The Relationship between Inner Product and Counting Cycles

Xiaoming Sun[1],*, Chengu Wang[2],**, and Wei Yu[3],***

[1] Institute of Computing Technology,
Chinese Academy of Sciences
sunxiaoming@ict.ac.cn
[2] IIIS, Tsinghua University
wangchengu@gmail.com
[3] Aarhus University
yuwei@cs.au.dk

Abstract. CYCLE-COUNTING is the following communication complexity problem: Alice and Bob each holds a permutation of size n with the promise there will be either a cycles or b cycles in their product. They want to distinguish between these two cases by communicating a few bits. We show that the quantum/nondeterministic communication complexity is roughly $\tilde{\Omega}((n-b)/(b-a))$ when $a \equiv b \pmod 2$. It is proved by reduction from a variant of the inner product problem over $\mathbb{Z}_m$. It constructs a bridge for various problems, including IN-SAME-CYCLE [10], ONE-CYCLE [14], and BIPARTITENESS on constant degree graph [9]. We also give space lower bounds in the streaming model for the CONNECTIVITY, BIPARTITENESS and GIRTH problems [7]. The inner product variant we used has a quantum lower bound of $\Omega(n \log p(m))$, where $p(m)$ is the smallest prime factor of m. It implies that our lower bounds for CYCLE-COUNTING and related problems still hold for quantum protocols, which was not known before this work.

1 Introduction

The model of communication complexity was first introduced in [18], and then was studied extensively. The communication complexity model deals with the

* The author acknowledges supported in part by the National Natural Science Foundation of China Grant 61170062, 61061130540, the National Basic Research Program of China Grant 2011CBA00300, 2011CBA00301, and Tsinghua University Initiative Scientific Research Program 2009THZ02120.

** The author acknowledges supported in part by the National Basic Research Program of China Grant 2011CBA00300, 2011CBA00301, the National Natural Science Foundation of China Grant 61033001, 61061130540, 61073174.

*** The author acknowledges support from the Danish National Research Foundation and The National Science Foundation of China (under the grant 61061130540) for the Sino-Danish Center for the Theory of Interactive Computation, within which part of this work was performed.

D. Fernández-Baca (Ed.): LATIN 2012, LNCS 7256, pp. 643–654, 2012.

following game between Alice and Bob. Given a function $f : X \times Y \mapsto Z$, Alice holds $x \in X$, and Bob holds $y \in Y$. They will follow a protocol to let both of them know the value of $f(x, y)$ by sending and receiving bits from each other. We call the least number of bits transmitted in the protocol $D(f)$, the deterministic communication complexity for computing f.

The model could be extended to the case with randomization. In this scenario, Alice and Bob have shared random coins. The messages could also depend on these random coins. At the end of the communication, Alice and Bob will decide an output for the protocol, and we call this $P(x, y)$. We say P is a randomized protocol of f with error ϵ if for any input (x, y), $\Pr[P(x, y) = f(x, y)] \geq 1 - \epsilon$. The number of bits transmitted for the worst input (x, y) and the best protocol P is the randomized communication complexity $R_\epsilon(f)$. We also investigate nondeterministic protocols, where there exists a powerful agent who wants to convince Alice and Bob the answer. For $b \in \{0, 1\}$, we define $N^b(f)$ to be the amount of communication to convince Alice and Bob $f(x, y) = b$, including both the proof and the bits exchanged by Alice and Bob in order to verify the proof in the most efficient proof system. Since a deterministic protocol is both a randomized protocol and a nondeterministic protocol, we have $R_{1/3}(f) \leq D(f)$ and $\max\{N^0(f), N^1(f)\} \leq D(f)$. For comprehensive explanations on communication complexity, we refer the reader to [13].

The key problem we are going to talk about in this paper is the Cycle-Counting problem introduced in [17]. The problem could be stated as Alice and Bob each holds a permutation, and they want to decide the number of cycles in the product of the permutations, given the promise on the input that there are either a cycles or b cycles in the product permutation.

There are other problems related to the Cycle-Counting problem. For example, the In-Same-Cycle problem [10] is to decide whether the composition of two permutations is a Hamiltonian cycle. It was proved in [10] that the deterministic lower bound for the In-Same-Cycle problem is $\Omega(n)$. Here, we show that a randomized lower bound of $\Omega(n)$ could also be obtained, by a reduction from a special instance of the cycle counting problem (say, separating one cycle and three cycles). Furthermore, the same lower bound of $\Omega(n)$ could be obtained for the One-Cycle problem and the Bipartiteness problem as well. The One-Cycle problem is to decide if the product of two permutations is one cycle or more than one cycle. It was used in [14] to show a separation between log-rank and nondeterministic lower bound, by showing a nondeterministic lower bound of $\Omega(n \log\log n)$. Our lower bound is only $\Omega(n)$, but it is for randomized protocols and our proof is much easier. The Bipartiteness problem is to decide if a graph split into Alice and Bob's hand is bipartite or not. A deterministic bound of $\Theta(n \log n)$ was proved for general graphs in [9]. Here we show that even for graphs of maximum degree 3, a lower bound of $\Omega(n)$ can be obtained for nondeterministic/randomized protocols.

