PAPER

# Tensor Rank and Strong Quantum Nondeterminism in Multiparty Communication*

**Marcos VILLAGRA**[†a)], ***Nonmember***, **Masaki NAKANISHI**[††b)], ***Member***,
**Shigeru YAMASHITA**[†††c)], ***Senior Member***, ***and*** **Yasuhiko NAKASHIMA**[†d)], ***Nonmember***

**SUMMARY** 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 $f$ when there is no prior shared entanglement between the players, 1) in the Number-On-Forehead model the cost is upper-bounded by the logarithm of $nrank(f)$; 2) in the Number-In-Hand model the cost is lower-bounded by the logarithm of $nrank(f)$. Furthermore, we show that when the number of players is $o(\log\log n)$, we have $NQP \not\subseteq BQP$ for Number-On-Forehead communication.

***key words:*** *multiparty communication complexity, quantum computation, quantum nondeterminism, tensor rank*

## 1. Introduction

Nondeterminism plays a fundamental role in complexity theory. For instance, the $P$ vs $NP$ problem asks if nondeterministic polynomial time is strictly more powerful than deterministic polynomial 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, in addition to 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 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 in the context of query and communication complexities started with de Wolf [1]. In particular, de Wolf [1], [2] introduced the notion of *nondeterministic rank* of a matrix, which was proved to completely characterize strong quantum nondeterministic communication. In the same piece of work, it was proved that strong quantum nondeterministic protocols are exponentially stronger than classical nondeterministic protocols. Similarly, Le Gall [3] 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 [2] and Le Gall [3] were on the context of 2-party communication complexity, i.e., there are two players with two inputs $x, y \in \{0,1\}^n$ 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 by [4] is $\lceil \frac{1}{2}\log rank(f) \rceil \leq Q(f) \leq D(f)$, where $D(f)$ is the deterministic communication complexity of $f$ and $Q(f)$ the quantum exact communication complexity**. It is conjectured that $D(f) = O(\log^c rank)$ for some constant $c$. This is the *log-rank conjecture* in communication complexity, one of the biggest open problems in the field. If it holds, it will imply that $Q(f)$ and $D(f)$ are poly-

Manuscript received June 14, 2012.
Manuscript revised September 10, 2012.

[†]The authors are with the Graduate School of Information Science, Nara Institute of Science and Technology, Ikoma-shi, 630–0192 Japan.
[††]The author is with the Faculty of Education, Art and Science, Yamagata University, Yamagata-shi, 990–8560 Japan.
[†††]The author is with the Department of Computer Science, Ritsumeikan University, Kusatsu-shi, 525–8577 Japan.

*A preliminary version of this paper appeared in Proceedings of the 9th Annual Conference on Theory and Applications of Models of Computation (TAMC'12), LNCS 7287, pp.400–411, Beijing, China, May 16–21, 2012.

a) E-mail: marcos.villagra@acm.org
b) E-mail: m-naka@e.yamagata-u.ac.jp
c) E-mail: ger@cs.ritsumei.ac.jp
d) E-mail: nakashim@is.naist.jp

DOI: 10.1587/transinf.E96.D.1

**All logarithms in this paper are base 2.

nomially related. This is in stark contrast to the characterization given by de Wolf [2] 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 $f(x, y) = 1$.

### 1.1 Contributions

In this paper, we continue the study of strong quantum nondeterminism in the context of multiparty protocols. Let $k \geq 2$ be the number of players evaluating a function $f(x_1, \ldots, x_k)$ where each $x_i \in \{0,1\}^n$. 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 computation of the protocol ends when the last player computes $f$. 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 the 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, unlike matrix rank for which there exist polynomial-time algorithms, computing tensor rank is *NP*-hard [5]. See the survey paper by Kolda and Bader [6] for more differences.

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 without prior shared entanglement for the NOF and NIH models respectively.

