $S \subseteq [n]$ of size at least $n - 2c$ such that $R \cap D_\ell \neq \emptyset$ for every $\ell \in S$.

We include the proof of Lemma 4.3 in Section A for completeness.

Since $d_H(z_0^*, z_1^*) \geq 0.1 \cdot n$, let $T \subseteq [n]$ denote the set of coordinates where z_0^* and z_1^* differ. By Lemma 4.3, assuming the communication complexity of Π is $o(n)$, there exists a set $S \subseteq [n]$ of size $|S| = n - o(n)$ such that for every $i \in S$, there exists a pair $(x^*, y^*) \in R$ satisfying $x^* \wedge y^* = e_i$.

Since $|T| \geq 0.1n$, we have $T \cap S \neq \emptyset$. Fix any index $j \in T \cap S$. Then:

- We have $(z_0^*)_j \neq (z_1^*)_j$ by definition of T ,
- And there exists $(x^*, y^*) \in R$ such that $x^* \wedge y^* = e_j$.

Combining the two facts, we obtain two inputs $(x^*, y^*, z_0^*) \in A$ and $(x^*, y^*, z_1^*) \in A$ such that

$$\text{DISJ}_3(z_0^*, x^*, y^*) = (z_0^*)_j \neq (z_1^*)_j = \text{DISJ}_3(z_1^*, x^*, y^*).$$

This shows that A is not monochromatic, thereby Π can not solve DISJ_3 completely. □

5 Open problems

A natural open problem is to extend our lifting theorem to the randomized setting. Specifically, we propose the following conjecture:

Conjecture 5.1. *For any partial function $f : [q] \times [q] \rightarrow \{0, 1\}$, we have*

$$\text{ORCC}^{\text{NOF}}(f \circ \text{GIP}) = \Theta(\text{ORCC}(f)),$$

where $\text{ORCC}(f)$ denotes the one-way randomized communication complexity of f , and $\text{ORCC}^{\text{NOF}}(f \circ \text{GIP})$ denotes the one-way number-on-forehead (NOF) randomized communication complexity of $f \circ \text{GIP}$.

Proving this conjecture would imply a separation between quantum and classical communication complexity in the one-way NOF model.

Another important open problem is to extend our lifting theorem (Theorem 1.3) to general communication protocols beyond the one-way setting. Such a result could provide an optimal separation between randomized and deterministic NOF communication.

References

- [BDFP17] Joshua Brody, Stefan Dziembowski, Sebastian Faust, and Krzysztof Pietrzak. Position-based cryptography and multiparty communication complexity. In *Theory of Cryptography Conference*, pages 56–81. Springer, 2017. 2
- [BDPW10] Paul Beame, Matei David, Toniann Pitassi, and Philipp Woelfel. Separating deterministic from randomized multiparty communication complexity. *Theory of Computing*, 6(1):201–225, 2010. 3
- [CFK⁺19] Arkadev Chattopadhyay, Yuval Filmus, Sajin Koroth, Or Meir, and Toniann Pitassi. Query-to-communication lifting using low-discrepancy gadgets. *arXiv preprint arXiv:1904.13056*, 2019. 2
- [CFL83] Ashok K Chandra, Merrick L Furst, and Richard J Lipton. Multi-party protocols. In *Proceedings of the fifteenth annual ACM symposium on Theory of computing*, pages 94–99, 1983. 2, 3
- [Cha07] Amit Chakrabarti. Lower bounds for multi-player pointer jumping. In *Twenty-Second Annual IEEE Conference on Computational Complexity (CCC’07)*, pages 33–45. IEEE, 2007. 2
- [CKGS98] Benny Chor, Eyal Kushilevitz, Oded Goldreich, and Madhu Sudan. Private information retrieval. *Journal of the ACM (JACM)*, 45(6):965–981, 1998. 2
- [DGS84] Pavol Duris, Zvi Galil, and Georg Schnitger. Lower bounds on communication complexity. In *Proceedings of the sixteenth annual ACM symposium on Theory of computing*, pages 81–91, 1984. 4
- [FKNN95] Tomás Feder, Eyal Kushilevitz, Moni Naor, and Noam Nisan. Amortized communication complexity. *SIAM Journal on computing*, 24(4):736–750, 1995. 5
- [GPW18] Mika Göös, Toniann Pitassi, and Thomas Watson. Deterministic communication vs. partition number. *SIAM Journal on Computing*, 47(6):2435–2450, 2018. 2
- [GPW20] Mika Göös, Toniann Pitassi, and Thomas Watson. Query-to-communication lifting for bpp. *SIAM Journal on Computing*, 49(4):FOCS17–441, 2020. 2
- [HG90] J. Hastad and M. Goldmann. On the power of small-depth threshold circuits. In *Proceedings [1990] 31st Annual Symposium on Foundations of Computer Science*, pages 610–618 vol.2, 1990. 2

