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

Quantum versus Classical Separation in Simultaneous Number-on-Forehead Communication

Guangxu Yang * Jiapeng Zhang *

June 20, 2025

Abstract

Quantum versus classical separation plays a central role in understanding the advantages of quantum computation. In this paper, we present the first exponential separation between quantum and bounded-error randomized communication complexity in a variant of the Number-on-Forehead (NOF) model. Namely, the three-player *Simultaneous Number-on-Forehead* model. Specifically, we introduce the *Gadgeted Hidden Matching Problem* and show that it can be solved using only $O(\log n)$ simultaneous quantum communication. In contrast, any simultaneous randomized protocol requires $\Omega(n^{1/16})$ communication.

On the technical side, a key obstacle in separating quantum and classical communication in NOF models is that all known randomized NOF lower bound tools, such as the discrepancy method, typically apply to both randomized and quantum protocols. In this regard, our technique provides a new method for proving randomized lower bounds in the NOF setting and may be of independent interest beyond the separation result.

1 Introduction

One of the central goals in the study of quantum advantage is to demonstrate separations between quantum and classical computation in various computational models. In this direction, substantial progress has been achieved in communication complexity, where a line of work [BCW98, Raz99, BYJK04, GKK+07, RK11, Gav16, GRT22, Gav19, Gav20, GGJL24] has established exponential separations in multiple settings. These results provide explicit problems that can be solved by quantum protocols using only $(\log n)^{O(1)}$ communication, whereas any classical randomized protocol solving the same problem must use $n^{\Omega(1)}$ communication.

However, all of the aforementioned results pertain to two-party communication models. In contrast, separations in multiparty communication, specifically the Number-on-Forehead (NOF) models, remain poorly understood. Lower bounds in the NOF models are especially intriguing because NOF protocols can simulate a broader range of computational models than those in the two-party setting. To this end, Göös, Gur, Jain, and Li [GGJL24] highlighted the separation of quantum and randomized communication in NOF models as an important open problem.

The main obstacle to obtaining strong quantum-versus-classical separations in the NOF setting, as noted by [GGJL24], lies in the lack of techniques for proving lower bounds for randomized

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

ISSN 1433-8092

NOF protocols. Existing approaches, such as the discrepancy method, often apply equally well to quantum communication, making it difficult to distinguish between the power of quantum and classical protocols in the NOF model [LSS09].

In this paper, we study the *simultaneous NOF model*, a variant of the NOF communication model. In this setting, each player i sends a single message, computed based on all inputs except x_i, to a referee (or the last player), who then determines the output after receiving all the messages. Although the simultaneous NOF model appears weaker than the standard NOF model, proving strong lower bounds in this setting remains highly challenging.

Strong simultaneous NOF lower bounds have significant implications in various areas, including lower bounds for the ACC circuit class [HG90, PRS97], private information retrieval [CKGS98], and position-based cryptography [BDFP17]. Furthermore, many known non-trivial NOF protocols such as the $\sqrt{\log N}$ protocol for *Exactly-N* [CFL83], the $O\left(\frac{n \log\log n}{\log n}\right)$ for multipointer jumping [BS15] and Shifting [HG90], and Grolmusz protocols for generalized inner-product [Gro94] and set disjointness [RY20] are all simultaneous protocols.

1.1 Our Results

In this paper, we establish the first exponential separation between quantum and bounded-error randomized communication complexity in the simultaneous NOF model. Our problem is inspired by the *Hidden Matching Problem* introduced by [BYJK04]. In the Hidden Matching Problem,

1. Alice is given a string $z \in \{0,1\}^n$.
2. Bob is given $M \in \mathcal{M}_n$ where $\mathcal{M}_n$ denotes the family of all possible perfect matchings on n nodes.

Their goal is for Bob to output a tuple $\langle i, j, b\rangle$ such that the edge (i, j) belongs to M and $b = z_i \oplus z_j$. As shown in [BYJK04], the Hidden Matching Problem admits an $O(\log n)$ simultaneous quantum communication protocol, while any one-way randomized protocol requires $\Omega(\sqrt{n})$ communication.

Inspired by [BYJK04], we introduce the *Gadgeted Hidden Matching Problem* (GHM). Let $m := n/2$. For each $i \in [m]$, we define a perfect matching M_i between $\{0, \ldots, m-1\}$ 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 the collection of these matchings. The GHM is defined as follows:

Definition 1.1. Let $g : \{0,1\}^n \times \{0,1\}^n \to [m]$ be any gadget function. The *Gadgeted Hidden Matching Problem*, denoted GHM $\circ\, g$, involves three inputs distributed among the players as follows:

- Alice receives $z, y \in \{0,1\}^n$,
- Bob receives $z, x \in \{0,1\}^n$,
- Charlie receives $x, y \in \{0,1\}^n$.