**Theorem 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 previous results by de Wolf [2]. Also, since $NQ_k^{NIH}$ is a lower bound for exact NIH quantum communication[†], denoted $Q_k^{NIH}$, we obtain the following corollary:

**Corollary 2:** $\lceil \log nrank(f) \rceil + 1 \leq Q_k^{NIH}(f)$.

The proof of Theorem 1 is given in Sect. 3. Even though it is a generalization of the techniques of [2], it requires technical insight. The proof does not generalize in a straightforward manner and it does not yield the same characterization as in the 2-player case. For example, $NQ_k^{NOF}$ cannot be lower-bounded in general by the tensor rank. To see this consider the $k$-party equality function $EQ$ given by $EQ_k(x_1, \ldots, x_k) = 1$ if and only if $x_1 = \cdots = x_k$. A nondeterministic tensor for $EQ_k$ is superdiagonal[††]. Thus, it has $2^n$ rank, and implies by Theorem 1 that $NQ_k^{NOF}(EQ_k) \leq n + 1$ and $NQ_k^{NIH}(EQ_k) \geq n + 1$. In particular, the communication complexity of $EQ_k$ is upper-bounded by $O(n)$ in the NOF model. However, it is easy to show that in the NOF model there exists a classical protocol for $EQ_k$ with a cost of 2 bits[†††]. Hence, the characterization for the 2-player case does not extends to the multiplayer case. In contrast, the lower bound on $NQ_k^{NIH}(EQ_k)$ that follows from Theorem 1 is not that loose; using the trivial protocol, where all players send their inputs, we have that $NQ_k^{NIH}(EQ_k) = O(kn)$. Thus, Theorem 1 yields a tight bound for $EQ_k$ whenever $k = O(1)$. However, whether the same phenomenon extends to all functions in the NIH model is unknown. See below in this section for some consequences on constructing tensors with high rank.

A more interesting function is the generalized inner product $GIP_k(x_1, \ldots, x_k) = (\sum_{i=1}^{k} \bigwedge_{j=1}^{n} x_{ij}) \mod 2$. We know that $nrank(GIP_k) \geq (k-1)2^{n-1} + 1$ (see Sect. 5 for a proof). Thus, we have the following result.

**Proposition 3:** $NQ_k^{NIH}(GIP_k) \geq n + \lceil \log(k-1) \rceil - 1$.

In NIH, using the trivial protocol, we obtain (with Corollary 2) a bound in quantum exact communication of $n + \lceil \log(k-1) \rceil - 1 \leq Q_k^{NIH}(GIP_k) \leq (k-1)n + 1$. Improving the lower bound will require new techniques for explicit construction of linear-rank tensors with important consequences to circuit lower bounds; see for example Raz [7] and the paper by Alexeev, Forbes and Tsimerman [8] for state-of-the-art tensor constructions. In general, we are still unable to upper-bound $NQ_k^{NIH}(f)$ in terms of $\log nrank$. In this way, we have a new *log-rank conjecture* for strong quantum nondeterministic communication complexity.

Although the bounds given by Theorem 1 could be loose for some functions, they are good enough for other applications. For instance, we show in Sect. 4 a separation between the NOF models of strong quantum nondeterminism and bounded-error quantum communication. We do so by applying Theorem 1 to a total function explicitly constructed for this task. This result could be considered as the quantum analog of a separation previously proved in [9]–[11] between classical nondetermistic and randomized NOF communication.

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

[††] An order-$k$ tensor is *superdiagonal* when $T[x_1, \ldots, x_k] \neq 0$ if and only if $x_1 = \cdots = x_k$.

[†††] In the blackboard model (explained in Sect. 2) for $k \geq 3$, 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. In the message-passing model the same protocol has a cost of $O(k)$ bits.

## 2. Preliminaries

In this paper we assume basic knowledge of communication complexity and quantum computing. We refer the interested reader to the books by [12] and [13] respectively. 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 1** (Simple Tensor): 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 $d \geq 3$.

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 spans the space $V^{n_1} \otimes \cdots \otimes V^{n_d}$, and hence, there exist tensors that are not simple. This leads to the definition of rank.

**Definition 2** (Tensor Rank): 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 [5] 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; see Kolda and Bader [6].