Besides communication complexity, we consider the streaming model as well. In streaming model, the input of a graph is represented by a sequence of edges in arbitrary order. The streaming complexity is the minimal amount of memory used by the algorithm if the algorithm only reads the input once sequentially. A lot of graph properties are studied in the streaming model. For example, in [5] counting triangles in a graph is investigated; in [8] approximation algorithms for matching, diameter and distance problems are given; and in [7] lots of graph properties including connectivity, bipartiteness, diameter and girth are discussed. For every problem discussed in this paper, the lower bound of the communication complexity implies the same lower bounds on the streaming complexity, by the standard reduction in [1]. Our lower bound of approximating the girth in the streaming model improves the result in [7] when the girth is large. Also, we prove the linear lower bound again for the connectivity and bipartiteness problems. All of them hold for randomized streaming algorithms reading the input in constant passes.

The lower bound for Cycle-Counting is obtained by reduction from a variant of the inner product modulo m problem. The problem could be briefly described as computing the inner product modulo m of two vectors in $\mathbb{Z}_m^n$, where Alice holds one of them, and Bob holds the other. The $m = 2$ case for this problem is well studied, and a lower bound of $\Omega(n)$ is known [13]. Besides, for prime m, the deterministic communication complexity is $\Omega(n \log m)$ [6, Theorem 3.4]. We are here to show a $\Omega(n \log p(m))$ nondeterministic/randomized lower bound for general m, where $p(m)$ is the smallest prime factor of m. This bound is tight for the case when m is prime ($p(m) = m$).

Furthermore, we know that the discrepancy method could also imply quantum communication complexity lower bounds [12]. In quantum settings, Alice and Bob have quantum computers and infinite shared entangled pairs of qubits, and they want to compute the function f with error ϵ by exchanging quantum bits. In the same way, we denote the quantum communication complexity of f (the minimum amount of qubits exchanged) by $Q_\epsilon^*(f)$. Since we can use quantum bits to generate random bits, $Q_{1/3}^*(f) = O(R_{1/3}(f))$ [12] and $R_{1/3}(f) \le D(f)$, which means that we can get randomized/deterministic lower bounds by quantum lower bounds. Thus in the rest of the paper, we will only talk about quantum and nondeterministic lower bounds.

2 Result Summary

In this section, we formally define all the problems, and state all the theorems only in the communication complexity model. The central problem is the following Cycle-Counting problem.

Definition 1 ($\mathbf{CC}_{n,a,b}$). *Let π, σ be permutations in symmetric group S_n with the promise that $\sigma \circ \pi$ has either a cycles or b cycles ($a < b$). The* Cycle-Counting *problem is a communication complexity problem that Alice holds π and Bob holds σ, and they want to return* 0 *for a cycles case and return* 1 *for b cycles case.*

We prove the following lower bound for $\mathrm{CC}_{n,a,b}$. It is almost tight (up to a $\log n$ factor) because of the upper bound for $\mathrm{CC}_{n,1,m}$.

Theorem 1. *The quantum/nondeterministic lower bound of* $\mathrm{CC}_{n,a,b}$ *is* $\Omega(\frac{n-b}{b-a+1} \cdot \log(p(b-a+1)-1) - \log(b-a+1))$ *when* $a \equiv b \pmod 2$, *where* $p(b-a+1)$ *is the smallest prime factor of* $b-a+1$.

Since the length of cycles are all the same in the hard case of $\mathrm{CC}_{n,1,b}$, to distinguish 1 cycle and b cycles is as hard as to distinguish girth n and girth n/b.

Corollary 1. $\Omega((\frac{n}{b}-1)\log(p(b)-1)-\log b)$ *communication is needed to determine whether the girth of a graph* G *is either* n *or* n/b *for quantum/nondeterministic protocols, if the edges of* G *is distributed to Alice and Bob, and* b *is odd.*

The streaming version of Corollary 1 improves the result in [7] when $b = O(n^{1/2-\epsilon})$.

Then, we show a similar lower bound holds for the In-Same-Cycle problem defined in [10].

Definition 2 (In-Same-Cycle). *Let* π, σ *be permutations in symmetric group* S_n. In-Same-Cycle$_n$ *is a communication complexity problem that Alice holds* π *and Bob holds* σ, *and they want to return* 1 *if elements* 1 *and* 2 *are in the same cycle of* $\sigma \circ \pi$, *and return* 0 *otherwise.*

As stated in [10], the In-Same-Cycle problem is a special case of the matroid intersection problem (abbr. MAT$-\cap$). So our lower bound holds for MAT$-\cap$ as well. Note that in [10] only nondeterministic lower bounds were discussed, here we also talk about quantum lower bound. We can show that by an easy argument that In-Same-Cycle is also hard in our hard case for $\mathrm{CC}_{n,1,3}$, thus we have the following corollary.

Corollary 2. *The quantum/nondeterministic lower bound of* In-Same-Cycle *is* $\Omega(n)$.

We also show the same lower bound holds for the following two problems, where the former was defined in [14] and the latter was defined in [9].