The goal is for Charlie to output a tuple $\langle \ell, r, b\rangle$ such that $(\ell, r) \in M_{g(x,y)}$ and $b = z_\ell \oplus z_r$.

Remarkably, this problem remains easy for quantum communication. Similar to the Hidden Matching Problem, Alice only needs to send a uniform superposition of the string z, with a communication cost of $O(\log n)$ qubits. Charlie can then perform a measurement on this superposition, which depends on the matching $M_{g(x,y)}$, and output the parity of some pair in $M_{g(x,y)}$ (see the appendix for more details). We note that Bob does not need to send any message using this protocol. Thus, the main result of our paper is the $n^{\Omega(1)}$ randomized simultaneous NOF communication.

Theorem 1.2. *There exists an explicit gadget function $g : \{0,1\}^n \times \{0,1\}^n \to [m]$ such that the randomized simultaneous NOF communication complexity of GHM $\circ\, g$ is $\Omega(n^{1/16})$.*

When g is clear from context, we simplify GHM $\circ\, g$ to GHM.

2 Preliminaries

We begin by fixing some notation. The set of integers $\{0, \ldots, n-1\}$ is denoted by $[n]$. We use capital letters like X to denote sets, and bold symbols like $\boldsymbol{X}$ to denote random variables. In particular, for a set X, we use $\boldsymbol{X}$ to denote the random variable that is uniformly distributed over the set X.

A *search problem* is a relation $S \subseteq X \times Y \times Z \times Q$, where Q is the set of possible solutions. On input $(x, y, z) \in X \times Y \times Z$, the goal is to find a solution $q \in Q$ such that $(x, y, z, q) \in S$. Note that for the (Gadgeted) Hidden Matching Problem, all inputs are guaranteed to have at least one solution.

2.1 Simultaneous Number-on-Forehead Model

In the three-party simultaneous NOF communication complexity model, Alice, Bob, and Charlie collaborate to compute a search problem $S \subseteq X \times Y \times Z \times Q$. Their inputs are as follows:

- Alice receives $(y, z) \in Y \times Z$.
- Bob receives $(x, z) \in X \times Z$.
- Charlie receives $(x, y) \in X \times Y$.

The randomized SM protocol $\Pi = (\Pi_A, \Pi_B, \Pi_C)$ proceeds as follows:

1. Alice and Bob simultaneously send messages to Charlie, where Alice's message $\Pi_A(y, z, r)$ depends only on the input (y, z) and public randomness r and Bob's message $\Pi_B(x, z, r)$ depends only on the input (x, z) and public randomness r.
2. After receiving both messages, Charlie outputs a solution $q = \Pi_C(\Pi_A(y, z), \Pi_B(x, z), x, y, r) \in Q$.

The protocol Π computes S with error ϵ if for any (x, y, z), $\mathbf{Pr}_r[(x, y, z, q) \in S] \geq 1 - \epsilon$.

2.2 Basics of Information Theory

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

Definition 2.1 (Entropy)**.** Given a random variable X, the Shannon entropy of X is defined by

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

For two random variables X, Y, the *conditional entropy* of X given Y is defined by

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

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 2.2 (Subadditivity of Entropy)**.** *For a list of random variables $X_1, X_2, \ldots, X_d$, we have:*

$$\mathbf{H}(X_1, X_2, \ldots, X_d) \leq \sum_{i=1}^{d} \mathbf{H}(X_i).$$

Definition 2.3 (Mutual Information)**.** The mutual information between joint random variables X and Y is defined as

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

Lemma 2.4 (Data Processing Inequality)**.** *Consider random variables X, Y, Z forming a Markov chain $X \to Y \to Z$. Then, the mutual information satisfies:*

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

Definition 2.5 (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:

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

3 The Randomized Lower Bound

We prove the our main theorem in this section. We first recall the statement.

Theorem 3.1 (Theorem 1.2 restated)**.** *There is a gadget g. Any randomized simultaneous NOF protocol that computes GHM $\circ$ g with an error probability less than $1/8$ requires $\Omega(n^{1/16})$ bits of communication.*

To prove the randomized communication lower bound, we first describe the gadget function and a hard input distribution for the communication problem.

3.1 The Gadgets and Hard Distributions

For $n > 0$, we set $m = n/2$ to be a prime [1] and $\alpha = \lfloor\sqrt{m}\rfloor$ in our proof.

[1] Using a prime number when proving the lower bound is reasonable, because for every integer n there exists a prime in the interval $[n/2, n]$.