### 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 definition.

**Definition 3** (Classical Nondeterministic Protocol): Let $k$ be the number of players. In order to communicate, the players take turns in an order predefined at the beginning of the protocol. Each 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, the protocol accepts $x$ with positive probability; if $f(x) = 0$, the protocol rejects $x$ with probability 1. The cost of the protocol is 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 by *message-passing*, 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 immediately. Clearly, any lower bound on the blackboard model is a lower bound for the message-passing model in this paper.

To model NOF and NIH in the quantum setting, we follow the work of Lee, Schechtman, and Shraibman [14], originally defined by Kerenidis [15].

**Definition 4** (Quantum Multiparty Protocol): Let $k$ be the number of players in the protocol. Define the Hilbert space by $\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_k \otimes C$, where each $\mathcal{H}_i$ is the Hilbert space of player $i$, and $C$ 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 $\mathcal{H}_i \otimes C$, and acts as the identity anywhere else;
2. in NOF, an arbitrary unitary that depends on all inputs except $x_i$ is applied on $\mathcal{H}_i \otimes C$, and acts as the identity anywhere else.

The cost of the protocol is the number of rounds.

The initial state is a pure state $|0\rangle \otimes \cdots \otimes |0\rangle |0\rangle$ without any 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 5** (Strong Quantum Nondeterministic Protocol): 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, denoted $NQ_k(f)$, is the cost of an optimum (i.e., minimal cost) $k$-party quantum nondeterministic communication protocol. 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.

The following lemma, given in Lee, Schechtman, and Shraibman [14], generalizes a previous observation made by Yao [16] and Kremer [17] on 2-party protocols.

**Lemma 4:** After $\ell$ qubits of communication on input $(x_1, \ldots, x_k)$, the state of a quantum protocol without prior shared entanglement can be written as

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

where $m_\ell$ is the $\ell$-th bit in $m$, and each vector $\left|A_m^t(x^t)\right\rangle$ 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

### 3.1 Lower Bound

The arguments in this section are generalizations of a previous result by [2] from 2-party to $k$-party communication for $k \geq 3$. First we need the following technical lemma (see below for a proof).

**Lemma 5:** If there exist $k$ families of vectors such that $\{\left|A_1^i(x_i)\right\rangle, \ldots, \left|A_r^i(x_i)\right\rangle\} \subseteq \mathbb{C}^d$ for all $i$ with $1 \leq i \leq k$ and $x_i \in \{0,1\}^n$ given that

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

then $nrank(f) \leq r$.

Now we proceed to prove the lower bound as stated in Theorem 1.

**Lemma 6:** $NQ_k^{NIH}(f) \geq \lceil \log nrank(f) \rceil + 1$

*Proof:* Consider a NIH $\ell$-qubit protocol for $f$. By Lemma 4 its final state is

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

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,

$$|\phi(x_1, \ldots, x_k)\rangle = \sum_{m\in S} \left|A_m^1(x_1)\right\rangle \cdots \left|A_m^k(x_k)\right\rangle |1\rangle . \quad (2)$$

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 5, we have that $nrank(f) \leq |S| = 2^{\ell-1}$, which implies the lower bound. □

*Proof of Lemma 5:* Let $k \geq 3$. We divide the proof 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 $\{\left|A_1^i(x_i)\right\rangle, \ldots, \left|A_r^i(x_i)\right\rangle\}$ for $1 \leq i \leq k/2$ construct a new family

$$\begin{aligned}\mathscr{D} &= \left\{ \bigotimes_{j=1}^{k/2} \left|A_1^j(x_j)\right\rangle, \ldots, \bigotimes_{j=1}^{k/2} \left|A_r^j(x_j)\right\rangle \right\} \\ &= \left\{ |A_1(y)\rangle, \ldots, |A_r(y)\rangle \right\},\end{aligned}$$

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

$$\begin{aligned}\mathscr{F} &= \left\{ \bigotimes_{j=k/2+1}^{k} \left|A_1^j(x_j)\right\rangle, \ldots, \bigotimes_{j=k/2+1}^{k} \left|A_r^j(x_j)\right\rangle \right\} \\ &= \left\{ |B_1(z)\rangle, \ldots, |B_r(z)\rangle \right\},\end{aligned}$$

where $z = (x_{k/2+1}, \ldots, x_k)$. 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 $k = 2$ from [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 number of elements $r$, 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 families $\{|A_1(y)\rangle, \ldots, |A_r(y)\rangle\} \subseteq \mathbb{C}^{d'}$ and $\{|B_1(z)\rangle, \ldots, |B_r(z)\rangle\} \subseteq \mathbb{C}^{d'+1}$, both with cardinality $r$.

