Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 73 (2025)

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

Guangxu Yang * Jiapeng Zhang *

April 7, 2026

Abstract

Numbers-on-Forehead (NOF) communication model is a central model in communication complexity. As a restricted variant, one-way NOF model is of particular interest. Establishing strong one-way NOF lower bounds has applications in circuit complexity, additive combinatorics, and cryptography. However, proving such lower bounds directly remains highly challenging due to a lack of effective techniques, leaving many fundamental questions wide open.

In this paper, we propose a new lifting theorem that establishes connections between *two-party* communication and *Numbers-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.

By our lifting theorem, we construct an explicit k-player function $f : [N]^k \to \{0,1\}$ such that: there exists a k-party randomized one-way NOF protocol computing it that sends a constant number of bits; but any k-party deterministic one-way NOF protocol computing it requires sending about $\Omega(\frac{\log N}{2^k})$ bits. In fact, our separation applies to a generalization of k-player one-way communication, where the first $k-1$ players speak freely, and the last player speaks once. At present, the best separation between deterministic and randomized NOF is $\Omega(\sqrt{\log N})$ vs $O(1)$ for three-party, due to Kelley and Lyu (FOCS 2025). Prior to our work, no stronger lower bound was known for any restricted communication model and for any number of players.

Beyond the lifting theorems, we demonstrate the versatility of our techniques by revisiting the Set Disjointness problem. We provide a simplified, alternative proof that the deterministic one-way three-party NOF complexity of disjointness is $\Omega(n)$, offering a new perspective on this classic problem beyond traditional discrepancy methods.

1 Introduction

Numbers-on-Forehead (NOF) communication, introduced by Chandra, Furst, and Lipton [CFL83], is a central model in communication complexity. In this model, the input is partitioned into k parts, and player i can see all parts except for their own (as if it were "written on their forehead").

*Research supported by NSF CAREER award 2141536.
Thomas Lord Department of Computer Science, University of Southern California.
Email: {guangxuy, jiapengz}@usc.edu

ISSN 1433-8092

Since its introduction, the NOF model has exhibited profound connections to a wide array of fields, including circuit complexity, streaming algorithms, additive combinatorics, and cryptography.

A remarkably natural and well-studied restriction of this model is *one-way* NOF communication model, in which each player is allowed to speak exactly once according to a fixed order. Studying the one-way model is compelling for two main reasons: first, since it is a natural weaker version, the techniques developed here may provide new insights into general NOF lower bounds; second, one-way NOF lower bounds are essentially sufficient for almost all downstream applications of the general model.

The major motivation for studying one-way Numbers-on-Forehead communication is to prove circuit lower bounds. Most notably, proving $\omega(\log n)$ lower bounds for any function f in k-party deterministic one-way NOF communication when $k = \log n$ will imply $f \notin \mathrm{ACC}^0$ circuits [HG90, BT94, Cha07, VW07]. Even more strikingly, achieving strong deterministic one-way NOF communication lower bounds for merely three players for some problems will imply the size-depth trade-off of Boolean circuits [Val77, PRS97], which is a long-standing open problem in circuit complexity.

Beyond circuit complexity, the ramifications of one-way NOF lower bounds permeate deeply into additive combinatorics. Remarkably, establishing strong deterministic one-way lower bounds for high-dimension permutaions intrinsically yields quantitative bounds for the Hales-Jewett theorem, constraints on dense Ruzsa-Szemer'edi graphs, and density bounds for 3-term arithmetic-progression-free sets [LS+17, JLL+25].

More broadly, one-way NOF communication model has wide applications in theoretical computer science, with particularly profound implications for cryptography. In cryptography, one-way NOF communication is intrinsically linked to Private Information Retrieval (PIR) [CKGS98], position-based cryptography [BDFP17], function inversion [CGK19], and leakage-resilient key exchange protocols [LMQW20]. Beyond these cryptographic primitives, it's further evidenced by its direct applications in distributed computing [DKO14], space-bounded pseudorandom generators [BNS92, GR14], oblivious branching programs [VW07], and streaming algorithms [Cha07, CDK19, KMPV19].

