Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 81 (2025)

Exponential Separation of Quantum and Classical One-Way Numbers-on-Forehead Communication

Guangxu Yang * Jiapeng Zhang *

March 19, 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 would imply circuit lower bounds, resolve well-known problems in additive combinatorics, and yield wide-ranging applications in areas such as cryptography and distributed computing. However, proving strong lower bounds in one-way NOF communication remains highly challenging; many fundamental questions in one-way NOF communication remain wide open. One of the fundamental questions, proposed by Gavinsky and Pudlák (CCC 2008), is to establish an explicit exponential separation between quantum and classical one-way NOF communication.

In this paper, we resolve this open problem by establishing the first exponential separation between quantum and randomized communication complexity in one-way NOF model. Specifically, we define a lifted variant of the Hidden Matching problem of Bar-Yossef, Jayram, and Kerenidis (STOC 2004) and show that it admits an $(O(\log n))$-cost quantum protocol in the one-way NOF setting. By contrast, we prove that any k-party one-way randomized protocol for this problem requires communication $\Omega(\frac{n^{1/3}}{2^{k/3}})$. Notably, our separation applies even to a generalization of k-player one-way communication, where the first player speaks once, and all other $k-1$ players can communicate freely.

1 Introduction

A fundamental objective in the study of quantum advantage is to exhibit computational separations across diverse models. Communication complexity has seen substantial progress toward this goal: a line of work [BCW98, Raz99, BYJK04, GKK+07, RK11, Gav16, GRT22, Gav19, Gav20, GGJL24] now establishes exponential separations in several two-party communication settings. Building on these foundations, Aaronson, Buhrman, and Kretschmer recently introduced *quantum information supremacy* [ABK24]—a paradigm focusing on tasks where a quantum device utilizes exponentially fewer resources (qubits) than any classical counterpart (bits). Their proposed task, rooted in the classical–quantum separation of the *Hidden Matching* problem, was recently realized in a landmark trapped-ion experiment [KGD+25].

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

ISSN 1433-8092

Despite these successes in two-party communication complexity, quantum advantage in the multiparty setting remains poorly understood. The premier model for multiparty communication is the Number-on-the-Forehead (NOF) model, introduced by Chandra, Furst, and Lipton [CFL83]. In this model, the input is partitioned into k parts, and player i can see all parts except their own (as if it were "written on their forehead"). While the $k = 2$ case coincides with the standard two-party model, for $k \geq 3$, NOF protocols can simulate a strictly broader range of computational models, making it a uniquely powerful and challenging framework. Recently, Göös, Gur, Jain, and Li [GGJL24] highlighted the separation of quantum and randomized communication in NOF models as a major open problem.

The main obstacle to obtaining strong separations between quantum and randomized protocols in the NOF model, already noted in [GGJL24, YZ25b], is the lack of techniques for proving lower bounds for deterministic and randomized NOF protocols. Most existing methods, such as the discrepancy method [RY15], apply equally well to quantum, randomized, and deterministic communication, making it difficult to distinguish the power of quantum versus classical protocols in the NOF setting [LS+09].

Therefore, it is natural to consider the quantum advantage of the NOF model in restricted settings. Similar to the research on two-party CC, the focus typically shifts from simultaneous models to one-way and then to two-way communication [BCW98, Raz99, BYJK04, GKK+07, RK11, Gav16, GRT22, Gav19, Gav20, GGJL24]. A remarkably natural and well-studied restriction of this model is the one-way NOF communication model, in which each player is allowed to speak exactly once according to a fixed order. Some progress has been made on the simultaneous NOF communication model, which is a weaker variant than the one-way NOF model. Gavinsky and Pudlák [GP08] established the first $O(\log n)$ vs $\Omega(n^{1/6k^2})$ separation between quantum and classical communication in the simultaneous NOF communication setting. Recently, Yang and Zhang [YZ25b] improved this to an $O(\log n)$ vs $\Omega(n^{1/16})$ separation for three-player simultaneous NOF. In [GP08] and [YZ25b], they further posed the following open problem:

Can exponential quantum advantage be established in one-way Numbers-on-Forehead communication?

As mentioned in [GP08], even the three-player case of one-way Numbers-on-Forehead communication is highly nontrivial and of independent interest.

Why we study one-way NOF communication. Although one-way NOF model may at first appear to be a restricted variant of the general NOF model, it nonetheless possesses significant theoretical motivations and a wide range of applications.

First, the model holds pivotal importance for several long-standing open problems in circuit complexity. For instance, proving an $\omega(\log n)$ lower bound for any function f in k-party deterministic one-way NOF communication with $k = \log n$ would imply that $f \notin \mathrm{ACC}^0$ [HG90, BT94, Cha07, VW07]. Even more strikingly, establishing strong deterministic one-way lower bounds for only three players in specific problems would yield significant size-depth trade-offs for Boolean circuits [Val77, PRS97]. Beyond circuit complexity, one-way NOF lower bounds have deep connections with additive combinatorics. Remarkably, establishing strong deterministic one-way NOF lower bounds for specific problems yields quantitative bounds for the Hales-Jewett theorem, dense Ruzsa-Szemer'edi graphs, k-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 protocols of Private Information Retrieval (PIR) [CKGS98], lower bounds in position-based cryptography, lower bounds in function inversion [BDFP17, CGK19], and leakage-resilient key exchange protocols [LMQW20]. Beyond these cryptographic primitives, it's further evidenced by its direct applications in lower bounds in distributed computing [DKO14], construction of space-bounded pseudorandom generators [BNS92, GR14],time-space trade-off of oblivious branching programs [VW07], and lower bounds of streaming algorithms [KMPV19].

