Electronic Colloquium on Computational Complexity, Report No. 4 (2012)

# TENSOR RANK AND STRONG QUANTUM NONDETERMINISM IN MULTIPARTY COMMUNICATION

MARCOS VILLAGRA*, MASAKI NAKANISHI†, SHIGERU YAMASHITA‡, AND YASUHIKO NAKASHIMA§

Abstract. In this paper we study quantum nondeterminism in multiparty communication. There are three (possibly) different types of nondeterminism in quantum computation: i) strong, ii) weak with classical proofs, and iii) weak with quantum proofs. Here we focus on the first one. A strong quantum nondeterministic protocol accepts a correct input with positive probability, and rejects an incorrect input with probability 1. In this work we relate strong quantum nondeterministic multiparty communication complexity to the rank of the communication tensor in the Number-On-Forehead and Number-In-Hand models. In particular, by extending the definition proposed by de Wolf to *nondeterministic tensor-rank* (*nrank*), we show that for any boolean function $f$ with communication tensor $T_f$,

(1) in the Number-On-Forehead model, the cost is upper-bounded by the logarithm of $nrank(T_f)$;
(2) in the Number-In-Hand model, the cost is lower-bounded by the logarithm of $nrank(T_f)$.

This naturally generalizes previous results in the field and relates for the first time the concept of (high-order) tensor rank to quantum communication. Furthermore, we show that strong quantum nondeterminism can be exponentially stronger than classical multiparty nondeterministic communication. We do so by applying our results to the matrix multiplication problem.

## 1. Introduction

1.1. **Background.** Nondeterminism plays a fundamental role in complexity theory. For instance, the **P** vs **NP** problem asks if nondeterministic time is strictly more powerful than deterministic time. Even though nondeterministic models are unrealistic, they can give insights into the power and limitations of realistic models (i.e., deterministic, random, etc.).

There are two ways of defining a nondeterministic machine, using randomness or as a proof system: a nondeterministic machine *i*) accepts a correct input with positive probability, and rejects an incorrect input with probability one; or *ii*) is a deterministic machine that receives besides the input, a proof or certificate which exists if and only if the input is correct. For classical machines (i.e., machines based on classical mechanics), these two notions of nondeterminism are equivalent. However, in the quantum setting they can be different. In fact, these two notions give rise to (possibly) three different kinds of quantum nondeterminism. In *strong quantum nondeterminism*, the quantum machine accepts a correct input with positive

*Email: `villagra-m@is.naist.jp`, NAIST, Nara 630-0192, Japan.
†Email: `m-naka@e.yamagata-u.ac.jp`, Yamagata University, Yamagata 990-8560, Japan.
‡Email: `ger@cs.ritsumei.ac.jp`, Ritsumeikan University, Shiga 525-8577, Japan.
§Email: `nakashim@is.naist.jp`, NAIST, Nara 630-0192, Japan.



ISSN 1433-8092

probability. In *weak quantum nondeterminism*, the quantum machine outputs the correct answer when supplied with a correct proof, which could be either classical or quantum.

The study of quantum nondeterminism started with de Wolf [4], in the context of query and communication complexities. In particular, de Wolf [4] introduced the notion of *nondeterministic rank* of a matrix, which was later proved to completely characterize strong quantum nondeterministic communication [5]. In the same piece of work, it was proved that strong quantum nondeterministic protocols are exponentially stronger than classical nondeterministic protocols. In the same spirit, Le Gall [9] studied weak quantum nondeterministic communication with classical proofs and showed a quadratic separation for a total function.

Weak nondeterminism seems a more suitable definition, mainly due to the requirement of the existence of a proof, a concept that plays fundamental roles in complexity theory. In contrast, strong nondeterminism lends itself to a natural mathematical description in terms of matrix rank. Moreover, strong nondeterminism is a more powerful model capable of simulating weak nondeterminism with classical and quantum proofs. The reverse, if weak nondeterminism is strictly a less powerful model or not is still an open problem.

The previous results by de Wolf [5] and Le Gall [9] were on the context of 2-party communication complexity, i.e., there are two players with two inputs $x$ and $y$ each, and they want to compute a function $f(x, y)$. Let $rank(f)$ be the rank of the communication matrix $M_f$, where $M_f[x, y] = f(x, y)$. A known result is $\frac{1}{2} \log rank(f) \leq Q(f) \leq D(f)$ [2], where $D(f)$ is the deterministic communication complexity of $f$ and $Q(f)$ the quantum exact communication complexity[1]. It is conjectured that $D(f) = O(\log^c rank)$ for some arbitrary constant $c$. This is the *log-rank conjecture* in communication complexity, one the biggest open problems in the field. If it holds, implies that $Q(f)$ and $D(f)$ are polynomially related. This is in contrast to the characterization given by de Wolf [5] in terms of the nondeterministic matrix-rank, which is defined as the minimal rank of a matrix (over the complex field) whose $(x, y)$-entry is non-zero if and only if $f(x, y) = 1$.

1.2. **Contributions.** In this paper, we continue with the study of strong quantum nondeterminism in the context of multiparty protocols. Let $k \geq 3$ be the number of players evaluating a function $f(x_1, \ldots, x_k)$. The players take turns predefined at the beginning of the protocol. Each time a player sends a bit (or qubit if it is a quantum protocol), he sends it to the player who follows next. The communication complexity of the protocol is defined as the minimum number of bits that need to be transmitted by the players in order to compute $f(x_1, \ldots, x_k)$. There are two common ways of communication: The Number-On-Forehead model (NOF), where player $i$ knows all inputs except $x_i$; and, Number-In-Hand model (NIH), where player $i$ only knows $x_i$. Also, any protocol naturally defines a *communication tensor* $T_f$, where $T_f[x_1, \ldots, x_k] = f(x_1, \ldots, x_k)$.