While the aforementioned applications highlight the importance of lower bounds, the one-way NOF model also admits surprising upper bounds. To the best of our knowledge, all known nontrivial protocols in the general NOF model are inherently one-way. This encompasses the $\sqrt{\log N}$ protocol for the *Exactly-N* problem [CFL83], the $O\left(\frac{n \log\log n}{\log n}\right)$ protocols for multipointer jumping [BS15] and Shifting [HG90], as well as the foundational Grolmusz-type protocols for the generalized inner product [Gro94] and set disjointness [RY20]. Furthermore, for a very natural class of functions [LS+17], such as the *Exactly-N* problem, the deterministic one-way NOF communication complexity is asymptotically equivalent to the deterministic NOF communication. Consequently, establishing lower bounds in the one-way NOF setting does not merely address a weakened model; it directly confronts and captures the full power of all existing NOF protocol techniques.

Motivated by these wide-ranging applications, developing new techniques for proving one-way NOF lower bounds is a crucial direction in communication complexity. Despite this, our understanding of the fundamental limits of the one-way NOF model is still preliminary. This knowledge gap primarily stems from a lack of generalizable techniques for establishing strong lower bounds. Currently, the primary tool is the generalized discrepancy method [She12, She14, RY15], which is largely restricted to low-discrepancy functions. While a few alternative approaches

exist [PRS97, VW07, KLM24, KL25], none have yet yielded a lower bound better than $\Omega(n^{1/(k-1)})$.

Lifting Theorems for One-Way Numbers-on-Forehead Communication Lifting theorems are a generic and powerful method for translating lower bounds from weaker computational models to stronger ones. A representative example is the query-to-communication lifting framework [RM97, Zha09, GPW18, PR17, GPW20, CFK+19, LMM+22, WYZ23, YZ24, MYZ25, WYY25], which converts query complexity lower bounds into communication lower bounds via gadget composition. This approach has driven a long line of successful research, yielding diverse applications in monotone circuit complexity, proof complexity, and combinatorial optimization. Yet, to the best of our knowledge, all existing lifting theorems apply only to two-party communication (or the closely related Numbers-in-Hand model). No lifting theorems have been established for the significantly more powerful Numbers-on-Forehead (NOF) model. Because one-way NOF lower bounds have profound connections to several major open problems but suffer from a severe lack of lower-bound techniques, developing NOF lifting theorems is a highly sought-after goal. Papers by Kumar, Meka, and Zuckerman [KMZ20], Pitassi [Pit21], and Beame [Bea24] have all raised the natural question:

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

This problem has remained resolutely open; in fact, the literature has lacked even plausible candidate statements for NOF lifting theorems. In this paper, we achieve a breakthrough by establishing the first lifting theorem that formally translates two-party lower bounds into the NOF model.

As a crucial first step in this direction, we prove a deterministic lifting theorem that converts two-party one-way communication lower bounds directly into one-way NOF lower bounds. By providing this lifting-based approach, we overcome the limitations of prior techniques and successfully resolve the fundamental open problems in one-way NOF communication. Specifically, we prove an explicit $\Omega(\frac{\log N}{2^k})$ versus $O(1)$ exponential separation between deterministic and randomized k-party one-way NOF communication, achieving a bound that is optimal for any constant k.

1.1 Our Main Results

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

Definition 1.1. *Let $f : [q] \times [q] \to \{0,1\}$ be a two-party base function and $g^k : [N]^k \to [q]$ be a k-party gadget. The lifted function over $k+1$ players, denoted as $f * g^k : [N]^k \times [q] \to \{0,1\}$, is defined by*

$$(f * g^k)(x_1, \ldots, x_k, z) = f(z, g^k(x_1, \ldots, x_k)).$$

In the standard $(k+1)$-party NOF setting, the inputs are distributed such that the $(k+1)$-th player sees $(x_1, \ldots, x_k)$ but not z, while for each $i \in [k]$, the i-th player sees all inputs except x_i.

A key observation driving our approach is that many canonical lower-bound candidates in the NOF model naturally fall into this lifted framework. Prominent examples include the *Generalized Inner Product* [RY20], *Set Disjointness* [RY20], *Pointer Jumping* [VW07, Cha07], and *Shifting* [PRS97] problems. 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 $\mathrm{EQ} * g$ by defining $g(x, y) := N - x - y$, and $\mathrm{EQ}(z, s) = 1$ if and only if $z = s$. Then, the condition $x + y + z = N$ holds if and only if $f(z, g(x, y)) = 1$.