Despite its profound implications and extensive applications, several fundamental questions regarding the one-way NOF communication model remain unresolved. Most notably, as recently highlighted by [GP08] and [YZ25b], establishing an explicit exponential separation between randomized and quantum one-way NOF communication remains a major open problem. Establishing strong lower bounds in one-way NOF communication remains highly challenging. In addition to the aforementioned discrepancy method, several other techniques have been developed for proving one-way NOF lower bounds [PRS97, BPSW05, VW07]. However, none of these approaches can surpass the $\Omega(n^{1/(k-1)})$ lower bound barrier.

Quantum advantage via lifting techniques 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 [RM97, Zha09, GPW18, PR17, GPW20, CFK+19, LMM+22, YZ24, MYZ25], which convert lower bounds in query complexity into communication complexity lower bounds, using a suitable base function composed with a gadget.

In the two-party setting, applying lifting to problems where quantum decision trees offer an exponential advantage over randomized ones, such as the Forrelation problem [Aar10, AA15], we can get the exponential separations between two-way quantum and classical communication complexity [GRT22, GGJL24]. Investigating whether similar lifting techniques can be extended to the more complex one-way NOF setting is a natural and highly promising direction.

Recently, Yang and Zhang [YZ25a] proposed a novel lifting framework connecting two-party communication with the Number-on-the-Forehead (NOF) model. Specifically, they established a deterministic lifting theorem that translates one-way two-party lower bounds into the one-way NOF setting. However, they left the randomized version as a significant open problem, achieving only deterministic bounds at present.

Inspired by the technique in [YZ25a], we successfully bypass this $\Omega(n^{1/(k-1)})$ lower bound barrier and resolve the aforementioned open problem. Specifically, we establish the first explicit exponential separation between randomized and quantum one-way NOF communication by using lifting techniques.

1.1 Our Contributions

In this paper, we establish the first exponential separation between quantum and randomized communication complexity in the one-way NOF model.

Our construction is based on a lifted version of the Hidden Matching (HM) problem introduced by Bar-Yossef et al. [BYJK04]. In the standard two-party HM problem:

1. Alice is given a string $z \in \{0,1\}^n$.

2. Bob is given a perfect matching $M \in \mathcal{M}_n$ on n nodes.

The goal is for Bob to output a tuple $\langle i, j, b\rangle$ such that the edge $(i, j) \in M$ and $b = z_i \oplus z_j$.

It was shown in [BYJK04] that HM admits an $O(\log n)$ simultaneous quantum protocol, whereas any one-way randomized protocol requires $\Omega(\sqrt{n})$ communication.

In our construction, we utilize a structured subset of perfect matchings. Fix m, for each $i \in [m]$, we define a perfect matching M_i between the sets $\{0, \ldots, m-1\}$ and $\{m, \ldots, 2m-1\}$ as:

$$M_i := \{(\ell, m + ((i + \ell) \bmod m)) : \ell \in [m]\}.$$

Let $\mathcal{M} = \{M_1, \ldots, M_m\}$ denote this collection. The Lifted Hidden Matching problem, denoted by HM $* g$, is defined as follows:

Definition 1.1. *Let $g : \{0,1\}^{n(k-1)} \to \{0,1\}^{n_0}$ be the gadget function with $n_0 = (\frac{n}{2^k})^{2/3}$. The Lifted Hidden Matching Problem, denoted HM $* g$, involves k inputs distributed among the players as follows: Let $m = n_0/2$,*

- *The i-th player receives $(x_1, ..., x_{i-1}, x_{i+1}, ..., x_k)$ where $x_1 \in [m]$ and $x_i \in \{0,1\}^n$ for $2 \le i \le k$.*

The goal is for the last player to output a tuple $\langle \ell, r, b\rangle$ such that $(\ell, r) \in M_{x_i}$ and $b = g(x_2, ..., x_k)_\ell \oplus g(x_2, ..., x_k)_r$.

Remarkably, this problem remains easy for quantum communication. Similar to the Hidden Matching Problem, the first player only needs to send a uniform superposition of the string $g(x_2, ..., x_k)$, with a communication cost of $O(\log n)$ qubits. The last player can then perform a measurement on this superposition, which depends on the matching M_{x_1}, and output the parity of some pair in M_{x_1} (see the appendix for more details). We note that other players do not need to send any message using this protocol. Thus, the main result of our paper is the $n^{\Omega(1)}$ randomized one-way NOF communication lower bound.

Theorem 1.2. *Let $n_0 = (\frac{n}{2^k})^{2/3}$, there exists an explicit gadget function $g : \{0,1\}^{n(k-1)} \to \{0,1\}^{n_0}$ such that the randomized one-way NOF communication complexity of HM $* g$ is $\Omega(\frac{n^{1/3}}{2^{k/3}})$.*

2 Preliminaries

2.1 Communication Complexity

We begin by recalling standard definitions in communication complexity. In the two-party communication model, Alice and Bob receive inputs $x \in X$ and $y \in Y$, respectively. Rather than computing a simple boolean function, their goal is to solve a *search problem* (or compute a relation) $\mathcal{P} \subseteq X \times Y \times Z$. For any given input (x, y), the objective is to output a valid answer $z \in Z$ such that $(x, y, z) \in \mathcal{P}$.

Definition 2.1 (Randomized one-way communication complexity)**.** *In the randomized one-way communication model, Alice and Bob share a public random string r. Alice sends a single message $\Pi(x, r)$ to Bob, and Bob outputs an answer $z \in Z$ based on y, the received message, and the shared randomness. A protocol has δ-error if, for every input (x, y), the probability over the shared randomness that Bob outputs an invalid answer is at most δ. The randomized one-way communication complexity of $\mathcal{P}$ with error δ is the maximum length of Alice's message over all inputs and random strings.*

By Yao's Minimax Principle, to prove a lower bound for randomized protocols with error δ in the worst case, it is sufficient to prove a lower bound for the *distributional complexity*—that is, the communication complexity of any deterministic protocol that errs with probability at most δ under a chosen input distribution (in our case, the uniform distribution).