Tensors are natural generalizations of matrices. They are defined as multi-dimensional arrays while matrices are 2-dimensional arrays. In the same way, the concept of matrix rank extends to *tensor rank*. However, the nice properties of matrix rank do not hold anymore for tensors; for instance, the rank could be different if the same tensor is defined over different fields [7].

[1] All logarithms in this paper are base 2.

We extend the concept of nondeterministic matrices to *nondeterministic tensors*. The *nondeterministic tensor rank*, denoted $nrank(f)$, is the minimal rank of a tensor (over the complex field) whose $(x_1, \ldots, x_k)$-entry is non-zero if and only if $f(x_1, \ldots, x_k) = 1$.

Let $NQ_k^{NOF}$ and $NQ_k^{NIH}$ denote the $k$-party strong quantum nondeterministic communication complexity for the NOF and NIH models respectively.

**Theorem 1.1.** *Let* $f : (\{0,1\}^n)^k \to \{0,1\}$, *then* $NQ_k^{NOF}(f) \leq \lceil \log nrank(f) \rceil + 1$, *and* $NQ_k^{NIH}(f) \geq \lceil \log nrank(f) \rceil + 1$.

This theorem generalizes the previous result by de Wolf, as it can be seen that by letting $k = 2$ we obtain exactly [5, Lemma 3.2]. Also, since $NQ_k^{NIH}$ is a lower bound for exact NIH quantum communication[2], denoted $Q_k^{NIH}$, we obtain the following corollary:

**Corollary 1.2.** $\lceil \log nrank(f) \rceil + 1 \leq Q_k^{NIH}(f)$.

One of the first direct consequences of Theorem 1.1 is on the equality function. The $k$-party equality function $EQ_k(x_1, \ldots, x_k) = 1$ if and only if $x_1 = \cdots = x_k$. A nondeterministic tensor for $EQ_k$ is superdiagonal with non-zero entries in the main diagonal, and 0 anywhere else. Thus, it has $2^n$ rank, and implies $NQ_k^{NOF}(EQ_k) \leq n + 1$ and $NQ_k^{NIH}(EQ_k) \geq n + 1$. However, note that $EQ_k$ is upper-bounded by $\mathcal{O}(n)$ in the NOF model, however this could be a very loose bound. In general, $NQ_k^{NOF}$ cannot be lower-bounded by $\log nrank$. To see this, it is easy to show that in the NOF model there exists a classical protocol for $EQ_k$ with a cost of 2 bits[3]. In contrast, the lower bound on $NQ_k^{NIH}(EQ_k)$ is not that loose; using the trivial protocol, where all players send their inputs, we have that $NQ_k^{NIH}(EQ_k) = \mathcal{O}(kn)$.

A more interesting function is the generalized inner product defined formally as $GIP_k(x_1, \ldots, x_k) = (\sum_{i=1}^{k} \bigwedge_{j=1}^{n} x_{ij}) \mod 2$. We know that $(2^n - 1)k/2 \leq nrank(GIP_k)$ (see Appendix A for a proof), and thus, $NQ_k^{NIH}(GIP_k) \geq n + \lceil \log(k/2) \rceil + 1$. In NIH, using the trivial protocol where each player send their inputs, we obtain (with Corollary 1.2) a bound in quantum exact communication of $\lceil \log(k/2) \rceil + n + 1 \leq Q_k^{NIH}(GIP_k) \leq (k-1)n + 1$. Improving the lower bound will require new techniques for explicit construction of linear-rank tensors, with important consequences to circuit lower bounds [15] (see for example the paper by Alexeev, Forbes, and Tsimerman [1] for state-of-the-art tensor constructions). In general, we are still unable to upper-bound $NQ_k^{NIH}(f)$ in terms of $\log nrank$.

Although the bounds given by Theorem 1.1 could be loose for some functions, they are good enough for other applications. For instance, we show in Section 4 a super-polynomial separation between the NOF models of strong quantum nondeterminism and classical nondeterminism. We do so by applying Theorem 1.1 to the matrix multiplication problem. To our knowledge, this is the first super-polynomial quantum-classical separation in any multiparty communication model.

[2]An exact quantum protocol accepts a correct input and rejects an incorrect input with probability 1.

[3]Let the first player check if $x_2, \ldots, x_k$ are equal. If they are, he sends a 1 bit to the second player, who will check if $x_1, x_3, \ldots, x_k$ are equal. If his strings are equal and he received a 1 bit from the first player, he sends a 1 bit to all players indicating that all strings are equal [8, Example 6.3].

## 2. Mathematical Preliminaries

In this paper we assume basic knowledge of communication complexity and quantum computing. We refer the interested reader to the books by Kushilevitz and Nisan [8] and Nielsen and Chuang [12]. Nevertheless, in this section we give a small review of tensors and quantum communication.

### 2.1. Tensors.

A *tensor* is a multi-dimensional array defined over some field. An order-$d$ tensor is an element of the tensor product of $d$ vector spaces.

**Definition 2.1.** Let $|v_i\rangle \in V^{n_i}$ be an $n_i$-dimensional vector for $1 \leq i \leq d$ on some vector space $V^{n_i}$. The $j_i^{th}$ component of $|v_i\rangle$ is denoted by $v_i(j_i)$ for $1 \leq j_i \leq n_i$. The tensor product of $\{|v_i\rangle\}$ is the tensor $T \in V^{n_1} \otimes \cdots \otimes V^{n_d}$ whose $(j_1, \ldots, j_d)$-entry is $v_1(j_1) \cdots v_d(j_d)$, i.e., $T[j_1, \ldots, j_d] = v_1(j_1) \cdots v_d(j_d)$. Then $T = |v_1\rangle \otimes \cdots \otimes |v_d\rangle$ and we say $T$ is a rank-1 or simple order-$d$ tensor. We also say that a tensor is of high order if its order is three or higher.