- [JLL⁺25] Michael Jaber, Yang P. Liu, Shachar Lovett, Anthony Ostuni, and Mehtaab Sawhney. Quasipolynomial bounds for the corners theorem, 2025. [3](#)
- [KL25] Zander Kelley and Xin Lyu. More efficient sifting for grid norms, and applications to multiparty communication complexity, 2025. [3](#)
- [KLM24] Zander Kelley, Shachar Lovett, and Raghu Meka. Explicit separations between randomized and deterministic number-on-forehead communication. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*, pages 1299–1310, 2024. [3](#)
- [KMPV19] John Kallaugher, Andrew McGregor, Eric Price, and Sofya Vorotnikova. The complexity of counting cycles in the adjacency list streaming model. In *Proceedings of the 38th ACM SIGMOD-SIGACT-SIGAI Symposium on Principles of Database Systems*, pages 119–133, 2019. [2](#)
- [KMZ20] Ashutosh Kumar, Raghu Meka, and David Zuckerman. Bounded collusion protocols, cylinder-intersection extractors and leakage-resilient secret sharing. *Cryptology ePrint Archive*, 2020. [2](#)
- [LMM⁺22] Shachar Lovett, Raghu Meka, Ian Mertz, Toniann Pitassi, and Jiapeng Zhang. Lifting with sunflowers. *Leibniz international proceedings in informatics*, 215, 2022. [2](#)
- [MYZ25] Xinyu Mao, Guangxu Yang, and Jiapeng Zhang. Gadgetless lifting beats round elimination: Improved lower bounds for pointer chasing. In *16th Innovations in Theoretical Computer Science Conference (ITCS 2025)*, pages 75–1. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2025. [2](#), [4](#)
- [NW91] Noam Nisan and Avi Wigderson. Rounds in communication complexity revisited. In *Proceedings of the twenty-third annual ACM symposium on Theory of computing*, pages 419–429, 1991. [4](#)
- [Pit21] Toniann Pitassi. Advances and new directions in communication complexity. In *Invited talk at STOC 2021*, 2021. [2](#)
- [PR17] Toniann Pitassi and Robert Robere. Strongly exponential lower bounds for monotone computation. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2017, Montreal, QC, Canada, June 19-23, 2017*, pages 1246–1255. ACM, 2017. [2](#)
- [PRS97] Pavel Pudlák, Vojtech Rödl, and Jirí Sgall. Boolean circuits, tensor ranks, and communication complexity. *SIAM Journal on Computing*, 26(3):605–633, 1997. [2](#)
- [PS82] Christos H Papadimitriou and Michael Sipser. Communication complexity. In *Proceedings of the fourteenth annual ACM symposium on Theory of computing*, pages 196–200, 1982. [4](#)
- [RM97] Ran Raz and Pierre McKenzie. Separation of the monotone nc hierarchy. In *Proceedings 38th Annual Symposium on Foundations of Computer Science*, pages 234–243. IEEE, 1997. [2](#)

- [RY15] Anup Rao and Amir Yehudayoff. Simplified lower bounds on the multiparty communication complexity of disjointness. In *30th Conference on Computational Complexity (CCC 2015)*, pages 88–101. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2015. [4](#)
- [RY20] Anup Rao and Amir Yehudayoff. *Communication Complexity: and Applications*. Cambridge University Press, 2020. [2](#)
- [VW07] E. Viola and A. Wigderson. One-way multi-party communication lower bound for pointer jumping with applications. In *2007 48th Annual IEEE Symposium on Foundations of Computer Science*, pages 427–437, Los Alamitos, CA, USA, oct 2007. IEEE Computer Society. [2](#), [4](#)
- [YZ22] Guangxu Yang and Jiapeng Zhang. Simulation methods in communication lower bounds, revisited. In *Electron. Colloquium Comput. Complex.*, 2022. [9](#), [11](#), [14](#)
- [YZ23] Guangxu Yang and Jiapeng Zhang. Lifting theorems meet information complexity: Known and new lower bounds of set-disjointness. *arXiv preprint arXiv:2309.13517*, 2023. [9](#), [11](#), [14](#)
- [YZ24] Guangxu Yang and Jiapeng Zhang. Communication lower bounds for collision problems via density increment arguments. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*, pages 630–639, 2024. [2](#)
- [Zha09] Shengyu Zhang. On the tightness of the buhrman-cleve-wigderson simulation. In *International Symposium on Algorithms and Computation*, pages 434–440. Springer, 2009. [2](#)

A Proof of Lemma [4.3](#)

Now we prove Lemma [4.3](#) by using the density increment argument by [[YZ22](#), [YZ23](#)].