To instantiate our lifting framework, we primarily rely on the Generalized Inner Product (GIP) function as our core gadget.

Definition 1.2. *Let q be a prime and $k, r \in \mathbb{N}^+$. The Generalized Inner Product function $\mathrm{GIP}^k_{q,r} : (\mathbb{F}_q^r)^k \to \mathbb{F}_q$ is defined as*

$$\mathrm{GIP}^k_{q,r}(x_1, \ldots, x_k) = \sum_{j \in [r]} \prod_{i \in [k]} x_{i,j}$$

where arithmetic operations are performed over the finite field $\mathbb{F}_q$. When the parameters q, r, and k are clear from the context, we simply write $\mathrm{GIP}(x_1, \ldots, x_k)$.

Building on this gadget, we establish our main technical result: a tight lifting theorem that translates the two-party one-way communication complexity of any base function f, denoted as $\mathrm{OCC}(f)$, directly into the one-way NOF communication complexity of the composed function $f * \mathrm{GIP}$, denoted as $\mathrm{OCC}^{\mathrm{NOF}}(f * \mathrm{GIP})$.

Theorem 1.3 (Main Theorem)**.** *Let q be a prime and k be a positive integer. Provided that $q, r = 2^{k+1}$, for any two-party Boolean function $f : [q] \times [q] \to \{0, 1\}$, we have*

$$\mathrm{OCC}^{\mathrm{NOF}}(f * \mathrm{GIP}^k_{q,r}) = \Theta(\mathrm{OCC}(f)).$$

Disjointness lower bounds. A preeminent challenge in NOF communication complexity is to establish an $\Omega(n)$ randomized lower bound for the Set Disjointness (DISJ) problem. This problem remains unresolved even in the three-party one-way NOF model and has profound implications for streaming algorithms [KMPV19] and distributed computing [DKO14].

Currently, the strongest deterministic lower bound of $\Omega(n)$ is obtained via the discrepancy method [RY15]. However, the discrepancy method faces an inherent "square-root barrier" in the NOF setting: it can only yield a randomized one-way lower bound of $\Omega(\sqrt{n})$ for DISJ, which is believed to be sub-optimal.

As a further demonstration of the versatility of our framework, we apply our techniques to provide a new, simplified proof for the deterministic one-way three-party NOF complexity of set disjointness.

Theorem 1.4. *The deterministic one-way three-party NOF complexity of Set Disjointness on n bits is $\Omega(n)$.*

In contrast to the discrepancy-based approach, our proof is built upon the lifting paradigm. By reducing the NOF problem to its two-party counterpart, our method circumvents the analytic limitations of discrepancy. We believe this lifting-based approach offers a more promising technical route toward resolving the $\Omega(n)$ randomized lower bound conjecture for NOF disjointness.

1.2 Applications of Our Main Theorem

We now discuss some applications of our main theorem.

1.2.1 Deterministic vs. randomized separation.

In the two-party setting, the equality function (EQ) is a well-known example demonstrating a separation between deterministic and randomized communication complexity. As a primary application of Theorem 1.3, we obtain an optimal, explicit separation between deterministic and randomized one-way NOF complexity by lifting the two-party EQ function.

Corollary 1.5. *For any $k \geq 2$ and $q, r = 2^k$, the deterministic one-way NOF complexity of $\mathsf{EQ} * \mathrm{GIP}^k_{q,r}$ is $\Omega(\frac{\log N}{2^k})$, while its randomized one-way NOF complexity is $O(1)$.*

Proof. It is a standard result in communication complexity that the two-party EQ function on $[q] \times [q]$ has a randomized one-way protocol with cost $O(1)$ using public coins. Since any $(k+1)$-party lifted function $f * g$ can be evaluated by having the $(k+1)$-th player first compute $s = g(x_1, \ldots, x_k)$ and then simulating the two-party protocol for $f(z, s)$, we have randomized one-way NOF complexity of $(\mathsf{EQ} * \mathrm{GIP})$ is $O(1)$