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, if $f(y, z) = 0$ then $\sum_{i=1}^{r} A_i(y)_u B_i(z)_v = 0$ for all $(u, v)$; if $f(y, z) = 1$ then $\sum_{i=1}^{r} A_i(y)_u B_i(z)_v \neq 0$ for some $(u, v)$. This holds because each vector $|A_i(y)\rangle$ and $|B_i(z)\rangle$ are the set of vectors $\left|A_i^t(x^t)\right\rangle$ 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 [2] 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 for a proof).

**Lemma 7:** Let $I$ be an arbitrary set of real numbers of size $2^{2n+1}$. Let $\alpha_1, \ldots, \alpha_{d'}$ and $\beta_1, \ldots, \beta_{d'+1}$ 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

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

There exists $\alpha_1,\ldots,\alpha_{d'},\beta_1,\ldots,\beta_{d'+1} \in I$ 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 a nondeterministic order-$k$ tensor of rank $r$. □

### 3.2 Upper Bound

The proof of the upper bound 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 [2].

**Lemma 8:** $NQ_k^{NOF}(f) \leq \lceil \log nrank(f) \rceil + 1$.

*Proof:* Let $T$ be a nondeterministic tensor for $f$ 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 $\left|\phi_{1\cdots k/2}\right\rangle = c_{1\cdots k/2}\Sigma V\left|x_1,\ldots,x_{k/2}\right\rangle$ 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, $\left|\phi_{1\cdots k/2}\right\rangle$ has at most $r$ non-zero entries, so the state can be compressed using $\log r$ qubits[†]. Bob sends these qubits to Alice. Alice then computes $U\left|\phi_{1\cdots k/2}\right\rangle$ and measures 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

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

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 9:** 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 $T'[x_1,\ldots,x_kx_{k+1}] = 0$ if and only if $f(x_1,\ldots,x_k) = 0$ for any given $x_{k+1}$. See Appendix for a proof.

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 $k$. □

## 4. Some Separations for Complexity Classes

In this section we take a complexity-theoretic view of quantum multiparty communication complexity. For this model we consider as "efficient communication" when a protocol computes a function with $polylog(n)$ bits [19].

**Definition 6:** We define the following communication complexity classes:

1. $BPP^{cc}$ is the class of boolean functions with a classical bounded-error protocol of cost $polylog(n)$;
2. $BQP^{cc}$ is the class of boolean functions with a quantum bounded-error protocol of cost $polylog(n)$;
3. $NQP^{cc}$ is the class of boolean functions with a quantum strong nondeterministic protocol of cost $polylog(n)$.

In the following we present two theorems that give separations between the complexity classes defined above. First, for better understanding, we start by showing a weaker but easier to prove result, a separation between $NQP^{cc}$ and $BPP^{cc}$. Then we use that result to separate $NQP^{cc}$ from $BQP^{cc}$. Although this latter result can be proved without the need of the former, starting with the separation from $BPP^{cc}$ seems easier to understand.

**Proposition 10:** For NOF communication we have that $NQP^{cc} \not\subseteq BPP^{cc}$ whenever the number of players $k = o(\log\log n)$.

*Proof:* To prove this we exhibit a function $f : X^k \to \{0,1\}$ such that $NQ_k^{NOF}(f) = O(\log n)$ and $R_{\epsilon,k}(f) = \Omega(n^{1/(k+1)}/(k2^{2^k}))$, where $R_{\epsilon,k}$ denotes the bounded-error NOF communication complexity with error probability upper-bounded by $\epsilon$. This will give the separation whenever $k = o(\log\log n)$.