From now on, we will refer to high-order tensors simply as tensors, and low-order tensor will be matrices, vectors, and scalars as usual.

It is important to note that the set of simple tensors span the space $V^{n_1} \otimes \cdots \otimes V^{n_d}$, and hence, there exists tensors that are not simple. This leads to the definition of rank.

**Definition 2.2.** The rank of a tensor is the minimum $r$ such that $T = \sum_{i=1}^{r} A_i$ for simple tensors $A_i$.

This agrees with the definition of matrix rank. The complexity of computing tensor rank was studied by Håstad [6] who showed that it is **NP**-complete for any finite field, and **NP**-hard for the rational numbers.

The process of arranging the elements of an order-$k$ tensor into a matrix is known as *matrization*. Since there are many ways of embedding a tensor into a matrix, in general the permutation of columns is not important, as long as the corresponding operations remain consistent [7].

### 2.2. Strong Quantum Nondeterministic Multiparty Communication.

In a multiparty communication protocol there are $k \geq 3$ players trying to compute a function $f$. Let $f : X^k \to \{0,1\}$ be a function on $k$ strings $x = (x_1, \ldots, x_k)$, where each $x_i \in X$ and $X = \{0,1\}^n$. There are two common ways of communication between the players: The Number-In-Hand (NIH) and the Number-On-Forehead (NOF) models. In NIH, player $i$ only knows $x_i$, and in NOF, player $i$ knows all inputs except $x_i$. First we review the classical defintion.

**Definition 2.3** (Classical nondeterministic multiparty protocol)**.** Let $k$ be the number of players. Besides the input $x$, the protocol receives a proof or certificate $c \in \{0,1\}^+$. The players take turns in an order predefined at the beginning of the protocol. To communicate, a player sends exactly one bit to the player that follows next. The computation of the protocol ends when the last player computes $f$. If $f(x) = 1$ then, there exists a $c$ that makes the protocol accept the input, i.e., the last player outputs 1. If $f(x) = 0$ then, the protocol rejects the input for all $c$, i.e., the last player outputs 0. The cost of the protocol is the length of $c$ plus the total number of bits communicated.

Hence, the *classical nondeterministic multiparty communication complexity*, denoted $N_k(f)$, is defined as the minimum number of bits required to compute $f(x)$. If the model is NIH or NOF, we add a superscript $N_k^{NIH}(f)$ or $N_k^{NOF}(f)$ respectively. Note that, the definition of the multiparty protocols in this paper (classical and quantum) are all unicast, i.e., a player sends a bit only to the player that follows next. This is in contrast to the more common *blackboard model.* In this latter model, when a player sends a bit, he does so by broadcasting it and reaching all players inmediately. Clearly, any lower bound on the blackboard model is a lower bound for the unicast model.

To model NOF and NIH in the quantum setting, we follow the work of Lee, Schechtman, and Shraibman [10].

**Definition 2.4** (Quantum multiparty protocol)**.** Let $k$ be the number of players in the protocol. Define the Hilbert space by $\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_k \otimes \mathcal{C}$, where each $\mathcal{H}_i$ is the Hilbert space of player $i$, and $\mathcal{C}$ is the one qubit channel. To communicate the players take turns predefined at the beginning of the protocol. On the turn of player $i$:

(1) in NIH, an arbitrary unitary that only depends on $x_i$ is applied on $\mathcal{H}_i \otimes \mathcal{C}$, and acts as the identity anywhere else;
(2) in NOH, an arbitrary unitary independent of $x_i$ is applied on $\mathcal{H}_i \otimes \mathcal{C}$, and acts as the identity anywhere else.

The cost of the protocol is the number of rounds.

If there is no entanglement, the initial state is a pure state $|0\rangle \otimes \cdots \otimes |0\rangle|0\rangle$. In general, the initial state could be anything that is independent of the input with no prior entanglement. If the final state of the protocol on input $x_1, \ldots, x_k$ is $|\psi\rangle$, it outputs 1 with probability $p(x_1, \ldots, x_k) = \langle\psi|\Pi_1|\psi\rangle$, where $\Pi_1$ is a projection onto the $|1\rangle$ state of the channel.

We say that $T$ is a *nondeterministic communication tensor* if $T[x_1, \ldots, x_k] \neq 0$ if and only if $f(x_1, \ldots, x_k) = 1$. Thus, $T$ can be obtained by replacing each 1-entry in the original communication tensor by a non-zero complex number. We also define the *nondeterministic rank* of $f$, denoted $nrank(f)$, to be the minimum rank over the complex field among all nondeterministic tensors for $f$.

**Definition 2.5.** A *$k$-party strong quantum nondeterministic communication protocol* outputs 1 with positive probability if and only if $f(x) = 1$.

The $k$-party quantum nondeterministic communication complexity is the cost of an optimum (i.e., minimal cost) $k$-party quantum nondeterministic communication protocol, and is denoted $NQ_k(f)$. If the model is NIH or NOF, we add a superscript $NQ_k^{NIH}(f)$ or $NQ_k^{NOF}(f)$ respectively. From the definition it follows that $NQ_k$ is a lower bound for the exact quantum communication complexity $Q_k$ for both NOF and NIH.