Definition 3.2 (Rich gadgets)**.** For $\alpha > 0$, we say that a gadget $g : \{0,1\}^n \times \{0,1\}^n \to [m]$ is *α-rich* if for every subset $Q \subseteq [m]$ with $|Q| = \alpha$, there exist sets $S, T \subseteq \{0,1\}^n$ with $|S| = |T| = \sqrt{\alpha}$ such that

$$\{g(x,y) : x \in S, y \in T\} = Q.$$

It is not difficult to construct rich gadgets under our parameter choices. Note that the total number of subsets $Q \subseteq [m]$ of size $|Q| = \alpha$ is at most

$$\binom{m}{\alpha} \leq m^{\sqrt{m}} = 2^{o(n)}.$$

Therefore, we can assign disjoint sets S_Q and T_Q for each Q and enforce that $g(S_Q, T_Q) = Q$. In the following proof, we fix the gadget g to be any α-rich gadget. We then define the hard distributions.

Definition 3.3. Given $S, T \subseteq \{0,1\}^n$ with $|S| = |T| = \sqrt{\alpha}$, we define the distribution $\mu(S,T)$ on $\{0,1\}^n \times \{0,1\}^n \times \{0,1\}^n$ as follows:

- Uniformly sample $x \in S$, $y \in T$ and $z \in \{0,1\}^n$.
- Output the triple (x, y, z).

In our proof, we show that there exists a pair (S,T) such that $\mu(S,T)$ is hard for any protocol. The choice of S and T depends on the gadget g.

3.2 Local Independent Protocols

To simplify our analysis, we first apply the following *local independentization* process to any simultaneous NOF protocol.

Definition 3.4 (Local independent protocols)**.** For fixed sets $S, T \subseteq \{0,1\}^n$ with $|S| = |T| = \sqrt{\alpha}$, and any protocol Π for GHM$\circ g$ under the distribution $\mu(S,T)$, we define its *local independentized* version Π^* as follows:

- For any $(y,z) \in T \times Z$, $\Pi^*_A(y,z)$ outputs the tuple $(\Pi_A(u,z))_{u \in T}$.
- For any $(x,z) \in S \times Z$, $\Pi^*_B(x,z)$ outputs the tuple $(\Pi_B(v,z))_{v \in S}$.
- $\Pi^*_C(x, y, \Pi^*_A(y,z), \Pi^*_B(x,z))$ outputs the same value as $\Pi_C(x, y, \Pi_A(y,z), \Pi_B(x,z))$.

The high-level intuition behind the local independentization process is that both Alice and Bob enumerate all their possible inputs and output all corresponding transcripts. We observe the following useful property of locally independent protocols.

Claim 3.5. *Let Π be a deterministic protocol for GHM$\circ g$ with δ-error under the distribution $\mu(S,T)$. Then the following statements hold:*

1. *The protocol Π^* is a deterministic protocol for GHM$\circ g$ with δ-error under the distribution $\mu(S,T)$.*
2. *The communication complexity Π^* is $\sqrt{\alpha} \cdot \mathrm{CC}(\Pi)$.*
3. *Under the distribution $\mu(S,T)$, the messages $\Pi^*_A(y,z)$ and $\Pi^*_B(x,z)$ depend only on z. That is, they are independent of y and x, respectively.*

The third item significantly simplifies our analysis. The proof of this claim is straightforward and is omitted here.

3.3 Information Complexity of Local Independent Protocols

Now we are ready to prove the main result. Our proof is based on lower bounding the information complexity. However, instead of analyzing the standard information complexity $\mathrm{I}(Z : \mathbf{\Pi})$, we lower bound the information complexity for the local independent protocols.

Theorem 3.6. *Let g be an α-rich gadget. There exist sets $S, T \subseteq \{0,1\}^n$ with $|S| = |T| = \sqrt{\alpha}$ such that for any protocol Π of GHM $\circ\, g$ under the distribution $\mu(S,T)$ with error $1/16$, we have*

$$\mathrm{I}(Z : \mathbf{\Pi^*}) = \Omega(m^{5/16}).$$

We note that our main theorem (Theorem 1.2) is a direct consequence of Theorem 3.6. By Theorem 3.6, we know the communication complexity of Π^* is at least $\Omega(m^{5/16})$, and hence the communication complexity of Π is at least $\Omega(m^{5/16}/\sqrt{\alpha}) = \Omega(m^{1/16})$.

Proof of Theorem 3.6. The proof proceeds by carefully constructing the sets S and T based on the gadget function g and the combinatorial structure provided by the following lemma.