Definition 2.2 (One-way NOF Communication Model for Search Problems)**.** *In the k-party one-way Numbers-on-Forehead (NOF) model, k players collaborate to solve a search problem $\mathcal{P} \subseteq X_1 \times \cdots \times X_k \times Z$. The inputs are distributed such that each player i knows all inputs except for their own x_i (i.e., player i sees x_{-i}).In the randomized one-way setting, the players communicate in a fixed order, from the first player to the last. Each player i sends a single message $\Pi_i(x_{-i}, r)$ based on their visible input, the previously sent messages, and the shared randomness r. The last player then outputs an answer $z \in Z$.*

Definition 2.3 (Cylinder Intersections)**.** *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.*

2.2 Basics of Information Theory

Our proof approach involves several standard definitions and results from information theory, which we now recall.

Definition 2.4 (Entropy)**.** *Given a random variable $\boldsymbol{X}$, the Shannon entropy of $\boldsymbol{X}$ is defined by*

$$\mathcal{H}(\boldsymbol{X}) := \sum_x \Pr(\boldsymbol{X} = x) \log\left(\frac{1}{\Pr(\boldsymbol{X} = x)}\right).$$

For two random variables $\boldsymbol{X}, \boldsymbol{Y}$, the conditional entropy of $\boldsymbol{X}$ given $\boldsymbol{Y}$ is defined by

$$\mathcal{H}(\boldsymbol{X} \mid \boldsymbol{Y}) := \mathbb{E}_{y \sim Y}\left[\mathcal{H}(\boldsymbol{X} \mid \boldsymbol{Y} = y)\right].$$

For $p \in [0, 1]$, the binary entropy function is defined as $H_2(p) = -p \log_2 p - (1 - p) \log_2(1 - p)$. It is well known that $H_2(p)$ is a concave function.

Lemma 2.5 (Subadditivity of Entropy)**.** *For a list of random variables $\boldsymbol{X}_1, \boldsymbol{X}_2, \ldots, \boldsymbol{X}_d$, we have:*

$$\mathcal{H}(\boldsymbol{X}_1, \boldsymbol{X}_2, \ldots, \boldsymbol{X}_d) \leq \sum_{i=1}^{d} \mathcal{H}(\boldsymbol{X}_i).$$

Definition 2.6 (Mutual Information)**.** *The mutual information between joint random variables $\boldsymbol{X}$ and $\boldsymbol{Y}$ is defined as*

$$\mathrm{I}(\boldsymbol{X}; \boldsymbol{Y}) = \mathcal{H}(\boldsymbol{X}) - \mathcal{H}(\boldsymbol{X}|\boldsymbol{Y}),$$

Lemma 2.7 (Data Processing Inequality)**.** *Consider random variables $\boldsymbol{X}, \boldsymbol{Y}, \boldsymbol{Z}$ forming a Markov chain $\boldsymbol{X} \to \boldsymbol{Y} \to \boldsymbol{Z}$. Then, the mutual information satisfies:*

$$\mathrm{I}(X; Y) \geq \mathrm{I}(X; Z).$$

Definition 2.8 (Hamming Distance)**.** *Let $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \{0, 1\}^n$ be two strings. Their Hamming distance $d_H(x, y)$ is defined as:*

$$d_H(x, y) := |\{i : x_i \neq y_i\}|.$$

Definition 2.9 (Total Variation Distance)**.** *For two discrete random variables $\boldsymbol{X}$ and $\boldsymbol{Y}$ taking values in a finite sample space Ω, the total variation distance between their probability distributions is defined as:*

$$\Delta_{TV}(\boldsymbol{X}, \boldsymbol{Y}) := \frac{1}{2} \sum_{\omega \in \Omega} |\Pr(\boldsymbol{X} = \omega) - \Pr(\boldsymbol{Y} = \omega)|.$$

In this paper, we use U_m to denote a random variable that is uniformly distributed over the Boolean hypercube $\{0,1\}^m$. For instance, $\Delta_{TV}(\boldsymbol{Z}, U_{n_0})$ measures the statistical distance between the distribution of a random variable $\boldsymbol{Z} \in \{0,1\}^{n_0}$ and the uniform distribution over $\{0,1\}^{n_0}$.

3 Quantum Advantage for One-Way NOF Communication

We prove the exponential separation between quantum and randomized one-way Numbers-on-Forehead (NOF) communication in this section. We first recall the statement.

Theorem 3.1 (Theorem 1.2 restated)**.** *There exists an explicit gadget function $g : \{0,1\}^{n(k-1)} \to \{0,1\}^{n_0}$ such that the randomized one-way NOF communication complexity of $HM * g$ is $\Omega\left(\frac{n^{1/3}}{2^{k/3}}\right)$.*

3.1 Step 1: Choosing the gadget function

Definition 3.2. *Let q be a prime power and $k, r > 0$. We define the function $\mathrm{GIP}^k_{q,r} : (\mathbb{F}_q^r)^k \to \mathbb{F}_q$ by*

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

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

We note that GIP is a cylinder intersection extractor:

Lemma 3.3. *[YZ25a] 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*

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

We modify the function $\mathrm{GIP}^{k-1}_{q,r}$ by setting the field size $q = 2^{n/2^k}$ and the number of blocks $r = 2^{k+1}$. We define our gadget function $g : \{0,1\}^{n(k-1)} \to \{0,1\}^{n_0}$ such that its output is represented by the first n_0 bits of $\mathrm{GIP}^{k-1}_{q,r}$.

Lemma 3.4. *Let $S \subseteq \{0,1\}^{n(k-1)}$ be any cylinder intersection of size $|S| \geq 2^{n(k-1) - n/2^k}$. Then for any $z \in \{0,1\}^{n_0}$,*

$$\Pr_{(x_2,\ldots,x_k) \in S}[g(x_2, \ldots, x_k) = z] \leq 2^{-n_0} + 2^{-2n_0}.$$

Proof. Let $N = n/2^k$, so the field size is $q = 2^N$. We identify $\mathbb{F}_q$ with the Boolean hypercube $\{0,1\}^N$. By the discrepancy bound for the GIP function over the cylinder intersection S, the distribution of

the full output of GIP is extremely close to uniform. Specifically, for any $y \in \{0,1\}^N$, the point-wise probability is bounded by:

$$\Pr_{(x_2,\ldots,x_k)\in S}[\mathrm{GIP}(x_2,\ldots,x_k) = y] \le 2^{-N} + 2^{-2N},$$

based on the exponential sum bound for our choice of $r = 2^{k+1}$ and $k \le \frac{\log n}{2}$.