By our main lifting theorem (theorem 1.3), the deterministic one-way NOF complexity of the lifted function is tightly characterized by the two-party one-way complexity of the base function $\mathrm{OCC}^{\mathrm{NOF}}(\mathsf{EQ} * \mathrm{GIP}^k_{q,r}) = \Theta(\mathrm{OCC}(\mathsf{EQ}))$, For the EQ function on $[q] \times [q]$, the deterministic one-way communication complexity is well-known to be $\Omega(\log q)$. Since $N = q^r$ and $r = 2^{k+1}$, we observe $\log q = \log(N^{1/r}) = \frac{\log N}{r} = \frac{\log N}{2^{k+1}}$. Thus, $\mathrm{OCC}^{\mathrm{NOF}}(\mathsf{EQ} * \mathrm{GIP}) = \Omega\left(\frac{\log N}{2^k}\right)$.

Combining the two bounds yields the desired exponential separation of $\Omega(\frac{\log N}{2^k})$ versus $O(1)$ for any number of players k. □

Corollary 1.5 provides an explicit construction achieving an $\Omega(\log N)$ versus $O(1)$ separation for a constant number of players. This result resolves the quest for an optimal explicit separation in the one-way NOF setting, bypassing several long-standing technical barriers.

Comparison with Prior Work. Establishing an explicit separation between deterministic and randomized communication complexity remains a major open problem [BDPW10, KLM24, JLL+25, KL25]. Early work by Beame, David, Pitassi, and Woelfel [BDPW10] demonstrated an optimal separation by showing the existence of a three-party function $f : [N]^3 \to \{0, 1\}$ with randomized NOF complexity $O(1)$ and deterministic NOF complexity $\Omega(\log N)$. However, their result relied entirely on a counting argument and was inherently non-explicit.

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 $\Omega(\log \log \log N)$ [Shk06] until the recent breakthrough by Jaber, Liu, Lovett, Ostuni, and Sawhney [JLL+25], who showed an $\Omega((\log N)^{\Omega(1)})$ deterministic lower bound. For other explicit constructions, Kelley, Lovett, and Meka [KLM24] first established an $\Omega((\log N)^{1/3})$ versus $O(1)$ separation, a bound that was recently sharpened to $\Omega(\sqrt{\log N})$ versus $O(1)$ by Kelley and Lyu [KL25].

Compared to these advances, our work overcomes two fundamental limitations:

- Prior explicit techniques [KLM24, JLL+25, KL25] have struggled to reach lower bound better than $\Omega(\sqrt{\log N})$ bound even in the three-player one-way NOF setting. By using a lifting approach, we naturally inherit the strength of two-party lower bounds, achieving the optimal $\Omega(\log N)$ vs $O(1)$ separation.

- Proving deterministic lower bounds for $k > 3$ players is notoriously difficult. For instance, the result of [JLL+25] for *Exactly-N* degrades to $\Omega(\log\log\log\log N)$ for four players, and the previous best for $k > 3$ was only $\Omega(\log\log N)$ [BDPW10]. Our lifting theorem maintains its tightness for any constant k, providing the first optimal separation in this regime.

Prior to our work, no stronger lower bound was known for any restricted communication model and for any number of players. Also, in the quest to establish an optimal explicit separation between deterministic and randomized NOF communication, many candidate functions exhibit a remarkable property: *their deterministic one-way NOF communication complexity is asymptotically equivalent to deterministic NOF communication complexity*.

A prominent example is the *Exactly-N* function [RY20], where the deterministic one-way and NOF communication complexities coincide. More generally, this equivalence holds for the class of graph functions.

Definition 1.6 (Graph Function)**.** *A function $f : [N]^k \to \{0,1\}$ is a graph function if for every tuple of inputs $(x_2, \ldots, x_k)$ held by the first players, there exists a unique value $b \in [N]$ such that $f(b, x_2 \ldots, x_k) = 1$.*

For any such graph function, it is known that the deterministic one-way NOF communication complexity is equal to the deterministic NOF communication complexity [LS+17].