Lemma 3.7. *There is a sequence $Q \in [m]^\alpha$ consisting of distinct elements such that for any subsequence $Q' = (q_1, \ldots, q_r) \subseteq Q$ with $r \geq \alpha/2$, the following holds: for any sequence $L = (\ell_1, \ldots, \ell_r)$, either*

- *L contains at least $\Omega(m^{5/16})$ distinct elements, or*
- *the set $R := \{m + ((\ell_i + q_i) \bmod m) \mid 1 \leq i \leq r\}$ satisfies $|R| \geq \Omega(m^{5/16})$.*

We defer the proof of Lemma 3.7 to Section 3.3.1 and first prove Theorem 3.6 by assuming it. Let $Q \in [m]^\alpha$ be the sequence guaranteed by the Lemma 3.7. Since g is a α-rich gadget, there exist subsets $S, T \subseteq \{0,1\}^n$ with $|S| = |T| = \sqrt{\alpha}$ such that,

$$\{g(x,y) : x \in S, y \in T\} = Q.$$

Now we show that this pair S, T is the desired set that satisfies Theorem 3.6. Let Π be a deterministic protocol for GHM $\circ\, g$ under $\mu(S,T)$, and let Π^* be the local independentized version of it. Our goal is to prove a lower bound on the mutual information $\mathrm{I}(Z : \mathbf{\Pi^*})$. Recall that the output of Π^* has the form

$$\Pi^*(x,y,z) = (\Pi^*_A(z), \Pi^*_B(z), \Pi^*_C(x,y,\Pi^*_A(z), \Pi^*_B(z))).$$

Here $\Pi^*_A(z), \Pi^*_B(z)$ depend only on z as Π^* is locally independent. The output of Π^*_C is a triple (ℓ, r, b), where $\ell, r \in [n]$ and $b \in \{0,1\}$. The output is correct if (ℓ, r) is an edge in $M_{g(x,y)}$ and $b = z_\ell \oplus z_r$.

Since Charlie knows the matching $M_{g(x,y)}$ and outputs Π^*_C, we may assume without loss of generality that (ℓ, r) is always an edge in $M_{g(x,y)}$. Hence, errors occur only if $b \neq z_\ell \oplus z_r$. The error probability of Π^* under the input distribution $\mu(S,T)$ can therefore be written as

$$\mathcal{E}_{\Pi^*}(\boldsymbol{S}, \boldsymbol{T}, \boldsymbol{Z}) = \mathop{\mathbf{Pr}}_{(x,y,z)\sim\mu(S,T)}[\Pi^*(x,y,z) \notin \mathrm{GHM}(x,y,z)] = \mathop{\mathbf{Pr}}_{(x,y,z)\sim\mu(S,T)}[b \neq z_\ell \oplus z_r].$$

By Claim 3.5, we have $\mathcal{E}_{\Pi^*}(\boldsymbol{S}, \boldsymbol{T}, \boldsymbol{Z}) \leq 1/16$. Since the messages from Alice and Bob now depend only on z, their combined message induces a partition of Z. For each message τ, we define

$$Z_\tau = \{z \mid (\Pi^*_A(z), \Pi^*_B(z)) = \tau\}$$

and let Z_τ be uniformly distributed over Z_τ. Define the conditional error as

$$e_\tau := \mathcal{E}_{\Pi^*}(\boldsymbol{S}, \boldsymbol{T}, \boldsymbol{Z}_\tau) = \mathop{\mathbf{Pr}}_{(x,y,z)\sim\mu(S,T)}[\Pi^*(x,y,z) \notin \mathrm{GHM}(x,y,z) \mid z \in Z_\tau].$$

Notice that $\mathbb{E}[e_\tau] = \mathcal{E}_{\Pi^*}(\boldsymbol{S}, \boldsymbol{T}, \boldsymbol{Z}) \le 1/16$, then by Markov's inequality we have

$$\mathbf{Pr}[e_\tau \ge 1/8] \le 1/2.$$

The following lemma shows that any message τ with small error reveals a lot of information.

Lemma 3.8. *For every message τ with $e_\tau < 1/8$, we have:*

$$\mathbf{H}(\boldsymbol{Z}) - \mathbf{H}(\boldsymbol{Z} | (\Pi_A^*(z), \Pi_B^*(z)) = \tau) = \Omega(m^{5/16}).$$

By assuming Lemma 3.8 and using the fact that $\mathbf{Pr}[e_\tau < 1/8] \ge 1/2$, we have

$$\mathrm{I}(\boldsymbol{Z} : \boldsymbol{\Pi^*}) = \Omega(m^{5/16}).$$

□

Now we focus on the proof of Lemma 3.8.