In particular, we analyze the following total function. Let $x_1,\ldots,x_k \in X$ with $X = \{0,1\}^n$, then

$$f(x_1,\ldots,x_k) = \begin{cases} 1 & \text{if } |x_1 \wedge \cdots \wedge x_k| \neq 1 \\ 0 & \text{if } |x_1 \wedge \cdots \wedge x_k| = 1 \end{cases}, \qquad (3)$$

where $\wedge$ denotes the bit-wise AND and $|x|$ is the Hamming

[†]An $n$-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 [18] to show an exponential separation between classical and quantum 2-party communication.

weight of $x$. This function was previously studied by de Wolf [2] in the 2-player case.

*Upper Bound:* For each $i$ let $x_i = x_{i1} \dots x_{in}$ and let $T_j$ be an order-$k$ tensor where $T_j[x_1, \dots, x_k] = 1$ if $x_{1j} \wedge \cdots \wedge x_{kj} = 1$ and $T_j[x_1, \dots, x_k] = 0$ otherwise. Note that for each $j$ the tensor $T_j$ has rank 1. Define the order-$k$ tensor $T$ by

$$T[x_1, \dots, x_k] = \sum_{j=1}^{n} T_j[x_1, \dots, x_k] - 1.$$

This tensor has rank $n$. Also $T$ is a nondeterministic communication tensor for $f$ since $T[x_1, \dots, x_k] = 0$ if and only if $|x_1 \wedge \cdots \wedge x_k| = 1$. Hence, by Theorem 1 the upper bound follows.

*Lower Bound:* To prove the lower bound we will use, without loss of generality, the sign version of Eq. (3), i.e.,

$$f(x_1, \dots, x_k) = \begin{cases} 1 & \text{if } |x_1 \wedge \cdots \wedge x_k| \neq 1 \\ -1 & \text{if } |x_1 \wedge \cdots \wedge x_k| = 1 \end{cases}. \tag{4}$$

We make use of a result by Lee and Shraibman [20]. Let $\mu^\alpha$ be the *approximate cylinder intersection norm* as defined in [20], and let $\widetilde{deg}(f)$ be the *approximate degree* of a boolean function $f$ [21].

**Lemma 11:** Let $f_n : \{0,1\}^n \to \{-1,1\}$ be a symmetric[†] function, and let $F_f : (\{0,1\}^n)^k \to \{-1,1\}$ be a function (not necessarily symmetric) defined by $F_f(x_1, \dots, x_k) = f(x_1 \wedge \cdots \wedge x_k)$. Let $\alpha > 1/(1-2\epsilon)$ and set $c = 2e(k-1)2^{2^{k-1}}$, then

$$R_{1/4,k}(F_{f_n}) = \Omega(\log \mu^\alpha(F_{f_n})) = \Omega\left(\frac{\widetilde{deg}(f_m)}{2^k}\right),$$

where $n = \left(c/\widetilde{deg}(f_m)\right)^{k-1} m^k$.

Note that Lemma 11 is a generalization of [20, Corollary 6.1] to symmetric functions. However, as pointed by the authors of [20], this generalization is straightforward and can be easily proved by following the proof of [20, Corollary 6.1], and it is therefore omitted from this paper.

Define the following Hamming weight function:

$$w(x) = \begin{cases} 1 & \text{if } |x| \neq 1 \\ -1 & \text{if } |x| = 1 \end{cases}.$$

This way we can write Eq. (4) as $f(x_1, \dots, x_k) = w(x_1 \wedge \cdots \wedge x_k)$. Also note that $w$ is symmetric and we can apply Lemma 11. Together with the characterization given by Paturi [22] of the approximate degree of symmetric functions we have that

$$\log \mu^\alpha(f) = \Omega\left(\frac{n^{1/(k+1)}}{k2^{2^k}}\right). \tag{5}$$

□

**Theorem 12:** For NOF communication we have that $NQP^{cc} \not\subseteq BQP^{cc}$ whenever the number of players $k = o(\log \log n)$.

*Proof:* To prove this we rely again in Eq. (4) and the fact that $NQ_k^{NOF}(f) = O(\log n)$. Here we show that $Q_{\epsilon,k}(f) = \Omega(n^{1/(k+1)}/(k2^{2^k}) - k)$, where $Q_\epsilon$ denotes the bounded-error NOF communication complexity with error probability upper-bounded by $\epsilon$.