Our gadget function $Z = g(x_2,\ldots,x_k)$ outputs exactly the first n_0 bits of GIP. For any specific prefix $z \in \{0,1\}^{n_0}$, there are exactly 2^{N-n_0} full outputs $y \in \{0,1\}^N$ that match this prefix. Therefore, the probability of obtaining z over the cylinder intersection S is the sum of the probabilities of these matching extensions:

$$\begin{aligned}\Pr_{(x_2,\ldots,x_k)\in S}[g(x_2,\ldots,x_k) = z] &= \sum_{y\in\{0,1\}^N : y \text{ matches } z} \Pr_{(x_2,\ldots,x_k)\in S}[\mathrm{GIP}(x_2,\ldots,x_k) = y] \\ &\le 2^{N-n_0}\left(2^{-N} + 2^{-2N}\right) \\ &= 2^{-n_0} + 2^{-N-n_0} \le 2^{-n_0} + 2^{-2n_0}.\end{aligned}$$

Where the last inequality follows by the fact that $n_0 = (n/2^k)^{2/3} \le n/2^k = N$. □

3.2 Step 2: Simplifying one-way NOF protocols

To prove the randomized communication lower bound, by Yao's minimax principle, it is sufficient to prove a lower bound for any protocol that achieves a constant advantage under a uniform input distribution.

To simplify our analysis, we first apply the following simplified process to any one-way NOF protocol. Let $m = n_0/2$ denote the number of possible matchings.

Definition 3.5 (Simplified protocols)**.** *For any protocol Π for HM $*$ g under the uniform distribution, we define its simplified version Π^* as follows:*

- *The first player sends $\Pi_1^*(x_{-1}) = \Pi_1(x_{-1})$.*
- *For each $2 \le i \le k$, the i-th player sends $\Pi_i^*(x_{-i}) = (\Pi_i(j, x_2, ..., x_{i-1}, x_{i+1}, ..., x_k))_{j\in[m]}$.*

The high-level intuition behind the simplified protocols is that each player i with $2 \le i \le k$ enumerates its transcript for all possible values of $x_1 \in [m]$ and sends the entire list. We observe the following useful property of simplified protocols.

Claim 3.6. *Let Π be a deterministic protocol for HM $*$ g with δ-error under the uniform distribution. Then the following statements hold:*

1. *The protocol Π^* is a deterministic protocol for HM $*$ g with δ-error under the uniform distribution.*
2. *$|\Pi_1^*| = |\Pi_1|$ and $|\Pi_i^*| = m\cdot|\Pi_i|$ for $2 \le i \le k$. The communication complexity of Π^* is $|\Pi_1| + m\cdot\sum_{i=2}^k |\Pi_i|$.*
3. *Under the uniform distribution, the protocol Π^* depend only on $(x_2, ..., x_k)$. That is, they are independent of x_1, respectively.*

Proof. The claim follows directly from the construction of Π^*. For item 1, the last player knows the actual value of x_1 (due to the NOF model) and can simply extract the x_1-th component from the tuple sent by each player $i \geq 2$. This perfectly simulates the original protocol Π, thus achieving the exact same δ-error. Item 2 is immediate since each player $i \geq 2$ sends exactly m simulated transcripts of Π_i. Item 3 holds because Player 1 does not see x_1 in the NOF model, and for $i \geq 2$, enumerating the messages over all possible dummy values $j \in [m]$ completely removes the dependence on the actual input x_1. □

We emphasize that item 3 is crucial and significantly simplifies our subsequent analysis. By ensuring that the entire communication transcript of Π^* is strictly independent of x_1, we can evaluate how much information the protocol reveals about the gadget output $g(x_2, \ldots, x_k)$ without needing to condition on the specific matching M_{x_1}.

3.3 Step 3: Proving communication lower bounds for simplified protocols

To analyze the communication complexity of simplified protocols, we begin with a key observation: since the protocol Π^* is independent of x_1, it inherently lacks information regarding the matching M_{x_1}. Consequently, to solve the Hidden Matching problem, Π^* must contain sufficient information about $g(x_2, \ldots, x_k)$. The intuition of our analysis is to consider two exhaustive cases based on how the information about g is distributed among the players:

- **Case 1:** The first player's message $\Pi_1^*(x_2, \ldots, x_k)$ contains enough information about $g(x_2, \ldots, x_k)$ such that the last player can compute HM $* g$. In this case, we must have $|\Pi_1^*| = \Omega(\sqrt{n_0})$, following the known randomized one-way communication complexity of the *Hidden Matching* problem [BYJK04].
- **Case 2:** The remaining $k-1$ players collectively communicate sufficient information about $g(x_2, \ldots, x_k)$ through NOF communication. In this case, the total communication must satisfy $\sum_{i=2}^{k} |\Pi_i^*| = \Omega(n/2^k)$. This follows from the *cylinder intersection extractor* properties of g, which dictate that the distribution of $g(x_2, \ldots, x_k)$ remains statistically close to uniform unless the communication is $\Omega(n/2^k)$.