1.2.2 Lifting Theorems for Circuit Lower Bounds

A primary motivation for studying NOF communication is its deep connection to circuit complexity. Specifically, lower bounds on one-way NOF complexity translate directly into size lower bounds for SYM^+ circuits. These are depth-2 circuits consisting of a symmetric gate at the top and AND gates of fan-in at most k at the bottom.The importance of the class SYM^+ arises from its ability to simulate ACC^0: any circuit in ACC^0 can be transformed into a SYM^+ circuit of size $s = 2^{\mathrm{poly}(\log n)}$ with fan-in $k = \mathrm{poly}(\log n)$ [BT94]. The following classical result establishes the link between these models:

Theorem 1.7 ([HG90])**.** *If a function F is computable by a SYM^+ circuit (or a depth-2 unweighted threshold circuit) with size s and bottom fan-in k, then there exists a $(k+1)$-party deterministic one-way NOF protocol for F with cost*

$$\mathrm{OCC}^{\mathrm{NOF}}(F) = O(k \log s).$$

Currently, the strongest known lower bound via one-way NOF communication lower bounds for SYM^+ circuits is $s = \Omega(2^{n/2^k})$, established only for specific functions like the quadratic character [BNS92].

The motivation for our work mirrors the classical line of research for AC^0 circuits: just as Boppana [Bop97] established that small-size AC^0 circuits can't compute high average sensitivity functions, we show that small-size SYM^+ circuits can't compute functions composed with large one-way communication complexity. By combining theorem 1.7 with our main result (theorem 1.3), we derive a new lifting framework for circuit lower bounds:

Corollary 1.8. *Let f be a two-party function. Any SYM^+ circuit computing $f * \mathrm{GIP}^k_{q,r}$ with bottom fan-in k must have size*

$$s = 2^{\Omega(\mathrm{OCC}(f)/2^k)}.$$

Our lifting theorem generalizes the known result for SYM^+ circuits, providing a systematic way to produce SYM^+ lower bounds for a broad class of problems. Furthermore, a long-standing challenge in complexity theory is to prove $s = \omega(\text{poly}(n))$ when $k = \text{polylog}(n)$ for an explicit function, which would yield the first super-polynomial lower bounds for ACC^0 circuits. By reducing circuit size to two-party communication, our lifting theorem offers a promising new avenue toward resolving these fundamental questions in circuit complexity.

1.2.3 Round-communication trade-off in NOF

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 k-round and $k+1$-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 1.9. *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 $\text{Ind} : [q] \times [q] \to \{0,1\}$ 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 1.10. *For $k \geq 2$ and $r = 2^{k+1}$, the deterministic k-round NOF communication complexity of $\text{Ind} * \text{GIP}^k_{q,r}$ is $\Omega(\log q)$, while its $(k+1)$-round NOF communication complexity is $O(\log\log q)$.*

1.3 Discussion and Future Directions

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

Conjecture 1.11. *For any partial function $f : [q] \times [q] \to \{0,1\}$, we have*

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

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

Proving this conjecture would imply a separation between quantum and classical communication complexity in the one-way NOF model [YZ25]. Perhaps more importantly, we believe that the technical machinery required to resolve this conjecture would provide the necessary tools to prove an $\Omega(n)$ randomized lower bound for the Set Disjointness problem in the one-way NOF model.

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 $f : X \times Y \to \{0,1\}$. 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* $\mathrm{OCC}(f)$*.*

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* $f : [q] \times [q] \to \{0,1\}$*. 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* $f : X_1 \times \cdots \times X_k \to \{0,1\}$*. 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 $f(x_1, \ldots, x_k)$*.*

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

Definition 2.4. *A set* $S \subseteq X_1 \times \cdots \times X_k$ *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* $S = S_1 \cap \cdots \cap S_k$*, where each* S_i *is a cylinder.*

3 A Lifting Theorem for One-Way NOF Model

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

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

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

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

for any two-party communication problem $f : [q] \times [q] \to \{0,1\}$ and $r \geq 2^{k+1}$. The upper bound, i.e., $\mathrm{OCC}^{\mathrm{NOF}}(f * \mathrm{GIP}_{q,r}^k) = O(\mathrm{OCC}(f))$, 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 $|Z| = 2^{\mathrm{OCC}(f)}$. Our goal is to prove that

$$\mathrm{OCC}^{\mathrm{NOF}}(f * \mathrm{GIP}) = \Omega\left(\log |Z|\right).$$

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 $(\pi_1, \ldots, \pi_k)$, as well as distinct rows $z_0^*, z_1^* \in Z$ and inputs $(x_1^*, \ldots, x_k^*) \in [N]^k$, such that