Proof of Lemma 3.8. For a fixed message τ with $e_\tau < 1/8$. Recall by Definition 1.1 that the problem $\mathrm{GHM} \circ g$ is defined on a set of perfect matching $\{M_1, \ldots, M_m\}$ where

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

As S and T are now fixed, we are specifically interested in those matching:

$$\mathcal{M} = \{M_i : \exists x \in S, y \in T, g(x,y) = i\}$$

Furthermore, since g is α-rich, for each $M_i \in \mathcal{M}$, there is a unique pair $x \in S$ and $y \in T$ such that $g(x,y) = i$. We denote it by $(x,y) = g^{-1}(i)$. For each $M_i \in \mathcal{M}$, let

$$e_{\tau,M_i} = \mathcal{E}_{\Pi^*}(Z_\tau, M_i) := \mathop{\mathbf{Pr}}_{(x,y,z)\sim\mu(S,T)}\left[\Pi^*(x,y,z) \notin \mathrm{GHM}(x,y,z) \mid z \in Z_\tau, M_{g(x,y)} = M_i\right]$$

Recall that $\mathbb{E}_{M_i}[e_{\tau,M_i}] = e_\tau < 1/8$. Then by Markov's inequality again, the set

$$\mathcal{M}' := \{M_i \in \mathcal{M} : e_{\tau,M_i} \le 1/4\}$$

has size at least $|\mathcal{M}'| \ge |\mathcal{M}|/2 = \alpha/2$.

For every $M_i \in \mathcal{M}'$, let $(x,y) = g^{-1}(i)$, and let (ℓ_i, r_i, b_i) be the tuple output by $\Pi_C^*(x,y,\tau)$. Recall that Charlie always outputs a pair (ℓ_i, r_i) that belongs to the matching defined by (x,y). Hence, it must have the form

$$r_i = m + ((\ell_i + i) \bmod m).$$

Let $G_\tau = (L, R, E)$ be a bipartite graph with vertices $L = \{0, 1, \ldots, m-1\}$ and $R = \{m, m+1, \ldots, 2m-1\}$. An edge connects $\ell \in L$ and $r \in R$ if and only if there exists (x,y) with $M_{g(x,y)} \in \mathcal{M}'$ such that

$$(\ell, r) = \Pi_C^*(x,y,\tau).$$

By applying Lemma 3.7 with $Q' := \{i : M_i \in \mathcal{M}'\}$, we conclude that either at least $\Omega(m^{5/16})$ vertices on the left side of G_τ are incident to at least one edge, or at least $\Omega(m^{5/16})$ vertices on the right side are incident to at least one edge.

In the first case, let $A \subseteq E$ be a set of edges such that each vertex on the left side is incident to exactly one edge in A. In the second case, choose A such that each vertex on the right side is incident to at most one edge in A. In both cases, we have $|A| = \Omega(m^{5/16})$.

Recall that the set of edges E is identical to $\mathcal{M}'$, so A is indeed a subset of $\mathcal{M}'$. Let $v \in \{0,1\}^A$ be the vector defined by

$$v_i = b_i,$$

where (ℓ_i, r_i, b_i) is the output of $\Pi_C^*(g^{-1}(i), \tau)$ for each $i \in A$.

On the other hand, for each $z \in Z_\tau$, define a vector $u_z \in \{0,1\}^A$ by

$$(u_z)_i = z_{\ell_i} \oplus z_{r_i}.$$

Recall that $(u_z)_i$ corresponds to the correct answer of GHM $\circ\, g$ on input (ℓ_i, r_i, z). Hence,

$$\mathcal{E}_{\Pi^*}(\boldsymbol{Z}_\tau, \mathbf{A}) = \Pr_{(x,y,z)\sim\mu(S,T)}[(u_z)_i \neq v_i \mid M_i \in A, z \in Z_\tau] = \frac{\mathbb{E}[d_H(\boldsymbol{u}_z, v)]}{|A|} \leq 2e_\tau \leq 1/4,$$

where $\boldsymbol{u}_z$ denotes the distribution induced by sampling $z \sim \boldsymbol{Z}_\tau$ and computing u_z.

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 $\boldsymbol{u}_z$.

Lemma 3.9 ([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 $\mathbb{E}[d_H(\boldsymbol{W}, v)] \leq \varepsilon \cdot k$ for some $0 \leq \varepsilon \leq 1/2$. Then the entropy of $\boldsymbol{W}$ is bounded by,*

$$\mathbf{H}(\boldsymbol{W}) \leq k \cdot H_2(\varepsilon),$$

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

Proof. Without loss of generality, we assume that $v = 0^k$. Let $\boldsymbol{W} = (\boldsymbol{W}_1, \ldots, \boldsymbol{W}_k)$, where each $\boldsymbol{W}_i$ is a Bernoulli random variable with $p_i := \mathbf{Pr}[\boldsymbol{W}_i = 1]$. Then

$$\mathbb{E}[d_H(\boldsymbol{W}, 0^k)] = \sum_{i=1}^k p_i \leq \varepsilon \cdot k.$$

By subadditivity of entropy and the concavity of $H_2(\cdot)$, we have

$$\mathbf{H}(\boldsymbol{W}) \leq \sum_{i=1}^k \mathbf{H}(\boldsymbol{W}_i) = \sum_{i=1}^k H_2(p_i) \leq k \cdot H_2\left(\frac{1}{k}\sum_{i=1}^k p_i\right) \leq k \cdot H_2(\varepsilon).$$