Definition 3 (One-Cycle). *Let* π, σ *be permutations in symmetric group* S_n. One-Cycle$_n$ *is a communication complexity problem that Alice holds* π *and Bob holds* σ, *and they want to return* 1 *if* $\sigma \circ \pi$ *is a Hamiltonian cycle, or return* 0 *otherwise.*

Definition 4 (Bipartiteness). *Let* $G_A = \langle V, E_A \rangle, G_B = \langle V, E_B \rangle$ *be two graphs on the same* n *vertices.* Bipartiteness$_n$ *is a communication complexity problem that Alice holds* G_A *and Bob holds* G_B, *and they want to return* 1 *if* $G_A \cup G_B = \langle V, E_A \cup E_B \rangle$ *is a bipartite graph, or return* 0 *otherwise.*

We show the hard case for $\mathrm{CC}_{n,1,3}$ is also a hard case for both of them, implying the following quantum/nondeterministic lower bound. A similar argument exists for the Bipartiteness problem.

Corollary 3. *The quantum/nondeterministic lower bound of* Bipartiteness$_n$ *is* $\Omega(n)$ *even for graphs with maximum degree* 3, *and the quantum/nondeterministic for* One-Cycle$_n$ *is* $\Omega(n)$.

By the standard relationship between (one-way) communication complexity and streaming lower bound [1], the following corollary is easy to get.

Corollary 4. *Any randomized streaming algorithm reading the input in constant passes that computes* In-Same-Cycle, Bipartiteness *or* One-Cycle *on a stream of edges will require $\Omega(n)$ space.*

Unlike the previous proof in [10] which directly investigated the properties of the cycle counting type problem, we prove the lower bound of $\mathrm{CC}_{n,a,b}$ by reducing from the "Inner Product modular m" problem, which is defined as following.

Definition 5 ($\mathbf{IP}_{m,n}$, $\mathbf{IP}^{01}_{m,n}$ and $\mathbf{IP}^{01*}_{m,n}$). *The inner product problem (*$\mathrm{IP}_{m,n}$*) is a communication complexity problem that Alice holds $x \in \mathbb{Z}^n_m$ and Bob holds $y \in \mathbb{Z}^n_m$, and they want to return the value of the inner product $\langle x, y\rangle = \sum_{i=1}^n x_i y_i$* mod *$m$.*

In the reduction we need two promised variants of $\mathrm{IP}_{m,n}$*:* $\mathrm{IP}^{01}_{m,n}$ *is the* $\mathrm{IP}_{m,n}$ *problem with the promise that $\langle x, y\rangle$ is either* 0 *or* 1*; and* $\mathrm{IP}^{01*}_{m,n}$ *is the* $\mathrm{IP}^{01}_{m,n}$ *problem with the promise that $y \in (\mathbb{Z}^*_m)^n$, where $\mathbb{Z}^*_m$ the primitive residue class modulo m (the set of integers relatively prime to m).*

The Inner Product problem on the binary field ($m = 2$ case) is well studied. It is known that $Q^*_{1/3}(\mathrm{IP}_{2,n}) = \Omega(n)$ [12], and $D(\mathrm{IP}_{p,n}) = \Omega(n \log p)$ for prime p [6]. However, what we actually need for this paper is the $\mathrm{IP}^{01*}_{m,n}$ problem. The problem looks classic but the authors of the paper failed to find a reference for the lower bound. So the proof for the following theorem is claimed in the paper to be "new" with conservation.

Theorem 2. *The quantum/nondeterministic lower bound of* $\mathrm{IP}^{01}_{m,n}$ *is $\Omega(n \log p(m) - \log m)$, and the lower bound of* $\mathrm{IP}^{01*}_{m,n}$ *is $\Omega(n \log(p(m) - 1) - \log m)$, where $p(m)$ stands for the smallest prime factor of m.*

Since $\mathrm{IP}^{01}_{m,n}$ is a special case of $\mathrm{IP}_{m,n}$, so the lower bound of $\mathrm{IP}^{01}_{m,n}$ also holds for $\mathrm{IP}_{m,n}$.

3 The Cycle Counting Problem and Its Variants

In this section we show the reduction from the inner product problem to the cycle counting problem, and its variants.

Theorem 3 (Theorem 1 Restated). *Let $p(x)$ denote the smallest prime factor of x, the following statements hold for the communication complexity of* Cycle-Counting*,*

1. *$Q^*_{1/3}(\mathrm{CC}_{n,1,m}) = \Omega((n/m - 1) \cdot \log(p(m) - 1) - \log m)$, for even m this lower bound is a trivial constant;*
2. *$Q^*_{1/3}(\mathrm{CC}_{n,a,b}) = \Omega((n - b)/(b - a + 1) \cdot \log(p(b - a + 1) - 1) - \log(b - a + 1))$, if $a \not\equiv b \pmod 2$ this lower bound is a trivial constant;*

3. $D(\mathrm{CC}_{n,a,b}) = 1$, *if* $a \not\equiv b \pmod 2$*;*
4. $R_{1/3}(\mathrm{CC}_{n,1,m}) = \min\{O(n \log n), O(n/m \cdot \log n \cdot \log(n/m))\}$.

Proof. Here we prove the reduction from $\mathrm{IP}^{01*}_{m,n}$ to $\mathrm{CC}_{m(n+1),1,m}$.