Theorem A.1 (Restatement of Lemma [4.3](#)). *Let $R \subseteq \{0, 1\}^n \times \{0, 1\}^n$ be any rectangle. If*

$$|R \cap D_0| \geq |D_0| \cdot 2^{-c},$$

then there exists a subset $S \subseteq [n]$ of size at least $n - 2c$ such that $R \cap D_i \neq \emptyset$ for every $i \in S$.

Recall that

$$D_0 := \{(x, y) \in \{0, 1\}^n \times \{0, 1\}^n : x \wedge y = 0^n\}, \quad D_\ell := \{(x, y) \in \{0, 1\}^n \times \{0, 1\}^n : x \wedge y = e_\ell\}$$

where e_ℓ denotes the unit vector with a 1 in the ℓ -th coordinate and zeros elsewhere. For any subset $I \subseteq [n]$ and any $\ell \in I$, we define

$$D_0^I := \{(x, y) \in \{0, 1\}^I \times \{0, 1\}^I : x \wedge y = 0^I\}, \quad D_\ell^I := \{(x, y) \in \{0, 1\}^I \times \{0, 1\}^I : x \wedge y = e_\ell\}.$$

We now introduce the density function, which will be used in the density increment argument.

Definition A.2 (Density function). Let $I \subseteq [n]$, and let $R = X \times Y \subseteq \{0, 1\}^I \times \{0, 1\}^I$ be a rectangle. The density of R with respect to D_0^I is defined as

$$E^I(R) := \log \left(\frac{|R \cap D_0^I|}{|D_0^I|} \right).$$

Note that $E^I(R) \leq 0$ for any rectangle R , and that $|D_0^I| = 3^{|I|}$, as each coordinate allows three disjoint assignments: $(0, 0)$, $(0, 1)$, $(1, 0)$. We will write $E(R)$ when the underlying index set I is clear from context.

A crucial step in our argument is the projection operation, which allows us to restrict attention to a subset of coordinates while preserving the rectangle structure.

Definition A.3 (Projection). Let $R = X \times Y \subseteq \{0, 1\}^I \times \{0, 1\}^I$ be a rectangle. For any coordinate $i \in I$ and side $C \in \{X, Y\}$, the projection of R onto coordinate i from side C is defined as a rectangle $\Pi_{i,C}(R) = X' \times Y' \subseteq \{0, 1\}^{I \setminus \{i\}} \times \{0, 1\}^{I \setminus \{i\}}$, where:

- If $C = X$, then $X' = \{x_{I \setminus \{i\}} : x \in X, x_i = 0\}$ and $Y' = \{y_{I \setminus \{i\}} : y \in Y\}$.
- If $C = Y$, then $X' = \{x_{I \setminus \{i\}} : x \in X\}$ and $Y' = \{y_{I \setminus \{i\}} : y \in Y, y_i = 0\}$.

Here, $x_{I \setminus \{i\}}$ denotes the restriction of the string $x \in \{0, 1\}^I$ to the coordinates in $I \setminus \{i\}$.

The projection operation satisfies two useful properties. The first property is that projection preserves the absence of specific structured sets:

Fact A.4. Let $R \subseteq \{0, 1\}^I \times \{0, 1\}^I$ be a rectangle such that $R \cap D_j^I = \emptyset$ for some $j \in I$. Then, for every $i \in I$ and every $C \in \{X, Y\}$, we have

$$\Pi_{i,C}(R) \cap D_j^{I \setminus \{i\}} = \emptyset.$$

The proof of Fact A.4 follows directly from the definition of projection and is omitted.

The second property quantifies how projection can increase the density, and is captured by the following projection lemma:

Lemma A.5 (Projection Lemma). Let $R = X \times Y \subseteq \{0, 1\}^I \times \{0, 1\}^I$ be a rectangle. If there exists a coordinate $i \in I$ such that $R \cap D_i^I = \emptyset$, then there exists $C \in \{X, Y\}$ such that

$$E^{I \setminus \{i\}}(\Pi_{i,C}(R)) \geq E^I(R) + \frac{1}{2}.$$

Given Lemma A.5 and Fact A.4, the proof of Lemma 4.3 becomes straightforward. We iteratively apply the projection operation on coordinates $i \notin S$, choosing at each step a suitable side $C \in \{X, Y\}$ as guaranteed by Lemma A.5, which increases the density function by at least $1/2$ per step. Since the density is upper bounded by zero, this process can be repeated at most $2c$ times, yielding a subset $S \subseteq [n]$ of size at least $n - 2c$ such that $R \cap D_i \neq \emptyset$ for all $i \in S$.