**Lemma 2.6** (Lee, Schechtman, and Shraibman [10])**.** *After $\ell$ qubits of communication on input $(x_1, \ldots, x_k)$, the state of a quantum protocol without shared entanglement can be written as*

$$\sum_{m \in \{0,1\}^\ell} |A_m^1(x^1)\rangle|A_m^2(x^2)\rangle \cdots |A_m^k(x^k)\rangle|m_\ell\rangle,$$

*where $m$ is the message sent so far, $m_\ell$ is the $\ell$-th bit in the message, and each vector $|A_m^t(x^t)\rangle$ corresponds to the $t$-th player which depends on $m$ and the input*

$x^t$. *If the protocol is NOF then* $x^t = (x_1, \ldots, x_{t-1}, x_{t+1}, \ldots, x_k)$*; if it is NIH then* $x^t = (x_t)$.

## 3. Proof of Theorem 1.1

The arguments in this section are generalizations of a previous result by de Wolf [5] from 2-party to $k$-party communication.

We start by proving the lower bound. First we need the following technical lemma. It is a generalization of [5, Lemma 3.2] from $k = 2$ to any $k \geq 3$. See below for a proof.

**Lemma 3.1.** *If there exists $k$ families of vectors $\{|A_1^i(x_i)\rangle, \ldots, |A_r^i(x_i)\rangle\} \subseteq \mathbb{C}^d$ for all $i$ with $2 \leq i \leq k$ and $x_i \in \{0,1\}^n$ such that*

$$\sum_{i=1}^{r} |A_i^1(x_1)\rangle \otimes \cdots \otimes |A_i^k(x_k)\rangle = 0 \text{ if and only if } f(x_1, \ldots, x_k) = 0,$$

*then $nrank(f) \leq r$.*

Now we proceed to prove the lower bound in Theorem 1.1.

**Lemma 3.2.** $NQ_k^{NIH}(f) \geq \lceil \log nrank(f) \rceil + 1$

*Proof.* Consider a NIH $\ell$-qubit protocol for $f$. By Lemma 2.6 its final state is

$$|\psi\rangle = \sum_{m \in \{0,1\}^\ell} |A_m^1(x_1)\rangle \cdots |A_m^k(x_k)\rangle |m_\ell\rangle. \tag{3.1}$$

Assume all vectors have the same dimension $d$. Let $S = \{m \in \{0,1\}^\ell : m_\ell = 1\}$, and consider only the part of the state that is projected onto the 1 state of the channel,

$$|\phi(x_1, \ldots, x_k)\rangle = \sum_{m \in S} |A_m^1(x_1)\rangle \cdots |A_m^k(x_k)\rangle |1\rangle. \tag{3.2}$$

The vector $|\phi(x_1, \ldots, x_k)\rangle$ is 0 if and only if $f(x_1, \ldots, x_k) = 0$. Thus, by Lemma 3.1, we have that $nrank(f) \leq |S| = 2^{\ell-1}$, which implies the lower bound. □

*Proof of Lemma 3.1.* First note that the case k=2 was proven by de Wolf [5, Lemma 3.2]. Here we give a proof for $k \geq 3$. We divide it in two cases: when $k$ is odd and even.

*Even $k$:* There are $k$ size-$r$ families of $d$-dimensional vectors. We will construct two new families of vectors denoted $\mathscr{D}$ and $\mathscr{F}$. First, divide the $k$ families in two groups of size $k/2$. Then, tensor each family in one group together in the following way: for each family $\{|A_1^i(x_i)\rangle, \ldots, |A_r^i(x_i)\rangle\}$ for $1 \leq i \leq k/2$ construct a new family

$$\mathscr{D} = \left\{ \bigotimes_{i=1}^{k/2} |A_1^i(x_i)\rangle, \ldots, \bigotimes_{i=1}^{k/2} |A_r^i(x_i)\rangle \right\} = \{|A_1(y)\rangle, \ldots, |A_r(y)\rangle\},$$

where $y = (x_1, \ldots, x_{k/2})$. Do the same to construct $\mathscr{F}$ for $k/2+1 \leq i \leq k$ obtaining

$$\mathscr{F} = \left\{ \bigotimes_{i=k/2+1}^{k} |A_1^i(x_i)\rangle, \ldots, \bigotimes_{i=k/2+1}^{k} |A_r^i(x_i)\rangle \right\} = \{|B_1(z)\rangle, \ldots, |B_r(z)\rangle\},$$

where $z = (x_{k/2+1}, \dots, x_k)$. Thus, $\mathscr{D}$ and $\mathscr{F}$ will become two size-$r$ family of vectors, each vector with dimension $dk/2$. Then apply the theorem for $k = 2$ on these two families and the lemma follows.

*Odd k:* Here we can use the same approach by constructing again two new families $\mathscr{D}$ and $\mathscr{F}$ by dividing the families in two groups of size $\lfloor k/2 \rfloor$ and $\lceil k/2 \rceil$. However, although both families will have the same size $r$, the dimension of the vectors will be different. In fact, the dimension of the vectors in one family will be $d' = d\lfloor k/2 \rfloor$ and in the other $d' + 1$. So, in order to prove the theorem we will consider having two size-$r$ families $\{|A_1(y)\rangle, \dots, |A_r(y)\rangle\} \subseteq \mathbb{C}^{d'}$ and $\{|B_1(z)\rangle, \dots, |B_r(z)\rangle\} \subseteq \mathbb{C}^{d'+1}$.

Denote the entry of each vector $|A_i(y)\rangle, |B_i(z)\rangle$ by $A_i(y)_u$ and $B_i(z)_v$ respectively for all $(u, v) \in [d'] \times [d' + 1]$. Note that

$$\begin{array}{l} \text{if } f(y,z) = 0 \text{ then } \sum_{i=1}^r A_i(y)_u B_i(z)_v = 0 \text{ for all } (u,v); \\ \text{if } f(y,z) = 1 \text{ then } \sum_{i=1}^r A_i(y)_u B_i(z)_v \neq 0 \text{ for some } (u,v). \end{array}$$

This holds because each vector $|A_i(y)\rangle$ and $|B_i(z)\rangle$ are the set of vectors $|A_i^t(x^t)\rangle$ tensored together and separated in two families of size $\lfloor k/2 \rfloor$ and $\lceil k/2 \rceil$ respectively.