Let (x, y) be an input of the $\mathrm{IP}^{01*}_{m,n}$ problem where $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$, $x_i, y_i \in \mathbb{Z}_m$ for $i \in [n]$. According to the definition of $\mathrm{IP}^{01*}_{m,n}$, we have y_i is relatively prime to m for $i \in [n]$. Thus by Euclid algorithm we know that there is a y_i^{-1} for each y_i such that $y_i y_i^{-1} \equiv 1 \pmod m$. Let $y' = (y'_0, y'_1, \ldots, y'_{n-1}, y'_n) = (y_1^{-1}, y_1 y_2^{-1}, \ldots, y_{n-1} y_n^{-1}, y_n)$ and $x' = (x'_0, x'_1, \ldots, x'_n) = (0, x_1, \ldots, x_n)$.

We are going to construct a bipartite (black vertices on one side and white ones on the other) graph $G = \langle V, E \rangle$ as shown in Fig. 1, where $V = \{v_{i,j} | 0 \le i \le 2n{+}1, 0 \le j \le m{-}1\}$. Alice holds the edges from black vertices to white vertices, and Bob holds the edges from white vertices to black vertices. That is, the edge set Alice holds is $\{(v_{2i,j}, v_{2i+1,(j+x'_i) \bmod m})\}$, and the edge set Bob holds is $\{(v_{2i+1,j}, v_{(2i+2) \bmod (2n+2),(j \times y_i) \bmod m})\}$. Each row represents an element of $\mathbb{Z}_m$. The in-degree and out-degree of each vertex are both exactly 1, thus this bipartite graph is a union of two permutations. Imagining that we traverse the graph starting from vertex $v_{0,t}$, we will reach the 0-th layer again after following $2(n+1)$ edges, and the row we will reach is

$$\begin{aligned}
&(((((t + x'_0) \times y'_0) + x'_1) \times y'_1) + \cdots + x'_n) \times y'_n \mod m \\
&= (y'_0 y'_1 \cdots y'_n t + x'_0 y'_0 y'_1 \cdots y'_n + x'_1 y'_1 y'_2 \cdots y'_n + \cdots + x'_n y'_n) \mod m \\
&= (t + x_1 y_1 + x_2 y_2 + \cdots + x_n y_n) \mod m.
\end{aligned}$$

Since $x_1 y_1 + x_2 y_2 + \cdots + x_n y_n$ is promised to be 0 or 1 modulo m, we know that we will reach either $v_{0,t}$ or $v_{0,(t+1) \bmod m}$. That is, there will be either m cycles or a single cycle. By distinguishing these two cases, we can know the answer for

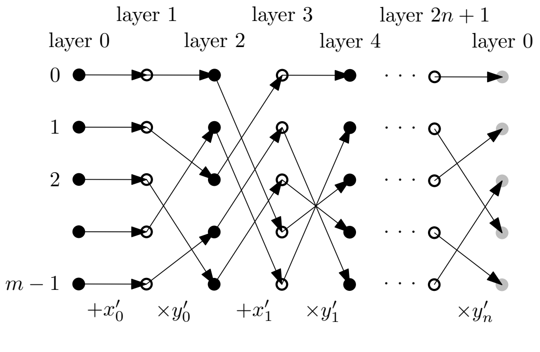

Fig. 1. The construction of a $\mathrm{CC}_{m(n+1),1,m}$ instance from an $\mathrm{IP}^{01*}_{n,m}$ instance. In this example, $m = 5$, $x'_0 = 0$, $y'_0 = 2$, $x'_1 = 3$, $y'_1 = 4$ and $y'_n = 3$. The gray vertices in the last layer are identical to the first layer. The graph is actually undirected. Directions here only serve the purpose for understanding.

$\mathrm{IP}^{01*}_{m,n}$, so $Q^*_{1/3}(\mathrm{CC}_{n,1,m}) \geq Q^*_{1/3}(\mathrm{IP}^{01*}_{m,n/m-1})$. By Theorem 2, $Q^*_{1/3}(\mathrm{CC}_{n,1,m}) = \Omega((n/m-1)\cdot\log(p(m)-1)-\log m)$. The $\mathrm{CC}_{n,a,b}$ problem could reduced from $\mathrm{CC}_{n-a+1,1,b-a+1}$ problem by adding $a-1$ dummy self cycles, resulting a lower bound of $Q^*_{1/3}(\mathrm{CC}_{n,a,b}) \geq Q^*_{1/3}(\mathrm{CC}_{n-a+1,1,b-a+1}) = \Omega((n-b)/(b-a+1)\cdot\log(p(b-a+1)-1)-\log(b-a+1))$. Due to space limitation, the proof for the upper bounds are delayed to the full version of this paper. □

For the In-Same-Cycle problem and the One-Cycle problem, one can easily observe that the reduction we used to get a lower bound of $\mathrm{CC}_{n,1,3}$ is also a reduction for both In-Same-Cycle and One-Cycle.

For the Bipartiteness problem, the proof is almost the same as the proof of the lower bound of $\text{Cycle-Counting}_{n,1,3}$, but we add an edge between $(0,0)$ and $(0,1)$ (the bold edge in Fig. 2). We know that a graph is bipartite if and only if there are no odd cycles in the graph. If the inner product is 0, the graph has of 3 even cycles, and the bold edge does not contribute to Bipartiteness. If the inner product is 1, after walking $2(n+1)$ steps from $(0,0)$ we reach $(0,1)$, then we go back to $(0,0)$ by the bold edge, so it contains an odd cycle of length $2n+3$, which means the graph is not bipartite. Therefore, the quantum/nondeterministic communication complexities of In-Same-Cycle, Bipartiteness and One-Cycle are all $\Omega(n)$. Thus, Corollary 2 and Corollary 3 follow.