□

By applying this lemma to $\boldsymbol{u}_z$ with $\varepsilon = 1/4$ and $k = |A|$, we obtain $\mathbf{H}(\boldsymbol{u}_z) \leq |A| \cdot H_2(1/4)$. Therefore,

$$\begin{aligned}\mathbf{H}(\boldsymbol{Z} \mid (\Pi_A^*(z), \Pi_B^*(z)) = \tau) &= \mathbf{H}(\boldsymbol{u}_z \mid (\Pi_A^*(z), \Pi_B^*(z)) = \tau) + \mathbf{H}(\boldsymbol{Z} \mid \boldsymbol{u}_z, (\Pi_A^*(z), \Pi_B^*(z)) = \tau) \\ &\leq |A| \cdot H_2(1/4) + \mathbf{H}(\boldsymbol{Z} \mid \boldsymbol{u}_z, (\Pi_A^*(z), \Pi_B^*(z)) = \tau).\end{aligned}$$

Finally, since each vertex (on either the left or right side) in the matching is incident to at most one edge in A, we conclude that

$$\mathbf{H}(\boldsymbol{Z} \mid \boldsymbol{u}_z, (\Pi_A^*(z), \Pi_B^*(z)) = \tau) \le \mathbf{H}(\boldsymbol{Z}) - |A|.$$

Putting everything together,

$$\mathbf{H}(\boldsymbol{Z} \mid (\Pi_A^*(z), \Pi_B^*(z)) = \tau) \le \mathbf{H}(\boldsymbol{Z}) - |A|(1 - H_2(1/4)).$$

Since $|A| = \Omega(m^{5/16})$ and $1 - H_2(1/4) > 0$, this yields the desired entropy loss.

□

3.3.1 Proof of Lemma 3.7

We prove Lemma 3.7 in this section. Recall that m is a prime number and $\alpha = \sqrt{m}$. This is a purely combinatorial problem, and we first recall the statement.

Lemma 3.10 (Restate of Lemma 3.7)**.** *There exists a sequence $Q \in [m]^\alpha$ consisting of distinct elements such that for any subsequence $Q' = (q_1, \ldots, q_r) \subseteq Q$ with $r \ge \alpha/2$, the following holds: for any sequence $L = (\ell_1, \ldots, \ell_r)$, either*

- *L contains at least $\Omega(m^{5/16})$ distinct elements, or*
- *the set $R := \{m + ((\ell_i + q_i) \bmod m) \mid 1 \le i \le r\}$ satisfies $|R| \ge \Omega(m^{5/16})$.*

Here, $\alpha = \lfloor \sqrt{m} \rfloor$ is the parameter we chose previously.

The following periodic definition is the core concept in our proof of this lemma.

Definition 3.11. We view the sequence $Q \in [m]^\alpha$ as a set of integers modulo m. A subset $A \subseteq Q$ is called *periodic* if there exists a nonzero $b \in [m] \setminus \{0\}$ such that

$$A + b := \{(a + b) \bmod m \mid a \in A\} \subseteq Q.$$

We say that Q is β-periodic-free if no periodic subset $A \subseteq Q$ with size $|A| \ge \beta$.

In our proof, we specifically choose $\beta = 8 \log m$.

Lemma 3.12. *Let $\beta = 8 \log m$. Then there exists a subset $Q \subseteq [m]$ of size $|Q| = \alpha$ that is β-periodic-free.*

Proof. We use a probabilistic argument to prove that, i.e., we choose Q uniformly at random with $|Q| = \alpha$. Fix $b \in [m] \setminus \{0\}$, define

$$A_b = \left\{ a \in [m] \;\middle|\; a \in Q \text{ and } (a + b) \bmod m \in Q \right\}.$$

and we aim to bound

$$\Pr_Q \left[\exists b \in [m] \setminus \{0\}, |A_b| \ge \beta \right]$$

First, we use the following claim to simplify our proof.