- The first k players output $(\pi_1, \ldots, \pi_k)$ for both inputs $(x_1^*, \ldots, x_k^*, z_0^*)$ and $(x_1^*, \ldots, x_k^*, z_1^*)$.
- $(f * \mathrm{GIP})(x_1^*, \ldots, x_k^*, z_0^*) \neq (f * \mathrm{GIP})(x_1^*, \ldots, x_k^*, z_1^*)$.

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

Let Π be any one-way protocol with communication bits less than $(\log |Z|)/3$. By the pigeonhole principle, there exists a message tuple $(\pi_1, \ldots, \pi_k)$ 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

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

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,*

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

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

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

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 $(x_1^*, \ldots, x_k^*)$ in the intersection, i.e.,

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

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

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

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

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*

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

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

□

3.1 Proof of Lemma 3.1

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

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

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

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

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

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

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

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

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 $(2\sqrt{|L|}-1)^2 \geq |L|-1$. □

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 $v \in \mathbb{F}_q$,

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

Proof. Let $\mathbf{1}:\mathbb{F}_q\to\{0,1\}$ 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,

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

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

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

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

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

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

$$\gamma_\alpha^2 \leq \mathbb{E}_{x_1,\ldots,x_{k-1}}\left[\mathbf{1}_{S_k}(x_1,\ldots,x_{k-1})^2 \mathbb{E}_{x_k,x_k'}\left[\prod_{i=1}^{k-1}\mathbf{1}_{S_i}(x_1,\ldots,x_k)\mathbf{1}_{S_i}(x_1,\ldots,x_k')\chi_\alpha\left(\sum_j\left(x_{k,j}+x_{k,j}'\right)\prod_{i=1}^{k-1}x_{i,j}\right)\right]\right]$$

$$\leq \mathbb{E}_{x_k,x_k'}\mathbb{E}_{x_1,\ldots,x_{k-1}}\left[\prod_{i\in[k-1]}\left(\mathbf{1}_{S_i}(x_1,\ldots,x_k)\cdot\mathbf{1}_{S_i}(x_1,\ldots,x_k')\right)\chi_\alpha\left(\sum_j\left(x_{k,j}+x_{k,j}'\right)\prod_{i\in[k-1]}x_{i,j}\right)\right]$$

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

$$\gamma_\alpha^{2^{k-1}} \leq \mathbb{E}_{(x_2,\ldots,x_k),(x_2',\ldots,x_k')}\left[\left|\mathbb{E}_{x_1}\left[\chi_\alpha\left(\sum_j x_{1,j}\cdot\prod_{i>1}(x_{i,j}+x_{i,j}')\right)\right]\right|\right]$$

Recall that for any character χ_α, it holds that $\sum_{z\in\mathbb{F}_q}\chi_\alpha(z)=0$. Hence, for any $(x_2,\ldots,x_k),(x_2',\ldots,x_k')$, 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,

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

It implies that

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

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

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

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

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 $G:(\mathbb{F}_q^r)^k\to\{0,1\}$ be a function defined by*

$$G(x_1,\ldots,x_k)=\mathrm{GIP}(x_1,\ldots,x_k)\mod 2$$

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, $\mathrm{DISJ}_2(x, y) = 1$ if and only if x and y are disjoint, i.e., $\bigwedge_{i=1}^{n}(\overline{x}_i \vee \overline{y}_i)$.