Note that to prove Proposition 10 we derived a lower bound on $\mu^\alpha$, i.e., Eq. (5). We can use the same lower bound to prove the separation for $BQP^{cc}$. In order to do that we make use of the following two results by Lee, Schechtman, and Shraibman [14]. Let $\gamma^\alpha$ be the *approximate quantum norm* as defined in [14].

**Lemma 13:** Let $T$ be an order-$k$ sign-tensor, then $Q_{\epsilon,k}(T) = \Omega(\log \gamma^\alpha(T))$.

**Lemma 14:** For every order-$k$ tensor $T$, $\gamma(T) \leq \mu(T) \leq C^k \gamma(T)$, for some absolute constant $C$.

Thus, by these two lemmas above and Eq. (5) we have

$$\log \gamma^\alpha(f) = \Omega\left(\frac{n^{1/(k+1)}}{k2^{2^k}} - k\right).$$

□

## 5. Nondeterministic Rank Lower Bound of GIP

In this section we give a lower bound on the nondeterministic rank of the Generalized Inner Production (GIP) function. Remember that for $k \geq 2$ players $GIP_k(x_1, \dots, x_k) = (\sum_{i=1}^{k} \bigwedge_{j=1}^{n} x_{ij}) \mod 2$.

**Lemma 15:** $nrank(GIP_k) \geq (k-1)2^{n-1} + 1$.

*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. In general, a mode-$i$ fiber is a vector obtained by fixing all except the $i^{th}$ index. 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 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; see Kolda and Bader [6]. 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 $i$; see Lathauwer, de Moore, and Vandewalle [23].

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

[†]A function is called symmetric if it only depends on the number of 1s in the input.

Kushilevitz and Nisan [12]. The same holds even if $M_{IP_n}$ is defined over $\mathbb{C}$.

Let $\mathbf{1}$ denote the string of length $n$ with only 1s in it, and let $T'$ be the $(x'_3, \ldots, x'_k)$-slice of $T$ where $x'_i = \mathbf{1}$ for $i = 3, \ldots, k$. In this way $T'[x_1, x_2] \neq 0$ whenever $\langle x_1 |\ x_2 \rangle = 1$ and hence $rank(T') = rank(M_{IP_n}) = 2^n - 1$.

Let $x^{(i)}$ denote the string $x$ with the $i^{th}$ bit flipped. For $i = 3, \ldots, k$ consider the $(x'_3 \ldots x'_{k-1} x'^{(i)}_k)$-slice of $T$ denoted $T'_i$ where $x'_k(i)$ is the string $\mathbf{1}$ with the $i^{th}$ bit flipped to 0. Then

$$T'_i[x_1, x_2] \neq 0 \text{ whenever } \langle x_1 |\ x_2 \rangle - x_{1i}x_{2i} = 1. \qquad (6)$$

Note that the non-zero entries of $T'_i$ for any $i$ agrees with the non-zero entries of $M_{IP_{n-1}}$, where $M_{IP_{n-1}}$ is obtained by deleting the $i^{th}$ bits of $x_1$ and $x_2$ in $M_{IP_n}$ for all $x_1, x_2$. Thus, $rank(T'_i) = 2^{n-1} - 1$ for all $i = 3, \ldots, n$.

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

$$T_{(1)} = \begin{bmatrix} T' & T'_3 & \cdots & T'_k & \cdots \end{bmatrix},$$

with $2^{(k-1)n}$ columns, where the right part (after $T'_k$) of $T_{(1)}$ is filled with the slices from $T$ that are different to $T'$ and $T'_i$ for all $i = 3, \ldots, n$. We know that $T'$ and $T'_i$ for each $i = 3, \ldots, k$ have $(2^n - 1)$ and $2^{n-1} - 1$ linearly independent columns respectively. Also, each of these columns are pair-wise linearly independent. To see this, just take any two slices $T'_i$ and $T'_j$ for any $i \neq j$, fix one column in each and compute the inner product according to Eq.(6). Thus, $rank(T) \geq rank_1(T) \geq 2^n - 1 + (k-2)(2^{n-1} - 1) = (k-1)2^{n-1} + 1$. □