Claim 3.13. *Let m be a prime, for any $b \in [m] \setminus \{0\}$ and $a \in [m]$,*

$$\left\{ a + k\, b \bmod m \;\middle|\; k = 0, 1, \ldots, m - 1 \right\} \;=\; [m].$$

By Claim 3.13, we have that $\mathbf{Pr}_Q[\,|A_b| \geq \beta\,] = \mathbf{Pr}_Q[\,|A_1| \geq \beta\,]$ for any $b \in [m] \setminus \{0\}$. Hence, it suffices to analyze the case $b = 1$. We partition $[m]$ into three residue classes, defining

$$S_\gamma := \{\, x \in [m] \mid x \equiv \gamma \pmod 3 \,\} \quad \text{for } \gamma \in \{0,1,2\}.$$

For each γ and a set $Q \subseteq [m]$, we define:

$$P_\gamma = \{(a, a+1) \mid a \in S_\gamma\}, \qquad X_a(Q) := \mathbf{1}(a \in Q,\ a+1 \in Q), \qquad Y_\gamma(Q) := \sum_{(a,a+1)\in P_\gamma} X_a(Q).$$

Clearly, we have $|A_1| = Y_0(Q) + Y_1(Q) + Y_2(Q)$. Therefore, the desired probability becomes

$$\Pr_Q[\,|A_1| \geq \beta\,] = \Pr_Q[\,Y_0(Q) + Y_1(Q) + Y_2(Q) \geq \beta\,].$$

In what follows, we prove that for every $\gamma \in \{0,1,2\}$.

$$\mathbf{Pr}\left[Y_\gamma(Q) \geq \frac{8}{3} \cdot \log m\right] \leq \exp\left(-2(\log m)^2\right) \tag{$*$}$$

Instead of sampling exactly $|Q| = \alpha$ elements, we alternatively consider the Bernoulli distribution Q^*, where each element $x \in [m]$ is included in Q^* independently with probability α/m. Observe that all pairs in P_γ are pairwise disjoint. By the negative association of random variables [JDP83], we then have that

$$\Pr_Q\big[Y_\gamma(Q) \geq t\big] \leq \Pr_{Q^*}\big[Y_\gamma(Q^*) \geq t\big].$$

Under the Bernoulli distribution, $Y_\gamma(Q^*) = \sum_{(a,a+1)\in P_\gamma} X_a(Q^*)$ is a sum of $|P_\gamma| = \lfloor m/3 \rfloor$ independent indicator variables. For each a, we have

$$\mathbf{Pr}[X_a = 1] = \mathbf{Pr}[a \in Q^*, a+1 \in Q^*] = \left(\frac{\alpha}{m}\right)^2 = \frac{1}{m},$$

and hence the expected value $\mu := \mathbb{E}[Y_\gamma(Q^*)] \leq 1/3$. We apply Chernoff's inequality:

$$\mathbf{Pr}\left[Y_\gamma(Q^*) \geq \frac{8\log m}{3}\right] = \mathbf{Pr}\left[Y_\gamma(Q^*) \geq (1+\delta)\mu\right] \leq \left(\frac{e^\delta}{(1+\delta)^{1+\delta}}\right)^\mu,$$

where

$$\delta := \frac{\frac{8\log m}{3}}{\mu} - 1 \geq 8\log m - 1.$$

Since $\mu \leq 1/3$, it follows that

$$\Pr_Q[Y_\gamma(Q) \geq \tfrac{8}{3}\log m] \leq \mathbf{Pr}[Y_\gamma(Q^*) \geq \tfrac{8}{3}\log m] \leq \exp\left(-2(\log m)^2\right).$$

Thus, by $(*)$:

$$\mathbf{Pr}\left[|A_1| \geq 8\log m\right] = \mathbf{Pr}\left[\sum_{\gamma=0}^{2} Y_\gamma(Q) \geq 8\log m\right] \leq \sum_{\gamma=0}^{2} \mathbf{Pr}\left[Y_\gamma(Q) \geq \tfrac{8}{3}\log m\right] \leq 3\exp\left(-2(\log m)^2\right).$$

Recall that $\beta = 8\log m$, applying a union bound over all $b \in [m] \setminus \{0\}$ gives

$$\Pr_{Q:|Q|=\sqrt{m}}[\exists\, b \in [m] \setminus \{0\} \text{ such that } |A_b| \geq \beta] \leq (m-1) \cdot \frac{1}{2m} < \frac{1}{2}.$$

Hence, there exists a subset $Q \subseteq [m]$ of size $|Q| = \alpha$ that is β-periodic-free.

□

Now we are ready to prove Lemma 3.7.

Proof of Lemma 3.7. Fix any $Q = (q_1, ..., q_\alpha) \subseteq [m]$ with $|Q| = \alpha$ that is *β-periodic-free* by Lemma 3.12. Since any subset of a *β-periodic-free* set is also *β-periodic-free*, any subsequence $Q' \subseteq Q$ of size $|Q'| = \alpha/2$ remains *β-periodic-free*.