The following lemma was implicitly proved by de Wolf [5] for families of vectors with the same dimension. However, we show that the same arguments hold even if the families have different dimensionality (see Appendix B).

**Lemma 3.3.** *Let $I$ be an arbitrary set of numbers of size $2^{2n+1}$. Let $\alpha_1, \dots, \alpha_{d'}$ and $\beta_1, \dots, \beta_{d'+1}$ be numbers from $I$, and define the quantities*

$$a_i(y) = \sum_{u=1}^{d'} \alpha_u A_i(y)_u \quad \text{and} \quad b_i(z) = \sum_{v=1}^{d'+1} \beta_v B_i(z)_v.$$

*Also let*

$$v(y,z) = \sum_{i=1}^{r} a_i(y) b_i(z) = \sum_{u=1}^{d'} \sum_{v=1}^{d'+1} \alpha_u \beta_v \left( \sum_{i=1}^{r} A_i(y)_j B_i(z)_k \right).$$

*There exists with positive probability $\alpha_1, \dots, \alpha_{d'}, \beta_1, \dots, \beta_{d'+1} \in I$ such that for every $(y, z) \in f^{-1}(1)$ we have $v(y, z) \neq 0$.*

Therefore, by the lemma above we have that $v(y, z) = 0$ if and only if $f(y, z) = 0$. Now let $|a_i\rangle$ and $|b_i\rangle$ be $2^n$-dimensional vectors indexed by elements from $\{0, 1\}^n$, and let $M = \sum_{i=1}^r |a_i\rangle\langle b_i|$. Thus $M$ is an order-$k$ tensor with rank $r$. ☐

Now we continue the proof with the upper bound.

**Lemma 3.4.** $NQ_k^{NOF}(f) \leq \lceil \log nrank(f) \rceil + 1$.

The proof of Lemma 3.4 follows by fixing a proper matrization (separating the cases of odd and even $k$) of the communication tensor, and then applying the 2-party protocol by de Wolf [5] (see Appendix B).

## 4. A Quantum-Classical Super-polynomial Separation

In this section, we show that there exists a function with a super-polynomial gap between classical and quantum NOF models of quantum strong nondeterminism.

**Theorem 4.1.** *There is a super-polynomial gap between $N_k^{NOF}$ and $NQ_k^{NOF}$ when $k = o(\log n)$.*

In particular, we analyze the following total function: Let $X_1 = \cdots = X_k = \{0,1\}^{n\times n}$ be the set of all $n \times n$ boolean matrices. Also let $x_i \in X_i$ be a $n \times n$ boolean matrix, and denote by $x_i x_j$ the multiplication of matrices $x_i$ and $x_j$. Define

$$F(x_1, \dots, x_k) = (x_1 x_2 \cdots x_k)_{11},$$

i.e., $F(x_1, \dots, x_k)$ is the entry in the first row and first column in $x_1 \cdots x_k$.

This matrix multiplication function was studied by Raz [14], who showed a $\Omega(n/2^k)$ lower bound in the blackboard model of NOF bounded-error communication. However, this lower bound also holds for the classical blackboard nondeterministic NOF communication denoted $N_k^{NOF}(F)$. The reason is that the proof by Raz is based on an upper bound for discrepancy. Since $N_k^{NOF}(f) = \Omega(1/Disc(f))$ for any $f$ where $Disc(f)$ is the discrepancy [11], we inmediately obtain the following corollary:

**Corollary 4.2.** $N_k^{NOF}(F) = \Omega(n/2^k)$.

The condition on the number of players $k = o(\log n)$ in Theorem 4.1 comes from this lower bound. Improving it will require new techniques for classical multiparty communication.

Since any lower bound in the blackboard model also holds in the unicast model, we can use Corollary 4.2 to prove a separation for the unicast models in this paper. The following lemma implies the theorem.

**Lemma 4.3.** $NQ_k^{NOF}(F) = \mathcal{O}(k \log n)$.

*Proof.* By Theorem 1.1 we just need to give a tensor with rank at most $\mathcal{O}(n^k)$. Denote each entry of the matrix $x_i$ by $x_i[p,q]$, i.e., the $(p,q)$-entry of $x_i$. Also, all the operations in this proof are assumed to be over the binary field.

Let

$$T[x_1, \dots, x_k] = (x_1 \cdots x_k)_{11},$$

which is just the function $F$ plugged into $T$.

First, note that the multiplication is between $n \times n$ matrices. Hence, the maximum rank of the product is at most $n$. Therefore, we can write each entry of $T$ as

$$T[x_1, \dots, x_k] = \left( \left( \sum_{j_1=1}^{n} x_1^{j_1} \right) \cdots \left( \sum_{j_k=1}^{n} x_k^{j_k} \right) \right)_{11} = \sum_{j_1,\dots,j_k=1}^{n} (x_1^{j_1} \cdots x_k^{j_k})_{11}. \tag{4.1}$$

The notation $x_i^j$ can be interpreted as the $j^{th}$ term in the rank decomposition of matrix $x_i$. Now fix $j_1, \dots, j_k$, and by the definition of matrix multiplication we get that

$$(x_1^{j_1} \cdots x_k^{j_k})_{11} = \sum_{i_1,\dots,i_{k-1}=1}^{n} x_1^{j_1}[1, i_1] x_2^{j_2}[i_1, i_2] \cdots x_k^{j_k}[i_{k-1}, 1]. \tag{4.2}$$

Equations (4.1) and (4.2) have $n^k$ and $n^{k-1}$ terms. Putting them both together, we have that $T[x_1, \dots, x_k]$ have $n^{2k-1}$ summands. This already have $\mathcal{O}(n^k)$ terms; however, we need to make sure that each term in the summation defines a rank-1 tensor.