## 6. 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 logarithm of the rank of the nondeterministic communication tensor; ii) strong quantum nondeterministic NIH communication complexity is lower-bounded by the logarithm of the rank of the nondeterministic communication tensor. These results naturally generalize previous work by de Wolf [2]. 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 that $NQP^{cc} \not\subseteq BPP^{cc}$ and $NQP^{cc} \not\subseteq BQP^{cc}$ when the number of players is $o(\log \log n)$. It remains as an open problem to prove the same separations with an increased number of players.

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.

## Acknowledgements

The authors thank the anonymous reviewers from TAMC'12 for initial reviews and the anonymous referees of the IEICE Transactions for their useful suggestions on improving this paper. The first author also thanks the NEC C&C Foundation for partially supporting this research.

### References

[1] R. de Wolf, "Characterization of non-deterministic quantum query and quantum communication complexity," Proc. 15th Annual IEEE Conference on Computational Complexity, pp.271–278, 2000.
[2] R. de Wolf, "Nondeterministic quantum query and quantum communication complexities," SIAM J. Comput., vol.32, no.3, pp.681–699, 2003.
[3] F. Le Gall, "Quantum weakly nondeterministic communication complexity," Proc. 31st International Symposium on Mathematical Foundations of Computer Science, Lect. Notes Comput. Sci., vol.4162, pp.658–669, 2006.
[4] H. Buhrman and R. de Wolf, "Communication complexity lower bounds by polynomials," Proc. 16th Annual IEEE Conference on Computational Complexity, pp.120–130, 2001.
[5] J. Håstad, "Tensor rank is NP-complete," J. Algorithms, vol.11, no.4, pp.644–654, 1990.
[6] T. Kolda and B. Bader, "Tensor decompositions and applications," SIAM Review, vol.51, no.3, pp.455–500, 2009.
[7] R. Raz, "Tensor-rank and lower bounds for arithmetical formulas," Proc. 42nd ACM Symposium on Theory of Computing, pp.659–666, 2010.
[8] B. Alexeev, M. Forbes, and J. Tsimerman, "Tensor rank: Some lower and upper bounds," Proc. 26th Annual IEEE Conference on Computational Complexity, 2011.
[9] M. David, T. Pitassi, and E. Viola, "Improved separations between nondeterministic and randomized multiparty communication," ACM Trans. Computation Theory, vol.1, no.2, p.5, 2009.
[10] A. Chatopadhyay and A. Ada, "Multiparty communication complexity of disjointness," tech. rep., arXiv:0801.3624, 2008.
[11] D. Gavinsky and A. Sherstov, "A separation of NP and coNP in multiparty communication complexity," Theory of Computing, vol.6, no.10, pp.227–245, 2010.
[12] E. Kushilevitz and N. Nisan, Communication Complexity, Cambridge University Press, 1997.
[13] M. Nielsen and I. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2000.
[14] T. Lee, G. Schechtman, and A. Shraibman, "Lower bounds on quantum multiparty communication complexity," Proc. 24th IEEE Conference on Computational Complexity, 2009.
[15] I. Kerenidis, "Quantum multiparty communication complexity and circuit lower bounds," Mathematical Structures in Computer Science, vol.19, no.1, pp.119–132, 2009.
[16] A.C.C. Yao, "Quantum circuit complexity," Proc. 34th Annual Symposium on Foundations of Computer Science, 1993.
[17] I. Kremer, "Quantum communication," Master's thesis, The Hebrew University of Jerusalem, 1995.
[18] R. Raz, "Exponential separation of quantum and classical communication complexity," Proc. 31st Annual ACM Symposium on the Theory of Computing, pp.358–367, 1999.
[19] L. Babai, P. Frankl, and J. Simon, "Complexity classes in communication complexity theory," Proc. 27th Annual Symposium on Foundations of Computer Science, pp.337–347, 1986.
[20] T. Lee and A. Shraibman, "Disjointness is hard in the multiparty number-on-the-forehead model," Computational Complexity, vol.18, no.2, pp.309–336, 2009.