Let $L = (\ell_1, \ldots, \ell_r)$ be any sequence. If L contains at least $\Omega(m^{5/16})$ distinct elements, then the lemma follows immediately. Otherwise, let t denote the number of distinct elements in L, and let these be denoted by $c_1, \ldots, c_t$. We partition the set R as follows:

$$R = R_1 \cup \cdots \cup R_t, \quad \text{where } R_j = \left\{ m + ((\ell_i + q_i) \bmod m) \;\middle|\; \ell_i = c_j \right\}.$$

Without loss of generality, we assume that $|R_1| \geq |R_2| \geq \cdots \geq |R_t|$. Since elements of Q' are distinct, we have

$$|R_1| + \cdots + |R_t| = |Q'| \geq \alpha/2.$$

We claim that for any $i, j \in [t]$, it holds that

$$|R_i \cap R_j| \leq \beta.$$

Otherwise, if $|R_i \cap R_j| > \beta$, consider $A = R_i \cap R_j$. Then both $A - c_i - m$ and $A - c_j - m$ are subsets of Q', and since $b = c_i - c_j \neq 0$, the set $A - c_i - m$ would be a periodic subset of size larger than β, contradicting the fact that Q' is *β-periodic-free*. Thus, by inclusion-exclusion,

$$|R_1 \cup \cdots \cup R_j| \geq |R_1| + |R_2| - |R_2 \cap R_1| + \cdots + |R_j| - |R_j \cap R_1| - \cdots - |R_j \cap R_{j-1}| > |R_1| + \cdots + |R_j| - \beta \cdot j^2.$$

Since $|R_1| \geq \cdots \geq |R_t|$, $t \leq m^{5/16}$ and $\alpha = \sqrt{m}$, we have

$$|R_1 \cup \cdots \cup R_j| \geq \frac{j\alpha}{2t} - \beta j^2 \geq j \cdot m^{3/16}/2 - \beta j^2.$$

Choosing $j = m^{2.2/16}$, since $\beta = 8 \cdot \log m$ we obtain

$$|R| \geq m^{5.2/16}/2 - 8 \log m \cdot m^{4.1/16} > m^{5/16}$$

for sufficiently large m. □

4 Open Problems

We have shown an $\Omega(n^{1/16})$ randomized lower bound for the simultaneous NOF communication complexity of GHM ∘ g. On the other hand, the best known upper bound remains $\sqrt{n}$, where Alice simply sends $\sqrt{n}$ random bits of z. By the birthday paradox, with high probability, Charlie can recover the value of at least one matched pair from Alice's message. Bridging this gap remains a compelling open question.

Conjecture 4.1. *There exists a gadget g such that the randomized simultaneous NOF communication complexity of GHM ∘ g is $\Omega(\sqrt{n})$.*

Our techniques are currently tailored to the simultaneous NOF model. It remains open whether similar quantum-classical separations can be established in more general communication models, such as the one-way NOF model.

Conjecture 4.2. *There exists a gadget g such that the randomized one-way NOF communication complexity of GHM ∘ g is $\Omega(n^{\Omega(1)})$.*

References

[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

[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

[BS15] Joshua Brody and Mario Sanchez. Dependent random graphs and multiparty pointer jumping. *arXiv preprint arXiv:1506.01083*, 2015. 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, 8, 14

[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

[CKGS98] Benny Chor, Eyal Kushilevitz, Oded Goldreich, and Madhu Sudan. Private information retrieval. *Journal of the ACM (JACM)*, 45(6):965–981, 1998. 2

[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

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

[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

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

[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

[Gro94] Vince Grolmusz. The bns lower-bound for multiparty protocols is nearly optimal. *Information and computation*, 112(1):51–54, 1994. 2

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

[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

[JDP83] Kumar Joag-Dev and Frank Proschan. Negative association of random variables with applications. *The Annals of Statistics*, pages 286–295, 1983. 10

[LSS09] Troy Lee, Gideon Schechtman, and Adi Shraibman. Lower bounds on quantum multiparty communication complexity. In *2009 24th Annual IEEE Conference on Computational Complexity*, pages 254–262. IEEE, 2009. 2

[PRS97] Pavel Pudlák, Vojtech Rödl, and Jirí Sgall. Boolean circuits, tensor ranks, and communication complexity. *SIAM Journal on Computing*, 26(3):605–633, 1997. 2

[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

[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

[RY20] Anup Rao and Amir Yehudayoff. *Communication complexity: and applications*. Cambridge University Press, 2020. 2

Appendix

Quantum protocols for GHM_n [BYJK04]: We present a quantum protocol for the gadgeted hidden matching problem with communication complexity of $O(\log n)$ qubits. Let $z = (z_1, \cdots, z_n) \in \{0,1\}^n$ and $y \in [n]$ be Alice's input and $x, y \in [n]$ be Charlie's input.

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

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

$$B = \left\{ \frac{1}{\sqrt{2}} (|k\rangle \pm |\ell\rangle) \;\middle|\; (k,\ell) \in M_{g(x,y)} \right\}.$$

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 Charlie 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 Charlie 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 Charlie's input and that the algorithm is 0-error.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il