For each $m \in \{1, \dots, n^k\}$ define

$$T_m[x_1, \dots, x_k] = x_1^{j_1}[1, i_1] x_2^{j_2}[i_1, i_2] \cdots x_k^{j_k}[i_{k-1}, 1], \tag{4.3}$$

for some $j_1, \ldots, j_k, i_1, \ldots, x_{k-1}$ that directly corresponds to $m$ (fix some bijection between $m$ and $j_1, \ldots, j_k, i_1, \ldots, x_{k-1}$). Then, let $y_1, \ldots, y_{n\times n} \in \{0,1\}^{n\times n}$ be a enumeration of all $n \times n$ boolean matrices. For instance, $y_1$ is the all-0 matrix, and $y_{n\times n}$ is the all-1 matrix. Define vectors

$$|v_1\rangle = \left(y_1^{j_1}[1, i_1], \ldots, y_{2^{n\times n}}^{j_1}[1, i_1]\right) \text{ and } |v_k\rangle = \left(y_1^{j_k}[i_{k-1}, 1], \ldots, y_{2^{n\times n}}^{j_k}[i_{k-1}, 1]\right);$$

and for $r = 2, \ldots, k-1$ define

$$|v_r\rangle = \left(y_1^{j_1}[i_{r-1}, r], \ldots, y_{2^{n\times n}}^{j_k}[i_{r-1}, r]\right).$$

Note that each vector has $2^{n\times n}$ components, and are indexed by the set of $n \times n$ boolean matrices. If we pick $k$ matrices $y_{i_1}, \ldots, y_{i_k}$, we get that

$$T_m[y_{i_1}, \ldots, y_{i_k}] = y_{i_1}^{j_1}[1, i_1] \ldots, y_{i_1}^{j_k}[i_{k-1}, 1]. \tag{4.4}$$

This way, $T_m = |v_1\rangle \otimes |v_2\rangle \otimes \cdots \otimes |v_k\rangle$ for all $m$. Thus, $T_m$ has rank 1, and $T = \sum_{m=1}^{n^{2k-1}} T_m$. □

## 5. Concluding Remarks

In this paper we studied strong quantum nondeterministic communication complexity in multiparty protocols. In particular, we showed that i) strong quantum nondeterministic NOF communication complexity is upper-bounded by the tensor-rank of the nondeterministic communication tensor; ii) strong quantum nondeterministic NIH communication complexity is lower-bounded by the tensor-rank of the nondeterministic communication tensor. These results naturally generalizes previous work by de Wolf [5]. Moreover, the lower bound on NIH is also a lower bound for quantum exact NIH communication. This fact was used to show a $\Omega(n + \log k)$ lower bound for the generalized inner product function.

We also showed an exponential separation between quantum strong nondeterministic communication and classical nondeterministic communication in the NOF model. To our knowledge, this is the first separation in any multiparty model. However, it remains an open problem a separation (of any kind) between more common multiparty models, e.g., bounded-error communication.

In order to prove strong lower bounds using tensor-rank in NIH, we need stronger construction techniques for tensors. The fact that computing tensor-rank is **NP**-complete suggests that this could be a very difficult task. Alternatives for finding lower bounds on tensor-rank include computing the norm of the communication tensor, or a hardness result for approximating tensor-rank.

## References

1. Boris Alexeev, Michael Forbes, and Jacob Tsimerman, *Tensor rank: Some lower and upper bounds*, Proceedings of the 26th Annual IEEE Conference on Computational Complexity, 2011.
2. Harry Buhrman and Ronald de Wolf, *Communication complexity lower bounds by polynomials*, Proceedings of the 16th Annual IEEE Conference on Computational Complexity, 2001, pp. 120–130.
3. Lieven de Latahauwer, Bart de Moore, and Joos Vandewalle, *A multilinear singular value decomposition*, SIAM Journal on Matrix Analysis and Applications **21** (2000), no. 4, 1253–1278.
4. Ronald de Wolf, *Characterization of non-deterministic quantum query and quantum communication complexity*, Proceedings of the 15th Annual IEEE Conference on Computational Complexity, 2000, pp. 271–278.

5. ______, *Nondeterministic quantum query and quantum communication complexities*, SIAM Journal on Computing **32** (2003), no. 3, 681–699.
6. Johan Håstad, *Tensor rank is np-complete*, Journal of Algorithms **11** (1990), no. 4, 644–654.
7. Tamara Kolda and Brett Bader, *Tensor decompositions and applications*, SIAM Review **51** (2009), no. 3, 455–500.
8. Eyal Kushilevitz and Noam Nisan, *Communication Complexity*, Cambridge University Press, 1997.
9. François Le Gall, *Quantum weakly nondeterministic communication complexity*, Proceedings of the 31st International Symposium on Mathematical Foundations of Computer Science 2006, Lecture Notes in Computer Science, vol. 4162, 2006, pp. 658–669.
10. Troy Lee, Gideon Schechtman, and Adi Shraibman, *Lower bounds on quantum multiparty communication complexity*, Proceedings of the 24th IEEE Conference on Computational Complexity, July 2009.
11. Troy Lee and Adi Shraibman, *Disjointness Is Hard in the Multi-party Number-on-the-Forehead Model*, Proceedings of the 23rd IEEE Annual Conference on Computational Complexity, 2008.
12. Michael Nielsen and Isaac Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.
13. Ran Raz, *Exponential separation of quantum and classical communication complexity*, Proceedings of the 31st Annual ACM Symposium on the Theory of Computing, ACM, 1999, pp. 358–367.
14. ______, *The bns-chung criterion for multi-party communication complexity*, Computational Complexity **9** (2000), 113–122.
15. ______, *Tensor-rank and lower bounds for arithmetical formulas*, Proceedings of the 42nd ACM Symposium on Theory of Computing, 2010, pp. 659–666.