This intuition is formalized in the following theorem:

Theorem 3.7. *Let $g : \{0,1\}^{n(k-1)} \to \{0,1\}^{n_0}$ be the gadget function described in Lemma 3.4. For any simplified protocol Π^* for HM $* g$ under the uniform distribution with error $1/16$, we have*

$$|\Pi_1^*| = \Omega(\sqrt{n_0}) \quad \text{or} \quad \sum_{i=2}^{k} |\Pi_i^*| = \Omega(n/2^k).$$

We observe that our main result (Theorem 1.2) follows as a direct consequence of Theorem 3.7. Setting the parameters $n_0 = \left(\frac{n}{2^k}\right)^{2/3}$ and $m = n_0/2$, by Theorem 3.7 and Claim 3.6, for any protocol Π for HM $* g$ under the uniform distribution with error $1/16$:

$$|\Pi| = \Omega\left(|\Pi_1^*| + \frac{1}{m}\sum_{i=2}^{k} |\Pi_i^*|\right) = \Omega\left(\frac{n^{1/3}}{2^{k/3}}\right).$$

This completes the proof of Theorem 1.2.

We now dedicate the remainder of this section to establishing Theorem 3.7. Let Π^* be any simplified protocol that solves HM $* g$ with an overall expected error at most $1/16$. Let $\boldsymbol{\tau}$ denote the random variable representing the full transcript of the protocol Π^*. Let the inputs $(\boldsymbol{x_2}, \ldots, \boldsymbol{x_k})$ be random variables uniformly distributed over $\{0,1\}^{(k-1)n}$, and let $Z = g(\boldsymbol{x_2}, \ldots, \boldsymbol{x_k}) \in \{0,1\}^{n_0}$ be the induced hidden target random variable.

Proof of Theorem 3.7. We assume the communication cost of players 2 through k is bounded by $c_0 = \sum_{i=2}^{k} |\Pi_i^*| = o(n/2^k)$. Let $c_1 = |\Pi_1^*|$ denote the communication cost of the first player. We aim to prove that $c_1 = \Omega(\sqrt{n_0})$.

The proof proceeds in two main parts. In the first part, we leverage the condition $c_0 = o(n/2^k)$ alongside the properties of our cylinder intersection extractor to establish an information upper bound of $\mathrm{I}(Z;\boldsymbol{\tau}) \le c_1 + 2$, which we formalize as Lemma 3.8. In the second part, we utilize the structural properties of the one-way Hidden Matching problem and simplified protocols to prove a matching lower bound of $\mathrm{I}(Z;\boldsymbol{\tau}) = \Omega(\sqrt{n_0})$, which we formalize as Lemma 3.9.

By combining Lemma 3.8 and Lemma 3.9, we immediately conclude that:

$$c_1 + 2 \ge \mathrm{I}(Z;\boldsymbol{\tau}) \ge \Omega(\sqrt{n_0}),$$

which directly implies $|\Pi_1^*| = c_1 = \Omega(\sqrt{n_0})$. This completes the proof of Theorem 3.7. □

We first prove the information upper bound.

Lemma 3.8. *Assuming the communication cost of players 2 through k in Π^* is $c_0 = o(n/2^k)$, then $\mathrm{I}(Z;\boldsymbol{\tau}) \le c_1 + 2$, where $c_1 = |\Pi_1^*|$.*

Proof of Lemma 3.8. Let $\mathcal{X} = X_2 \times \cdots \times X_k$ be the input space visible to the first player. By Claim 3.6, the entire protocol Π^* is independent of x_1. Thus, the transcript random variable $\boldsymbol{\tau} = (\boldsymbol{\tau}_1, \boldsymbol{\tau}_{>1})$ is solely determined by inputs uniformly drawn from $\mathcal{X}$. For any specific realization, the first player's message τ_1 confines the inputs to a subset $S_{\tau_1} \subseteq \mathcal{X}$, where there are at most 2^{c_1} such subsets. Given τ_1, the subsequent messages $\tau_{>1}$ partition $\mathcal{X}$ into at most 2^{c_0} cylinder intersections. Thus, any specific transcript $\tau = (\tau_1, \tau_{>1})$ is associated with a cylinder intersection C_τ. The actual set of valid inputs generating τ is exactly $S_{\tau_1} \cap C_\tau$.

Let $p_\tau = \Pr[\boldsymbol{\tau} = \tau] = \frac{|S_{\tau_1} \cap C_\tau|}{|\mathcal{X}|}$ be the true probability of generating τ, and let $q_\tau = \frac{|C_\tau|}{|\mathcal{X}|}$ be the volume of its corresponding cylinder intersection. Since $S_{\tau_1} \cap C_\tau \subseteq C_\tau$, we trivially have $p_\tau \le q_\tau$. Note that for any fixed τ_1, the cylinders $\{C_\tau\}_{\tau_{>1}}$ partition $\mathcal{X}$, meaning $\sum_{\tau_{>1}} q_\tau = 1$. Consequently, the sum over all possible transcript realizations is tightly bounded:

$$\sum_{\tau} q_\tau = \sum_{\tau_1} \sum_{\tau_{>1}} q_\tau \le 2^{c_1} \times 1 = 2^{c_1}.$$

We classify a transcript τ as "bad" if its cylinder is small, i.e., $q_\tau \le 2^{-n/2^k}$. Since there are at most 2^{c_0} cylinders for any fixed τ_1, the total measure of bad cylinders given τ_1 is at most $2^{c_0} \cdot 2^{-n/2^k} = 2^{c_0 - n/2^k}$. The overall probability that the protocol generates a bad transcript is bounded by summing q_τ over all bad τ:

$$\Pr[\boldsymbol{\tau} \in \mathrm{Bad}] = \sum_{\tau \in \mathrm{Bad}} p_\tau \le \sum_{\tau \in \mathrm{Bad}} q_\tau \le \sum_{\tau_1} 2^{c_0 - n/2^k} \le 2^{c_1 + c_0 - n/2^k}.$$

We can safely assume $c_1 \le \frac{1}{2}\Omega(n/2^k)$ (otherwise the desired bound $c_1 = \Omega(\sqrt{n_0})$ holds trivially). Given $c_0 = o(n/2^k)$, we have $c_1 + c_0 - n/2^k \le -\Omega(n/2^k)$. Thus, $\Pr[\boldsymbol{\tau} \in \text{Bad}] \le 2^{-\Omega(n/2^k)}$. With overwhelming probability $1 - 2^{-\Omega(n/2^k)}$, the transcript τ is "good".