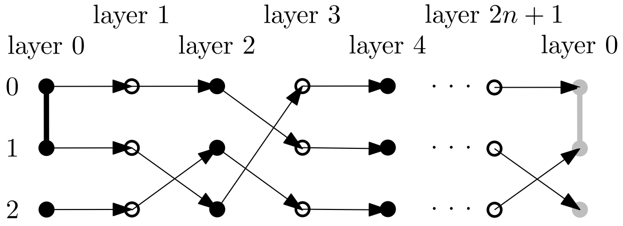

Fig. 2. Reduction from Inner Product to Bipartiteness

4 The Lower Bounds for Inner Product over $\mathbb{Z}_m$

In this section we prove an $\Omega(n\log p(m)-\log m)$ lower bound for $\mathrm{IP}^{01}_{m,n}$, and an $\Omega(n\log(p(m)-1)-\log m)$ lower bound for $\mathrm{IP}^{01*}_{m,n}$. The main idea of the proof is to give an upper bound on the discrepancy of the two problems. This could be done by first upper bounding the discrepancy by the sum of the norms of several matrices formed by applying characters of $\mathbb{Z}_m$ on the communication matrix. Then, we show that the norm of these matrices are nice enough to be computed directly, thus implying a communication lower bound by the relation between discrepancy of the communication matrix and quantum communication complexity. We also show that, by the relation of largest monochromatic rectangle and discrepancy, we can have the same bound for nondeterministic communication complexity. Here we use "excess count", a quantity used in multi-color discrepancy, to bound the binary discrepancy. It is the idea, not the multi-color discrepancy itself, to be used. The reason we use this "excess count" but not to bound binary discrepancy directly is because the distribution we use here is not uniform on the result, but uniform on each non-star entry in the $\mathrm{IP}^{01}_{m,n}$ problem (i.e. the numbers of 0's and 1's in the communication matrix are not the same), thus the binary discrepancy is hard to compute without the help of this quantity. In other words, we are proposing here a hard distribution and a simple way to compute discrepancy under this very distribution for the promised problems $\mathrm{IP}^{01}_{m,n}$and $\mathrm{IP}^{01*}_{m,n}$.

4.1 Preliminaries

Notations. In the next subsections, we denote the multiplicative group of nonzero complex numbers by $\mathbb{C}^\times$. G is always a finite Abelian group (e.g. $\mathbb{Z}_m$). We denote $G_{X\times Y}$ (or $\mathbb{C}_{X\times Y}$) the set of matrices on G (or $\mathbb{C}$) coordinated by $X \times Y$. We use $\langle x, y\rangle$ to denote the inner product over $\mathbb{Z}_m$ for $x, y \in \mathbb{Z}_m^n$.

Group and Representation Theory. We define a *character* of G to be a homomorphism $\chi : G \to \mathbb{C}^\times$. Thus we know that for $a, b \in G$, $\chi(a + b) = \chi(a)\chi(b)$, and clearly that $\chi(a)^m = \chi(ma) = \chi(0) = 1$. So the values of χ are the m-th roots of unity. In particular, if $G = \mathbb{Z}_m$, we have $\chi_i(a) = e^{\frac{2\pi i}{m}\cdot a}$ for $0 \le i < m$ are the characters of $\mathbb{Z}_m$. The *principal character* χ_0 of G is the character such that $\forall a, \chi_0(a) = 1$. The following properties about characters could be found on any algebra book, e.g., [2].

Lemma 1. *The following properties hold for Abelian group G of order m:*

1. *All the characters of G form a group $\hat{G}$, and $\hat{G}$ is an isomorphism of G.*
2. *Assuming the order of χ is d in $\hat{G}$, then we know $\forall a, \chi(da) = \chi(a)^d = \chi_0(a) = 1$.*
3. *For any $\chi \neq \chi_0$, $\sum_{a\in G} \chi(a) = 0$.*
4. *$\overline{\chi(a)} = \chi(-a)$, where $\overline{\chi(a)}$ is the conjugate of $\chi(a)$.*

Matrix Analysis. For an n dimensional vector $x = (x_1, x_2, \ldots, x_n)^T$, we define its ℓ_2-norm $\|x\|_2 = \sqrt{\sum_{k=1}^n x_k^2}$. For a matrix M, we use $M^\dagger$ to denote the conjugate transpose of M. For a function $\chi : G \to \mathbb{C}$ and a matrix $M \in G_{X\times Y}$, we use $\chi(M)$ to denote the matrix formed by $[\chi(M(x, y))]$, which is an element of $\mathbb{C}_{X\times Y}$.

We use the standard definition of spectral norm $\|\cdot\|$ for a matrix M to be $\|M\| = \max_{x\neq 0} \frac{\|Mx\|_2}{\|x\|_2}$, which is the largest singular value of M [11, Theorem 5.6.6].