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

$$\mathrm{DISJ}_3(x, y, z) := \mathrm{DISJ}_2\big(z,\ x \wedge y\big) = \bigwedge_{i=1}^{n} \left(\overline{z}_i \vee \overline{x}_i \vee \overline{y}_i\right).$$

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

Proof of Theorem 1.4. 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:

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

Define the set $D_0 := \left\{(x, y) \in \{0,1\}^n \times \{0,1\}^n : \bigwedge_{i=1}^{n}(\overline{x}_i \vee \overline{y}_i) = 1\right\}$, 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 of 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

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

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 $\mathbb{E}_{\ell,\ell'}\left[|N(\ell) \cap N(\ell')|\right]$ as

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

For the first term, we upper bound it by:

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

Hence, we have

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

Therefore, the contribution from the second term is at least

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

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

□

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 $d_H(z_0^*, z_1^*) \ge 0.1 \cdot n$ such that the following set

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

has large intersection with the set D_0, specifically,

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

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*

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

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 4.1 for completeness.

Since $d_H(z_0^*, z_1^*) \ge 0.1 \cdot n$, 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 $|T| \ge 0.1n$, 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

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

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

□

4.1 Proof of Lemma 4.3

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

Theorem 4.4 (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

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

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

Definition 4.5 (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 4.6 (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 $X' = \left\{x_{I\setminus\{i\}} : x \in X,\ x_i = 0\right\}$ and $Y' = \left\{y_{I\setminus\{i\}} : y \in Y\right\}$.*
- *If $C = Y$, then $X' = \left\{x_{I\setminus\{i\}} : x \in X\right\}$ and $Y' = \left\{y_{I\setminus\{i\}} : y \in Y,\ y_i = 0\right\}$.*

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 4.7. *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 4.7 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 4.8 (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*

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

Given Lemma 4.8 and Fact 4.7, 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 4.8, 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 4.8.

Proof of Lemma 4.8. 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

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

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

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

We now show that

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

This follows from the assumption $R \cap D_i^I = \emptyset$. Suppose, for contradiction, that $|\mathrm{ext}(x', y')| = 3$. 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:

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

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

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

For the B part, note that each $(x', y') \in B$ corresponds to a unique element in $R \cap D_{0'}^I$, so

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

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

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

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

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

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. □

Acknowledgements

The authors would like to thank Shachar Lovett, Xinyu Mao, Anthony Ostuni, Anup Rao, Tal Roth, Haoyu Wang, Shuo Wang, and Pei Wu for their insightful suggestions and valuable comments on an earlier version of this paper, which helped improve its presentation and technical depth.

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. 5, 6

[Bea24] Paul Beame. Cse 599i course notes: Spring 2024 — eth, seth and fine-grained complexity, lifting. Course notes, available online, 2024. 3

[BNS92] László Babai, Noam Nisant, and Márió Szegedy. Multiparty protocols, pseudorandom generators for logspace, and time-space trade-offs. *Journal of Computer and System Sciences*, 45(2):204–232, 1992. 2, 6

[Bop97] Ravi B Boppana. The average sensitivity of bounded-depth circuits. *Information processing letters*, 63(5):257–261, 1997. 6

[BS15] Joshua Brody and Mario Sanchez. Dependent random graphs and multiparty pointer jumping. *arXiv preprint arXiv:1506.01083*, 2015. 2

[BT94] Richard Beigel and Jun Tarui. On acc. *computational complexity*, 4(4):350–366, 1994. 2, 6

[CDK19] Graham Cormode, Jacques Dark, and Christian Konrad. Independent sets in vertex-arrival streams. In *46th International Colloquium on Automata, Languages, and Programming (ICALP 2019)*, pages 45–1. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2019. 2

[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. 3

[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. 1, 2, 5

[CGK19] Henry Corrigan-Gibbs and Dmitry Kogan. The function-inversion problem: Barriers and opportunities. In *Theory of Cryptography Conference*, pages 393–421. Springer, 2019. 2

[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, 3

[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. 7

[DKO14] Andrew Drucker, Fabian Kuhn, and Rotem Oshman. On the power of the congested clique model. In *Proceedings of the 2014 ACM symposium on Principles of distributed computing*, pages 367–376, 2014. 2, 4

[FKNN95] Tomás Feder, Eyal Kushilevitz, Moni Naor, and Noam Nisan. Amortized communication complexity. *SIAM Journal on computing*, 24(4):736–750, 1995. 8

[GPW18] Mika Göös, Toniann Pitassi, and Thomas Watson. Deterministic communication vs. partition number. *SIAM Journal on Computing*, 47(6):2435–2450, 2018. 3