## Appendix A. Rank Lower Bound on $GIP_k$

**Lemma A.1.** *$nrank(GIP_k) \geq (2^n - 1)k/2$.*

*Proof.* First, we start by generalizing the concept of rows and columns for tensors. Define a *fiber* to be a vector obtained by fixing every index except by one. Thus, a matrix column is a mode-1 fiber, and a row is a mode-2 fiber. For order-3 tensors, we have columns, rows and tubes, and so on for higher order tensors. In general, a mode-$i$ fiber is a vector obtained by fixing every but except the $i^{th}$ index. In the same way we define a *slice* to be a two-dimensional section of $T$ obtained by fixing all but two indices.

Here we will consider a particular form of matrization. Let $T \in \mathbb{C}^{n_1 \times \cdots \times n_k}$ be an order-$k$ tensor, with $n_i = 2^n$ for every $i$. The *$i$-mode unfolding* of $T$, denoted $T_{(i)}$, is the matrix obtained by arranging the $i$-mode fibers as columns. The permutations of the columns of $T_{(i)}$ is not important, as long as the corresponding operations remain consistent [7]. Define the *$i$-rank* of $T$ as $rank_i(T) = rank(T_{(i)})$. It is trivial that $rank_i(T) \leq rank(T)$ for every $i$ [3].

Now we proceed with the proof. Let $T$ be the order-$k$ communication tensor for $GIP_k$. Let $M_{IP_n}$ be the communication matrix for $GIP_2$, i.e., the 2-party inner product function on $n$ bits. It is well known that $rank(M_{IP_n}) = 2^n - 1$ (cf. [8, Example 1.29]).

Fix the $x'_3, \ldots, x'_k$ inputs to be the all-1 strings and consider the $(x'_3, \ldots, x'_k)$-slice of $T$ denoted $T_{x'_3 \cdots x'_k}$. Then $rank(T_{x'_3 \cdots x'_k}) = rank(M_{IP_n}) = 2^n - 1$, because by fixing $x_3, \ldots, x_k$ to all 1s, the entries of $T$ become $\langle x_1 | x_2 \rangle$ for all $x_1, x_2 \in \{0,1\}^n$.

Let $x^{(i)}$ denote the string $x$ with the $i^{th}$ bit flipped. For $i = 3, \ldots, k$ consider the slice $T_{x'_3 \cdots x'_{k-1} x'^{(i)}_k}$ of $T$. Then

$$T_{x'_3 \cdots x'_{k-1} x'^{(i)}_k}[x_1, x_2] = \langle x_1 | x_2 \rangle - x_{1i} x_{2i},$$

where the non-zero entries agrees with the non-zero entries of $M_{IP_{n-1}}$ by deleting the $i^{th}$ bits of $x_1$ and $x_2$. Thus, $rank(T_{x'_3 \ldots x'_{k-1} x'^{(i)}_k}) = (2^n - 1)/2$.

The 1-mode unfolding of $T$ is obtained by fixing every index except $x_1$. Thus

$$T_{(1)} = \begin{bmatrix} T_{x'_3 \ldots x'_k} & T_{x'_3 \ldots x'^{(3)}_k} & \cdots & T_{x'_3 \ldots x'^{(k)}_k} & \cdots \end{bmatrix},$$

with $2^{(k-1)n}$ columns. We known that $T_{x'_3 \ldots x'_k}$ and $T_{x'_3 \ldots x'^{(i)}_k}$ for each $i = 3, \ldots, k$ have $(2^n - 1)$ and $(2^n - 1)/2$ linearly independent columns respectively. Also, each of these columns are pair-wise linearly independent. Thus, $rank_1(T) \geq (2^n - 1)k/2$, which implies $rank(T) \geq (2^n - 1)k/2$. □

## Appendix B. Proofs of Technical Lemmas

B.1. **Proof of Lemma 3.3.** If $f(x, y) = 0$ then $v(x, y) =$ for all $\alpha_u, \beta_v$. If $f(x, y) \neq 0$ there exists $(u', v')$ such that $v(x, y) \neq 0$. Here we use the same arguments given by de Wolf [5], i.e., we show that $v(x, y) = 0$ happens with small probability. In fact, having families of vectors with different dimensions does not affect the argument. Consider the situation where all $\alpha_u$ and $\beta_v$ were chosen except $\alpha_{u'}$ and $\beta_{v'}$. Write $v(x, y)$ in terms of these two coefficients

$$v(x, y) = c_0 \alpha_{u'} \beta_{v'} + c_1 \alpha_{u'} + c_2 \beta_{v'} + c_3,$$

where $c_0 = \sum_{i=1}^r A_i(x)_u B_i(y)_v \neq 0$. If we fix $\alpha_{u'}$ then, $v(x, y)$ is a linear equation with at most one solution (zero). Therefore, we have at most $2^{2n+1} \cdot 1$ ways of choosing $\alpha_{u'}$ and $\beta_{v'}$ such that $v(x, y) = 0$. Thus

$$Pr[v(x, y) = 0] \leq \frac{2^{2n+1}}{(2^{2n+1})^2} < \frac{2^{2n+2}}{(2^{2n+1})^2} = 2^{-2n}.$$

By the union bound

$$Pr[\exists (x, y) \in f^{-1}(1) \text{ s.t. } v(x, y) = 0] \leq \sum_{(x,y) \in f^{-1}(1)} Pr[v(x, y) = 0] < 2^{2n} \cdot 2^{-2n} = 1.$$

The following is a probabilistic method argument. Since the above probability is strictly less than 1, there exists with positive probability sets $\{a_1(x), \ldots, a_r(x)\}$ and $\{b_1(y), \ldots, b_r(y)\}$ such that for every $(x, y) \in f^{-1}(1)$ we have $v(x, y) \neq 0$. □

B.2. **Proof of Lemma 3.4.** Let $T$ be a nondeterministic tensor for a function $f$ with $nrank(f) = r$. We divide the proof in two cases.