The Kronecker product (or tensor product) of two matrices $A = [a_{i,j}]$ and B is denoted by $A \otimes B$. It is defined to be the block matrix formed by $[a_{i,j}B]$. It has the following property from [11, Theorem 4.2.12, 4.2.15].

Lemma 2. *Assume that the nonzero singular values of two matrices A and B are $\{\mu_i | 1 \le i \le m\}$ and $\{\lambda_j | 1 \le j \le n\}$ respectively, then the singular values of $A \otimes B$ are $\{\mu_i\lambda_j | 1 \le i \le m, 1 \le j \le n\}$.*

Number Theory. We will use $\varphi(m)$ to denote the Euler function of m, which is defined to be the number of positive integers less than or equal to m that are co-prime to m. For integer $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, we know $\varphi(m) = m \cdot \prod_{i=1}^{k} (1 - 1/p_k)$ from [15, Theorem 7.5].

4.2 The Discrepancy Method

The discrepancy method uses the following discrepency value.

Definition 6 (Discrepancy). *Let $f : X \times Y \mapsto \{0, 1\}$ be a function, R be a rectangle, and μ be a probability distribution on $X \times Y$. Denote* $\mathrm{disc}_\mu(R, f) = |\sum_{(x,y)\in R} \mu(x, y)(-1)^{f(x,y)}|$, *and* $\mathrm{disc}_\mu(f) = \max_R \mathrm{disc}_\mu(R, f)$.

The discrepancy method is widely used in proving communication complexity lower bound [4,19,13], with many applications. It was also used to prove the quantum lower bound [12,16], as in the following lemma.

Lemma 3. *[12, Theorem 6] For any function f and any distribution μ, we have*

$$Q_\epsilon^*(f) = \Omega\left(\log \frac{1 - 2\epsilon}{\mathrm{disc}_\mu(f)}\right).$$

In the case of the communication complexity problem with promise, the discrepancy method still works if $\mu(x, y) = 0$ on (x, y) which is not in the promise.

We can use discrepancy to lower bound the quantum communication complexity. Similarly, we can use the weight of the largest monochromatic rectangle to give lower bound for nondeterministic communication complexity. For $b \in \{0, 1\}$, we define $\mathrm{mono}_\mu^b(f) = \max_{S\times T\subseteq X\times Y} \left\{\mu(S \times T) \middle| S \times T \subseteq f^{-1}(b)\right\}$. It is easy to see $\mathrm{mono}_\mu^b(f) \le \mathrm{disc}_\mu(f)$. Thus by [13, Proposition 2.15], we have the following lemma.

Lemma 4. *[13, Proposition 2.15] For any $b \in \{0, 1\}$ and any distribution μ on $X \times Y$, we have the nondeterministic communication complexity of f satisfies*

$$N^b(f) \ge \log_2 \frac{\mu(f^{-1}(b))}{\mathrm{mono}_\mu^b(f)} \ge \log_2 \frac{\mu(f^{-1}(b))}{\mathrm{disc}_\mu(f)}.$$

Since $\mathrm{mono}_\mu^b(f) \le \mathrm{disc}_\mu(f)$, we can use discrepancy to bound nondeterministic communication complexity as well.

Some tools from discrepancy on non-binary functions are also imported in this paper. The following concept of *excess count* has been used in [3] to give the definition of strong multi-color discrepancy, which could be used to give randomized communication complexity lower bounds for multi-valued functions.

Definition 7 (Excess Count). *Let $M \in G_{X\times Y}$ be a matrix. We define the* excess count *for an element $g \in G$ in a rectangle $S \times T \subseteq X \times Y$ as*

$$\mathrm{excess}_M(g, S \times T) = \left|\{(x, y) \in S \times T | M(x, y) = g\}\right| - \frac{|S||T|}{|G|}.$$

The excess count for an element g is defined as the maximum value among all possible rectangles $S \times T$,

$$\mathrm{excess}_M(g) = \max_{S\times T \subseteq X \times Y} \mathrm{excess}_M(g, S \times T).$$

Furthermore, the strong multi-color discrepancy is upper bounded by another value called weak multi-color discrepancy. The relationship between strong and weak multi-color discrepancy could be expressed in terms of excess count in the following lemma. Note that we are not going to define or use multi-color discrepancy in this paper. Instead, the lemma using "excess count" is enough for us.

By [3, Lemma 2.9] and $\left|\sum_{(x,y)\in S\times T} \chi(M(x,y))\right| \le \|\mathbf{1_S}\|_2 \cdot \|\chi(M)\| \cdot \|\mathbf{1_T}\|_2$, we can deduce the following lemma.

Lemma 5. *For matrix $M \in G_{X\times Y}$, we have*

$$\max_{g\in G}\{\mathrm{excess}_M(g)\} \le \frac{\sqrt{|X||Y|}}{|G|} \sum_{\substack{\chi\in\hat{G}\\ \chi\neq\chi_0}} \|\chi(M)\|.$$

4.3 Lower Bound for $\mathrm{IP}^{01}_{m,n}$ and $\mathrm{IP}^{01*}_{m,n}$

We define matrices $\Phi \in (\mathbb{Z}_m)_{m^n\times m^n}$ by $\Phi(x,y) = \langle x, y\rangle$ and $\Phi^* \in (\mathbb{Z}_m)_{m^n\times\varphi(m)^n}$ by $\Phi^*(x,y^*) = \langle x, y^*\rangle$ to be the communication matrices of $\mathrm{IP}_{m,n}$ on $\mathbb{Z}_m^n \times \mathbb{Z}_m^n$ and $\mathbb{Z}_m^n \times (\mathbb{Z}_m^*)^n$, respectively, where $x, y \in \mathbb{Z}_m^n$ and $y^* \in (\mathbb{Z}_m^*)^n$.