[GPW20] Mika Göös, Toniann Pitassi, and Thomas Watson. Query-to-communication lifting for bpp. *SIAM Journal on Computing*, 49(4):FOCS17–441, 2020. 3

[GR14] Anat Ganor and Ran Raz. Space pseudorandom generators by communication complexity lower bounds. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM 2014)*, pages 692–703. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2014. 2

[Gro94] Vince Grolmusz. The bns lower-bound for multiparty protocols is nearly optimal. *Information and computation*, 112(1):51–54, 1994. 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, 6

[JLL+25] Michael Jaber, Yang P. Liu, Shachar Lovett, Anthony Ostuni, and Mehtaab Sawhney. Quasipolynomial bounds for the corners theorem, 2025. 2, 5, 6

[KL25] Zander Kelley and Xin Lyu. More efficient sifting for grid norms, and applications to multiparty communication complexity, 2025. 3, 5

[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, 5

[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, 4

[KMZ20] Ashutosh Kumar, Raghu Meka, and David Zuckerman. Bounded collusion protocols, cylinder-intersection extractors and leakage-resilient secret sharing. *Cryptology ePrint Archive*, 2020. 3

[LMM+22] Shachar Lovett, Raghu Meka, Ian Mertz, Toniann Pitassi, and Jiapeng Zhang. Lifting with sunflowers. *Leibniz international proceedings in informatics*, 215, 2022. 3

[LMQW20] Xin Li, Fermi Ma, Willy Quach, and Daniel Wichs. Leakage-resilient key exchange and two-seed extractors. In *Annual International Cryptology Conference*, pages 401–429. Springer, 2020. 2

[LS+17] Nati Linial, Adi Shraibman, et al. On the communication complexity of high-dimensional permutations. *arXiv preprint arXiv:1706.02207*, 2017. 2, 6

[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. 3, 7

[NW91] Noam Nisan and Avi Widgerson. Rounds in communication complexity revisited. In *Proceedings of the twenty-third annual ACM symposium on Theory of computing*, pages 419–429, 1991. 7

[Pit21] Toniann Pitassi. Advances and new directions in communication complexity. In *Invited talk at STOC 2021*, 2021. 3

[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. 3

[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, 3

[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. 7

[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. 3

[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. 2, 4

[RY20] Anup Rao and Amir Yehudayoff. *Communication Complexity: and Applications*. Cambridge University Press, 2020. 2, 3, 6

[She12] Alexander A Sherstov. The multiparty communication complexity of set disjointness. In *Proceedings of the forty-fourth annual ACM symposium on Theory of computing*, pages 525–548, 2012. 2

[She14] Alexander A Sherstov. Communication lower bounds using directional derivatives. *Journal of the ACM (JACM)*, 61(6):1–71, 2014. 2

[Shk06] Ilya D Shkredov. On a generalization of szemerédi's theorem. *Proceedings of the London Mathematical Society*, 93(3):723–760, 2006. 5

[Val77] Leslie G Valiant. Graph-theoretic arguments in low-level complexity. In *International Symposium on Mathematical Foundations of Computer Science*, pages 162–176. Springer, 1977. 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, 3, 7

[WYY25] Xudong Wu, Guangxu Yang, and Penghui Yao. A lifting theorem for hybrid classical-quantum communication complexity. *arXiv preprint arXiv:2511.17227*, 2025. 3

[WYZ23] Shuo Wang, Guangxu Yang, and Jiapeng Zhang. Communication complexity of set-intersection problems and its applications. In *In Electronic Colloquium on Computational Complexity (ECCC)(TR23-164)*, 2023. 3

[YZ22] Guangxu Yang and Jiapeng Zhang. Simulation methods in communication lower bounds, revisited. In *Electron. Colloquium Comput. Complex.*, 2022. 13, 14, 15

[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. 13, 14, 15

[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. 3

[YZ25] Guangxu Yang and Jiapeng Zhang. Quantum versus classical separation in simultaneous number-on-forehead communication. *CoRR*, abs/2506.16804, 2025. 8

[Zha09] Shengyu Zhang. On the tightness of the buhrman-cleve-wigderson simulation. In *International Symposium on Algorithms and Computation*, pages 434–440. Springer, 2009. 3

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il