For any valid good transcript τ (where $p_\tau > 0$ and $q_\tau > 2^{-n/2^k}$), C_τ is a large cylinder intersection. By Lemma 3.4, the target random variable $Z = g(x_2, \ldots, x_k)$ is extremely uniform over C_τ, bounded by $\Pr[Z = z \mid C_\tau] \le 2^{-n_0} + 2^{-2n_0} \le 2^{-n_0+1}$. Conditioned on the realized transcript $\boldsymbol{\tau} = \tau$, the probability of Z scales by the density. Let $x = (x_2, \ldots, x_k) \in \mathcal{X}$, we have:

$$\begin{aligned}
\Pr[Z = z \mid \boldsymbol{\tau} = \tau] &= \frac{|\{x \in S_{\tau_1} \cap C_\tau : g(x) = z\}|}{|S_{\tau_1} \cap C_\tau|} \\
&\le \frac{|\{x \in C_\tau : g(x) = z\}|}{|S_{\tau_1} \cap C_\tau|} \\
&= \frac{\Pr[Z = z \mid C_\tau] \cdot |C_\tau|}{|S_{\tau_1} \cap C_\tau|} \\
&= \frac{\Pr[Z = z \mid C_\tau] \cdot q_\tau}{p_\tau} \le \frac{q_\tau}{p_\tau} 2^{-n_0+1}.
\end{aligned}$$

Taking the logarithm, the conditional entropy given a specific good transcript is lower-bounded by:

$$\mathcal{H}(Z \mid \boldsymbol{\tau} = \tau) \ge n_0 - 1 - \log \frac{q_\tau}{p_\tau}.$$

We now calculate the expected conditional entropy over the random variable $\boldsymbol{\tau}$. Since entropy is non-negative, we can simply drop the contribution from bad transcripts:

$$\mathcal{H}(Z \mid \boldsymbol{\tau}) = \sum_\tau p_\tau \mathcal{H}(Z \mid \boldsymbol{\tau} = \tau) \ge \sum_{\tau \in \text{Good}} p_\tau \left(n_0 - 1 - \log \frac{q_\tau}{p_\tau} \right).$$

By applying Jensen's inequality to the logarithmic term over the good transcripts:

$$\sum_{\tau \in \text{Good}} p_\tau \log \frac{q_\tau}{p_\tau} \le \log \left(\sum_{\tau \in \text{Good}} p_\tau \frac{q_\tau}{p_\tau} \right) \le \log \left(\sum_\tau q_\tau \right) \le \log(2^{c_1}) = c_1.$$

Thus, the expected conditional entropy is firmly bounded by:

$$\mathcal{H}(Z \mid \boldsymbol{\tau}) \ge \Pr[\boldsymbol{\tau} \in \text{Good}](n_0 - 1) - c_1 \ge \left(1 - 2^{-\Omega(n/2^k)}\right)(n_0 - 1) - c_1 \ge n_0 - c_1 - 1 - o(1).$$

Since Z is uniform over the entire space $\mathcal{X}$, its unconditional entropy is $\mathcal{H}(Z) \ge n_0$. Therefore, the mutual information revealed by the protocol is:

$$\mathrm{I}(Z; \boldsymbol{\tau}) = \mathcal{H}(Z) - \mathcal{H}(Z \mid \boldsymbol{\tau}) \le n_0 - (n_0 - c_1 - 1 - o(1)) = c_1 + 2.$$

This completes the proof. □

Now we focus on the second part of the proof. Recall that the last Player k (acting as the referee) knows x_1 and the full transcript $\boldsymbol{\tau}$. Since Π^* solves $\mathrm{HM} * g$ with an expected error at most 1/16, the transcript must contain sufficient information to solve the Hidden Matching problem. The following lemma provides the required information lower bound.

Lemma 3.9. *Let Π^* be any simplified protocol that solves HM $*$ g with an overall expected error at most 1/16. Then, $\mathrm{I}(Z;\boldsymbol{\tau}) = \Omega(\sqrt{n_0})$.*

Proof of Lemma 3.9. Let $\mathcal{M} = \{M_1, \ldots, M_m\}$ be the set of $m = n_0/2$ edge-disjoint perfect matchings. Recall that the transcript $\boldsymbol{\tau}$ is independent of the first player's input x_1 (which uniformly determines the matching $\boldsymbol{M} \in \mathcal{M}$). Therefore, for any fixed transcript τ and a specific chosen matching $M \in \mathcal{M}$, the output of the protocol is a constant triple (i_M, j_M, b_M), where $(i_M, j_M) \in M$ is the predicted edge and $b_M \in \{0,1\}$ is the predicted parity. Since the output edge is guaranteed to be in M, an error occurs for a fixed M if and only if $b_M \neq Z_{i_M} \oplus Z_{j_M}$.

Let ε_τ denote the overall error probability of the protocol conditioned solely on the transcript $\boldsymbol{\tau} = \tau$. Since the overall expected error is $\mathbb{E}_{\boldsymbol{\tau}}[\varepsilon_{\boldsymbol{\tau}}] \leq 1/16$, Markov's inequality implies that $\Pr[\boldsymbol{\tau} \in \mathcal{T}_{\text{good}}] \geq 1/2$, where $\mathcal{T}_{\text{good}}$ is defined as the set of transcripts satisfying $\varepsilon_\tau \leq 1/8$.

Fix any good transcript $\tau \in \mathcal{T}_{\text{good}}$. Let

$$\varepsilon_{\tau,M} = \Pr[b_M \neq Z_{i_M} \oplus Z_{j_M} \mid \boldsymbol{\tau} = \tau, \boldsymbol{M} = M]$$

denote the error conditioned on both the transcript τ and a specific matching M.