*Even k:* Fix two players, say $P_1$ (Alice) and $P_k$ (Bob). Also fix some matrization of $T$, i.e., let $M$ be such matrization and consider it as an operator $M : \mathcal{H}_{k/2+1} \otimes \cdots \otimes \mathcal{H}_k \to \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_{k/2}$. Thus $M$ is a $2^{kn/2} \times 2^{kn/2}$-matrix that maps elements from the $\mathcal{H}_{k/2+1} \otimes \cdots \otimes \mathcal{H}_k$ subspace to the $\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_{k/2}$ subspace. Let also $M = U \Sigma V$ be the singular value decomposition of $M$ such that $U, V$ are $2^{kn/2} \times 2^{kn/2}$ unitary matrices, and $\Sigma$ is a $2^{kn/2} \times 2^{kn/2}$ diagonal matrix containing the singular values of $M$ in the diagonal. The number of singular values is at most $rank(M) \leq r$.

Bob computes the state $|\phi_{1 \cdots k/2}\rangle = c_{1 \cdots k/2} \Sigma V |x_1, \ldots, x_{k/2}\rangle$ where $c_{1 \cdots k/2}$ is some normalizing constant that depends on $x_1, \ldots, x_{k/2}$. Since only the first entries of $\Sigma$ are non-zero, $|\phi_{1 \cdots k/2}\rangle$ has at most $r$ non-zero entries, so the state can be compressed using $\log r$ qubits[4]. Bob send these qubits to Alice. Alice then computes $U|\phi_{1\cdots k/2}\rangle$ and measure that state. If Alice observes $x_{k/2+1}, \ldots, x_k$ then she puts a 1 on the qubit channel, and otherwise she puts a 0. The probability of Alice putting a 1 on the channel is

$$\begin{aligned} \left|\langle x_{k/2+1}, \ldots, x_k|U|\phi_{1\cdots k/2}\rangle\right|^2 &= |c_{1\ldots,k/2}|^2 \left|\langle x_{k/2+1}, \ldots, x_k|U\Sigma V|x_1, \ldots, x_{k/2}\rangle\right|^2 \\ &= |c_{1\ldots,k/2}|^2 \left|\langle x_{k/2+1}, \ldots, x_k|M|x_1, \ldots, x_{k/2}\rangle\right|^2 \\ &= |c_{1\ldots,k/2}|^2 \left|M[x_1, \ldots, x_k]\right|^2 \\ &= |c_{1\ldots,k/2}|^2 \left|T[x_1, \ldots, x_k]\right|^2. \end{aligned}$$

Since $T[x_1, \ldots, x_k]$ is non-zero if and only if $f(x_1, \ldots, x_k) = 1$, this probability will be positive if and only if $f(x_1, \ldots, x_k) = 1$. Thus, this is a nondeterministic protocol with total cost $\log r + 1$.

*Odd $k$:* To use the protocol given in the even case, we add an extra degree of freedom to $T$.

**Lemma B.1.** *If $T$ is an order-$k$ tensor with rank $r$ then, there exists a tensor $T'$ of order $k+1$ with rank $r$ where $T[x_1, \ldots, x_k] = T'[x_1, \ldots, x_k x_{k+1}]$ for all $x_{k+1}$.*

By the above lemma, we have that for any given $x_{k+1}$, $T'[x_1, \ldots, x_k x_{k+1}] = 0$ if and only if $f(x_1, \ldots, x_k) = 0$ . See below for a proof of Lemma B.1.

Before the protocol starts, each player knows $T'$ (which has even order) and its matrization $M'$. We fix two players, $P_1$ (Alice) and $P_k$ (Bob), and they can now use the protocol for even $k$. $\square$

B.3. **Proof of Lemma B.1.** Let $T = \sum_{i=1}^r |v_1^i\rangle \cdots |v_k^i\rangle$ for some family of $d$-dimensional vectors. Define $T' = \sum_{i=1}^r |v_1^i\rangle \cdots |v_k^i\rangle |v_{k+1}^i\rangle$ where each $|v_{k+1}^i\rangle$ is the all-1 vector. Thus, component-wise we have that

$$T[x_1, \ldots, x_k] = \sum_{i=1}^r v_1^i(x_1) \cdots v_k^i(x_k),$$

and

$$T'[x_1, \ldots, x_k x_{k+1}] = \sum_{i=1}^r v_1^i(x_1) \cdots v_k^i(x_k) v_{k+1}^i(x_{k+1}),$$

where $v_{k+1}^i(x_{k+1}) = 1$ for all $i$ and for all inputs $x_{k+1}$. Then $T'[x_1, \ldots, x_k x_{k+1}] = \sum_{i=1}^r v_1^i(x_1) \cdots v_k^i(x_k)$ and $T'[x_1, \ldots, x_k x_{k+1}] = T[x_1, \ldots, x_k]$ for any $x_{k+1}$. $\square$

[4]A $n$ dimensional vector can be encoded as a quantum state with $\log n$ qubits by observing that a $k$-qubit state is a $2^k$-dimensional vector. This fact was used by Raz to show an exponential separation between classical and quantum 2-party communication [13].

ECCC ISSN 1433-8092

http://eccc.hpi-web.de