[21] N. Nisan and M. Szegedy, "On the degree of Boolean functions as real polynomials," Proc. 24th Annual ACM Symposium on Theory of Computing, pp.462–467, 1992.
[22] R. Paturi, "On the degree of polynomials that approximate symmetric Boolean functions," 24th Annual ACM Symposium on Theory of Computing, pp.468–474, 1992.
[23] L. de Lathauwer, B. de Moore, and J. Vandewalle, "A multilinear singular value decomposition," SIAM J. Matrix Anal. Appl., vol.21, no.4, pp.1253–1278, 2000.

## Appendix: Proofs of Technical Lemmas

### A.1 Proof of Lemma 7

If $f(y,z) = 0$ then $v(y,z) = 0$ for all $\alpha_u, \beta_v$. If $f(y,z) \neq 0$ there exists $(u', v')$ such that $v(y,z) \neq 0$. Here we use the same arguments given by [2], i.e., we show that $v(y,z) = 0$ 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 $v(y,z)$ in terms of these two coefficients

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

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

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

By the union bound

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

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

### A.2 Proof of Lemma 9

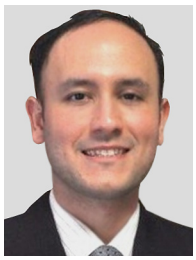
Let $T = \sum_{i=1}^{r} \left|v_1^i\right\rangle \cdots \left|v_k^i\right\rangle$ for some family of $d$-dimensional vectors. Define the tensor $T' = \sum_{i=1}^{r} \left|v_1^i\right\rangle \cdots \left|v_k^i\right\rangle \left|v_{k+1}^i\right\rangle$ where each $\left|v_{k+1}^i\right\rangle$ is the 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 $x_{k+1}$.



**Marcos Villagra** is a Ph.D. candidate at Graduate School of Information Science, Nara Institute of Science and Technology. He received the M.S. degree in Computer Science from Nara Institute of Science and Technology in 2010, and B.S. degrees in Informatics Engineering and Computer Science from Catholic University of Asuncion, Paraguay, in 2006 and 2005 respectively. From April 2008 he is a recipient of the MEXT scholarship for graduate studies granted by the Japanese Government. His research interests include computational complexity theory and quantum computing.

**Masaki Nakanishi** received the B.E., M.E. and Ph.D. degrees from Osaka University, Japan, in 1996, 1998 and 2002, respectively. He is currently with the Faculty of Education, Art and Science, Yamagata University, as an associate professor. His current interests include quantum computing and design of combinatorial algorithms.

**Shigeru Yamashita** is a professor of the Department of Computer Science, Ritsumeikan University. He received his B.E., M.E. and Ph.D. degrees in information science from Kyoto University, Kyoto, Japan, in 1993, 1995 and 2001, respectively. In 1995, he joined NTT Communication Science Laboratories, where he engaged in research of computer aided design of digital systems and new types of computer architectures. During 2000 to 2003, he was also a researcher at Quantum Computation and Information, ERATO, Japan Science and Technology Corporation. During 2003 to 2009, he was an associate professor of Graduate School of Information Science, Nara Institute of Science and Technology. He was a visiting researcher at Univ. Victoria, and Portland State Univ. in 2006. He received the 2000 IEEE Circuits and Systems Society Transactions on Computer-Aided Design of Integrated Circuits and Systems Best Paper Award. He is a member of IEEE and IPSJ.

**Yasuhiko Nakashima** received the B.E., M.E. and Ph.D. degrees in Computer Engineering from Kyoto University, Japan, in 1986, 1988, and 1998 respectively. He was a computer architect in the Computer and Systems Architecture Department, FUJITSU Limited in 1988–1999. From 1999 to 2005, he was an associate professor in the Graduate School of Economics, Kyoto University. Since 2006, he has been a professor in the Graduate School of Information Science, Nara Institute of Science and Technology. His research interest include processor architecture, emulation, CMOS circuit design, and evolutionary computation. He is a member of IEEE CS, ACM and IPSJ.