Since the expected error over uniformly chosen matchings is $\mathbb{E}_{M \in \mathcal{M}}[\varepsilon_{\tau,M}] = \varepsilon_\tau \leq 1/8$, applying Markov's inequality again yields a subset of matchings $\mathcal{M}'_\tau := \{M \in \mathcal{M} : \varepsilon_{\tau,M} \leq 1/4\}$ of size $|\mathcal{M}'_\tau| \geq m/2 = n_0/4$. We construct a simple bipartite graph $G'_\tau = (L, R, E'_\tau)$ whose edges are exactly the constant predictions (i_M, j_M) made under each $M \in \mathcal{M}'_\tau$. Because the original matchings are mutually edge-disjoint, G'_τ contains exactly $|E'_\tau| = |\mathcal{M}'_\tau| \geq n_0/4$ edges.

By Turán's theorem, a simple bipartite graph containing a spanning forest of rank r spans at most $2r$ vertices and thus has at most r^2 edges. Consequently, the rank of G'_τ must be at least $\sqrt{|E'_\tau|} \geq \sqrt{n_0/4}$. Let $A_\tau \subseteq E'_\tau$ be such a spanning forest, which provides $|A_\tau| = \Omega(\sqrt{n_0})$ linearly independent edges.

Let $u_Z, v \in \{0,1\}^{|A_\tau|}$ denote the true parities and the predicted parities on A_τ, respectively. By construction, each edge $e \in A_\tau$ originates from a unique matching in $\mathcal{M}'_\tau$; let M_e denote this matching. Since every matching in $\mathcal{M}'_\tau$ has a conditional error of at most 1/4, the probability of predicting the wrong parity for edge e is exactly $\varepsilon_{\tau,M_e} \leq 1/4$. By linearity of expectation, the expected Hamming distance between the true and predicted parities on A_τ is bounded by:

$$\mathbb{E}_Z[d_H(u_Z, v) \mid \boldsymbol{\tau} = \tau] = \sum_{e \in A_\tau} \varepsilon_{\tau,M_e} \leq \frac{1}{4}|A_\tau|.$$

Next, we apply the following lemma, a generalization of Fano's inequality due to Bar-Yossef, Jayram, and Kerenidis [BYJK04], to upper bound the entropy of u_Z.

Lemma 3.10 ([BYJK04])**.** *Let $\boldsymbol{W}$ be a random variable over $\{0,1\}^k$, and suppose there exists a fixed vector $v \in \{0,1\}^k$ such that $\mathbb{E}[d_H(\boldsymbol{W}, v)] \leq \epsilon \cdot k$ for some $0 \leq \epsilon \leq 1/2$. Then the entropy of $\boldsymbol{W}$ is bounded by,*

$$\mathcal{H}(\boldsymbol{W}) \leq k \cdot H_2(\epsilon),$$

where $H_2(\cdot)$ is the binary entropy function.

Applying the generalized Fano's inequality (Lemma 3.10) with $k = |A_\tau|$ and error bound 1/4, we have $\mathcal{H}(u_Z \mid \boldsymbol{\tau} = \tau) \leq |A_\tau| H_2(1/4)$. Furthermore, because the forest A_τ is acyclic, its parities

impose $|A_\tau|$ independent linear constraints on Z, leaving exactly $n_0 - |A_\tau|$ bits of uncertainty for any fixed u_Z. By the chain rule,

$$\mathcal{H}(Z \mid \boldsymbol{\tau} = \tau) \leq \mathcal{H}(u_Z \mid \boldsymbol{\tau} = \tau) + \mathcal{H}(Z \mid u_Z, \boldsymbol{\tau} = \tau) \leq |A_\tau| H_2(1/4) + n_0 - |A_\tau| = n_0 - \Omega(\sqrt{n_0}).$$

Taking the expectation over $\boldsymbol{\tau}$ and using the trivial bound $\mathcal{H}(Z \mid \boldsymbol{\tau} = \tau) \leq n_0$ for bad transcripts, the overall conditional entropy is bounded by:

$$\mathcal{H}(Z \mid \boldsymbol{\tau}) \leq \frac{1}{2}(n_0) + \frac{1}{2}\left(n_0 - \Omega(\sqrt{n_0})\right) = n_0 - \Omega(\sqrt{n_0}).$$

Finally, since the unconditional entropy of the target is $\mathcal{H}(Z) \geq n_0$, the mutual information revealed by the protocol is precisely lower-bounded:

$$\mathrm{I}(Z; \boldsymbol{\tau}) = \mathcal{H}(Z) - \mathcal{H}(Z \mid \boldsymbol{\tau}) \geq \Omega(\sqrt{n_0}).$$

This completes the proof. □

References

[AA15] Scott Aaronson and Andris Ambainis. Forrelation: A problem that optimally separates quantum from classical computing. In *Proceedings of the forty-seventh annual ACM symposium on Theory of computing*, pages 307–316, 2015. 3

[Aar10] Scott Aaronson. Bqp and the polynomial hierarchy. In *Proceedings of the forty-second ACM symposium on Theory of computing*, pages 141–150, 2010. 3

[ABK24] Scott Aaronson, Harry Buhrman, and William Kretschmer. A qubit, a coin, and an advice string walk into a relational problem. In Venkatesan Guruswami, editor, *Proceedings of the 15th Innovations in Theoretical Computer Science Conference*, volume 287 of *LIPIcs*, pages 1:1–1:24. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2024. 1

[BCW98] Harry Buhrman, Richard Cleve, and Avi Wigderson. Quantum vs. classical communication and computation. In *Proceedings of the thirtieth annual ACM symposium on Theory of computing*, pages 63–68, 1998. 1, 2

[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. 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. 3

[BPSW05] Paul Beame, Toniann Pitassi, Nathan Segerlind, and Avi Wigderson. A direct sum theorem for corruption and the multiparty nof communication complexity of set disjointness. In *20th Annual IEEE Conference on Computational Complexity (CCC'05)*, pages 52–66. IEEE, 2005. 3