We now proceed to prove Lemma A.5.

Proof of Lemma A.5. Let $R \subseteq \{0, 1\}^I \times \{0, 1\}^I$ be a rectangle such that $R \cap D_i^I = \emptyset$. Define $I' := I \setminus \{i\}$, and let

$$L := \{(x', y') \in D_0^{I'} : \exists (x, y) \in R \cap D_i^I \text{ such that } x_{I'} = x', y_{I'} = y'\}.$$

Note that for any $C \in \{X, Y\}$, we have

$$\Pi_{i,C}(R) \cap D_0^{I'} = \Pi_{i,C}(R) \cap L.$$

Our goal is to show that there exists $C \in \{X, Y\}$ such that $|\Pi_{i,C}(R) \cap L|$ is large.

For each $(x', y') \in L$, define the extension set

$$\text{ext}(x', y') := \{(x, y) \in R \cap D_0^I : x_{I'} = x', y_{I'} = y'\}.$$

We now show that

$$|\text{ext}(x', y')| \leq 2. \quad (1)$$

This follows from the assumption $R \cap D_i^I = \emptyset$. Suppose, for contradiction, that $|\text{ext}(x', y')| = 3$. Then all three extensions of (x', y') to coordinate i namely, $(x_i, y_i) = (0, 0), (1, 0), (0, 1)$ must be present in R . by the rectangle property of R , which would imply exists a pair $(x, y) \in R \cap D_i^I$ with $(x_i, y_i) = (1, 1)$, a contradiction. Hence, (1) holds.

Next, we partition L into two sets:

$$A := \{(x', y') \in L : |\text{ext}(x', y')| = 2\}, \quad B := \{(x', y') \in L : |\text{ext}(x', y')| = 1\}.$$

Observe that for any $(x', y') \in A$, both $(x', 0) \in X$ and $(y', 0) \in Y$, since R is a rectangle and both extensions with $x_i = 0$ and $y_i = 0$ must be in R . Therefore,

$$(x', y') \in \Pi_{i,C}(R) \quad \text{for all } C \in \{X, Y\},$$

which implies $|A| = |A \cap \Pi_{i,C}(R)|$ for any C .

For any such C , by (1), we have

$$2 \cdot |A \cap \Pi_{i,C}(R)| = 2 \cdot |A| \geq \left| \{(x, y) \in R \cap D_0^I : (x_{I'}, y_{I'}) \in A\} \right|.$$

For the B part, note that each $(x', y') \in B$ corresponds to a unique element in $R \cap D_0^I$, so

$$\left| \{(x, y) \in R \cap D_0^I : (x_{I'}, y_{I'}) \in B\} \right| = |B|.$$

Moreover, for each $(x', y') \in B$, there exists at least one choice of $C \in \{X, Y\}$ such that $(x', y') \in \Pi_{i,C}(R)$. By an averaging argument, there exists $C \in \{X, Y\}$ such that

$$2 \cdot |B \cap \Pi_{i,C}(R)| \geq |B| = \left| \{(x, y) \in R \cap D_0^I : (x_{I'}, y_{I'}) \in B\} \right|.$$

Putting both parts together, we have for this fixed C ,

$$\begin{aligned} 2 \cdot |L \cap \Pi_{i,C}(R)| &= 2 \cdot |A \cap \Pi_{i,C}(R)| + 2 \cdot |B \cap \Pi_{i,C}(R)| \\ &\geq \left| \{(x, y) \in R \cap D_0^I : (x_{I'}, y_{I'}) \in A\} \right| + \left| \{(x, y) \in R \cap D_0^I : (x_{I'}, y_{I'}) \in B\} \right| \\ &= |R \cap D_0^I|. \end{aligned}$$

Finally, using the definition of the density function:

$$\begin{aligned} E^{I'}(\Pi_{i,C}(R)) &= \log \left(\frac{|\Pi_{i,C}(R) \cap D_0^{I'}|}{3^{|I'|}} \right) = \log \left(\frac{3 \cdot |\Pi_{i,C}(R) \cap L|}{3^{|I|}} \right) \\ &\geq \log \left(\frac{3 \cdot |R \cap D_0^I|}{2 \cdot 3^{|I|}} \right) = E^I(R) + \log(3/2) \geq E^I(R) + \frac{1}{2}. \end{aligned}$$

This completes the proof. □