We first state the lemmas we need to get a lower bound of $\mathrm{IP}^{01}_{m,n}$ and $\mathrm{IP}^{01*}_{m,n}$ with the proof delayed to the full version of the paper.

Lemma 6. *Let $\chi \in \widehat{\mathbb{Z}_m}$, $\chi \neq \chi_0$ be an order d character of $\mathbb{Z}_m$, we have*

$$\|\chi(\Phi)\| = \left(\frac{m^2}{d}\right)^{n/2} \text{ and } \|\chi(\Phi^*)\| = \left(m \cdot \frac{\varphi(m)}{\varphi(d)}\right)^{n/2}.$$

Lemma 7. *In Φ, the number of 0's is at least m^{2n-1} and the number of 1's is at least $\varphi(m)\cdot m^{2n-2}$. In Φ^*, the number of k's is $m^{n-1}\cdot\varphi(m)^n$ for $k = 0, 1, \ldots, m-1$.*

By combining the above lemmas with Lemma 5, we have the following theorem.

Theorem 4 (Theorem 2 Restated). *For any $b \in \{0,1\}$, the quantum/ nondeterministic communication complexity of $\mathrm{IP}^{01}_{m,n}$ and $\mathrm{IP}^{01*}_{m,n}$ satisfy*

$$Q^*_{1/3}(\mathrm{IP}^{01}_{m,n}) = \Omega(n\log p(m) - \log m), \quad Q^*_{1/3}(\mathrm{IP}^{01*}_{m,n}) = \Omega(n\log(p(m)-1) - \log m)$$
$$N^b(\mathrm{IP}^{01}_{m,n}) = \Omega(n\log p(m) - \log m), \quad N^b(\mathrm{IP}^{01*}_{m,n}) = \Omega(n\log(p(m)-1) - \log m).$$

Proof. Let μ be the distribution uniformly distributed on the coordinates $(x,y) \in \mathbb{Z}_m^n \times \mathbb{Z}_m^n$ where $\langle x,y\rangle \in \{0,1\}$, and let μ^* be the distribution uniformly distributed on the coordinates $(x,y^*) \in \mathbb{Z}_m^n \times (\mathbb{Z}_m^*)^n$ where $\langle x,y^*\rangle \in \{0,1\}$. We are going to give upper bounds for $\mathrm{disc}_\mu(\mathrm{IP}_{m,n}^{01})$ and $\mathrm{disc}_{\mu^*}(\mathrm{IP}_{m,n}^{01*})$ to obtain lower bounds for their communication complexity.

We know $\mu(x,y) = \alpha$ is the same for all (x,y) satisfying $\langle x,y\rangle \in \{0,1\}$. So we can bound the discrepancy of $\mathrm{IP}_{m,n}^{01}$ by the excess of Φ in the following way:

$$\begin{aligned}
\mathrm{disc}_\mu(\mathrm{IP}_{m,n}^{01}) &= \max_{S\times T\subseteq X\times Y} \mathrm{disc}_\mu(\mathrm{IP}_{m,n}^{01}, S\times T)\\
&= \max_{S\times T\subseteq X\times Y} \left| \sum_{(x,y)\in S\times T} \mu(x,y)\cdot(-1)^{\Phi(x,y)} \right|\\
&= \max_{S\times T\subseteq X\times Y} \alpha\cdot \big|\, |\{(x,y)|\Phi(x,y)=0\}| - |\{(x,y)|\Phi(x,y)=1\}|\,\big|\\
&= \max_{S\times T\subseteq X\times Y} \alpha\,|\mathrm{excess}_\Phi(0,S\times T) - \mathrm{excess}_\Phi(1,S\times T)|\\
&\le \alpha\cdot \max_{S\times T\subseteq X\times Y} 2\max_{g\in\mathbb{Z}_m} |\mathrm{excess}_\Phi(g,S\times T)| \quad \text{(Triangle Inequality)}\\
&\le \alpha\cdot \frac{2\sqrt{m^n\cdot m^n}}{m} \sum_{\substack{\chi\in\widehat{\mathbb{Z}_m}\\ \chi\ne\chi_0}} \|\chi(\Phi)\|. \qquad \text{(Lemma 5)}
\end{aligned}$$

By Lemma 6 we know that for χ with order d the norm of $\chi(\Phi)$ is $\left(\frac{m^2}{d}\right)^{n/2}$. Since d is an order and $\chi \ne \chi_0$ we know $d|m$ and $d \ne 1$. So we have the norm of $\chi(\Phi)$ is $\left(\frac{m^2}{d}\right)^{n/2} \le \left(\frac{m^2}{p(m)}\right)^{n/2}$. By Lemma 7 we know that $\alpha \le 1/m^{2n-1}$, thus

$$\mathrm{disc}_\mu(\mathrm{IP}_{m,n}^{01}) \le \alpha\cdot 2m^{n-1}\cdot(m-1)\left(\frac{m^2}{p(m)}\right)^{n/2} \le \frac{2m}{p(m)^{n/2}}.$$