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

[BYJK04] Ziv Bar-Yossef, Thathachar S Jayram, and Iordanis Kerenidis. Exponential separation of quantum and classical one-way communication complexity. In *Proceedings of the thirty-sixth annual ACM symposium on Theory of computing*, pages 128–137, 2004. 1, 2, 3, 4, 8, 11, 16

[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. 2

[CGK19] Henry Corrigan-Gibbs and Dmitry Kogan. The function-inversion problem: Barriers and opportunities. In *Theory of Cryptography Conference*, pages 393–421. Springer, 2019. 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. 3

[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. 3

[Gav16] Dmitry Gavinsky. Entangled simultaneity versus classical interactivity in communication complexity. In *Proceedings of the forty-eighth annual ACM symposium on Theory of Computing*, pages 877–884, 2016. 1, 2

[Gav19] Dmitry Gavinsky. Quantum versus classical simultaneity in communication complexity. *IEEE Transactions on Information Theory*, 65(10):6466–6483, 2019. 1, 2

[Gav20] Dmitry Gavinsky. Bare quantum simultaneity versus classical interactivity in communication complexity. In *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*, pages 401–411, 2020. 1, 2

[GGJL24] Mika Göös, Tom Gur, Siddhartha Jain, and Jiawei Li. Quantum communication advantage in tfnp. *arXiv preprint arXiv:2411.03296*, 2024. 1, 2, 3

[GKK+07] Dmitry Gavinsky, Julia Kempe, Iordanis Kerenidis, Ran Raz, and Ronald De Wolf. Exponential separations for one-way quantum communication complexity, with applications to cryptography. In *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, pages 516–525, 2007. 1, 2

[GP08] Dmitry Gavinsky and Pavel Pudlák. Exponential separation of quantum and classical non-interactive multi-party communication complexity. In *2008 23rd Annual IEEE Conference on Computational Complexity*, pages 332–339, 2008. 2, 3

[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. 3

[GRT22] Uma Girish, Ran Raz, and Avishay Tal. Quantum versus randomized communication complexity, with efficient players. *computational complexity*, 31(2):17, 2022. 1, 2, 3

[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. 2

[KGD+25] William Kretschmer, Sabee Grewal, Matthew DeCross, Justin A. Gerber, Kevin Gilmore, Dan Gresh, Nicholas Hunter-Jones, Karl Mayer, Brian Neyenhuis, David Hayes, and Scott Aaronson. Demonstrating an unconditional separation between quantum and classical information resources, 2025. 1

[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. 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. 3

[LS+09] Troy Lee, Adi Shraibman, et al. Lower bounds in communication complexity. *Foundations and Trends® in Theoretical Computer Science*, 3(4):263–399, 2009. 2

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

[Raz99] Ran Raz. Exponential separation of quantum and classical communication complexity. In *Proceedings of the thirty-first annual ACM symposium on Theory of computing*, pages 358–367, 1999. 1, 2

[RK11] Oded Regev and Bo'az Klartag. Quantum one-way communication can be exponentially stronger than classical communication. In *Proceedings of the forty-third annual ACM symposium on Theory of computing*, pages 31–40, 2011. 1, 2

[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

[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

[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

[YZ25a] Guangxu Yang and Jiapeng Zhang. Deterministic lifting theorems for one-way number-on-forehead communication. *arXiv preprint arXiv:2506.12420*, 2025. 3, 6

[YZ25b] Guangxu Yang and Jiapeng Zhang. Quantum versus classical separation in simultaneous number-on-forehead communication. *CoRR*, abs/2506.16804, 2025. 2, 3

[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

Appendix

Quantum protocols for HM $*$ g [BYJK04]: We present a quantum protocol for lifted hidden matching problem with communication complexity of $O(\log n)$ qubits. and $x_2, ..., x_k \in \{0,1\}^n$ be the first player's input and $x_1, ..., x_{k-1} \in \{0,1\}^n$ be the last player's input.

Let $z = (z_1, ..., z_{n_0}) = g(x_2, ..., x_k)$.

1. The first player sends the state $|\psi\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n_0} (-1)^{z_i} |i\rangle$.

2. The last player performs a measurement on the state $|\psi\rangle$ in the orthonormal basis

$$B = \left\{ \frac{1}{\sqrt{2}}(|k\rangle \pm |\ell\rangle) \mid (k,\ell) \in M_{x_1)} \right\}.$$

The probability that the outcome of the measurement is a basis state $\frac{1}{\sqrt{2}}(|k\rangle + |\ell\rangle)$ is

$$|\langle\psi| \frac{1}{\sqrt{2}}(|k\rangle + |\ell\rangle)\rangle|^2 = \frac{1}{2n} \left((-1)^{z_k} + (-1)^{z_\ell}\right)^2.$$

This equals $2/n$ if $z_k \oplus z_\ell = 0$ and 0 otherwise. Similarly, for the states $\frac{1}{\sqrt{2}}(|k\rangle - |\ell\rangle)$, we have that

$$|\langle\psi| \frac{1}{\sqrt{2}}(|k\rangle - |\ell\rangle)\rangle|^2 = 0 \quad \text{if } z_k \oplus z_\ell = 0, \text{ and } \frac{2}{n} \text{ if } z_k \oplus z_\ell = 1.$$

Hence, if the outcome of the measurement is a state $\frac{1}{\sqrt{2}}(|k\rangle + |\ell\rangle)$, then the last player knows with certainty that $z_k \oplus z_\ell = 0$ and outputs $\langle k, \ell, 0\rangle$. If the outcome is a state $\frac{1}{\sqrt{2}}(|k\rangle - |\ell\rangle)$, then the last player knows with certainty that $z_k \oplus z_\ell = 1$ and hence outputs $\langle k, \ell, 1\rangle$. Note that the measurement depends only on the last player's input and that the algorithm is 0-error.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il