By Lemma 3,

$$Q_\epsilon^*(\mathrm{IP}_{m,n}^{01}) \ge \log\frac{1-2\epsilon}{\mathrm{disc}_\mu(\mathrm{IP}_{m,n}^{01})} = \Omega(n\log p(m) - \log m + \log(1-2\epsilon)).$$

For $\mathrm{IP}_{m,n}^{01*}$, we can also bound $\mathrm{disc}_{\mu^*}(\mathrm{IP}_{m,n}^{01*})$ by $\chi(\Phi^*)$ in the same way, yielding

$$\mathrm{disc}_{\mu^*}(\mathrm{IP}_{m,n}^{01*}) \le 2m(\varphi(p(m)))^{-n/2},$$

which in turn means

$$Q_\epsilon^*(\mathrm{IP}_{m,n}^{01*}) \ge \log\frac{1-2\epsilon}{\mathrm{disc}_\mu(\mathrm{IP}_{m,n}^{01*})} = \Omega(n\log(p(m)-1) - \log m + \log(1-2\epsilon)).$$

For nondeterministic lower bound, Lemma 7 claims that the number of 0's and the number of 1's in Φ^* is the same, implying $\mu^*({\mathrm{IP}_{m,n}^{01*}}^{-1}(0)) = \mu^*({\mathrm{IP}_{m,n}^{01*}}^{-1}(1)) = 1/2$.

Moreover, the number of 0's and 1's in $\varPhi$ are at least m^{2n-1} and $\varphi(m)m^{2n-2}$, respectively. So we have

$$\mu({\mathrm{IP}^{01}_{m,n}}^{-1}(0)) \geq m^{2n-1}/m^{2n} = 1/m$$
$$\mu({\mathrm{IP}^{01}_{m,n}}^{-1}(1)) \geq \varphi(m)m^{2n-2}/m^{2n} = \varphi(m)/m^2.$$

Substituting the above equality into Lemma 4, one can easily check we have finished the proof.

References

1. Alon, N., Matias, Y., Szegedy, M.: The space complexity of approximating the frequency moments. Journal of Computer and System Sciences 58, 137–147 (1999)
2. Babai, L.: The Fourier transform and equations over finite abelian groups. Lecture Notes, version 1.3 1 (2002)
3. Babai, L., Hayes, T., Kimmel, P.: The cost of the missing bit: Communication complexity with help. Combinatorica 21(4), 455–488 (2001)
4. Babai, L., Frankl, P., Simon, J.: Complexity classes in communication complexity theory. In: Symposium on Foundations of Computer Science, pp. 337–347 (1986)
5. Bar-Yossef, Z., Kumar, R., Sivakumar, D.: Reductions in streaming algorithms, with an application to counting triangles in graphs. In: Symposium on Discrete Algorithms, pp. 623–632 (2002)
6. Chu, J.I., Schnitger, G.: Communication complexity of matrix computation over finite fields. Theory of Computing Systems 28, 215–228 (1995)
7. Feigenbaum, J., Kannan, S., McGregor, A., Suri, S., Zhang, J.: Graph distances in the streaming model: the value of space. In: Symposium on Discrete Algorithms, pp. 745–754 (2005)
8. Feigenbaum, J., Kannan, S., McGregor, A., Suri, S., Zhang, J.: On graph problems in a semi-streaming model. Theoretical Computer Science 348(2-3), 207–216 (2005)
9. Hajnal, A., Maass, W., Turán, G.: On the communication complexity of graph properties. In: Symposium on Theory of Computing, pp. 186–191 (1988)
10. Harvey, N.J.A.: Matroid intersection, pointer chasing, and young's seminormal representation of s_n. In: Symposium on Discrete Algorithms, pp. 542–549 (2008)
11. Horn, R., Johnson, C.: Matrix analysis, vol. 2. Cambridge University Press (1990)
12. Kremer, I.: Quantum Communication. Master's thesis, The Hebrew University of Jerusalem (1995)
13. Kushilevitz, E., Nisan, N.: Communication Complexity. Cambridge University Press (1997)
14. Raz, R., Spieker, B.: On the "log rank"-conjecture in communication complexity. Combinatorica 15, 567–588 (1995)
15. Rosen, K.H.: Elementary Number Theory and Its Applications, 3rd edn. Addison-Wesley (1992)
16. Sherstov, A.A.: The pattern matrix method for lower bounds on quantum communication. In: Symposium on Theory of Computing, pp. 85–94. ACM (2008)
17. Verbin, E., Yu, W.: The Streaming Complexity of Cycle Counting, Sorting By Reversals, and Other Problems. In: Symposium on Discrete Algorithms (2011)
18. Yao, A.C.C.: Some complexity questions related to distributive computing. In: Symposium on Theory of Computing, pp. 209–213 (1979)
19. Yao, A.C.C.: Lower bounds by probabilistic arguments. In: Symposium on Foundations of Computer Science, pp. 420–428 (1983)