Communication complexity of entanglement assisted multi-party computation

Ruoyu Meng* and Aditya Ramamoorthy†
Iowa State University, Ames, IA 50011, USA

(Dated: May 9, 2023)

We consider a quantum and classical version multi-party function computation problem with n players, where players $2, \ldots, n$ need to communicate appropriate information to player 1, so that a "generalized" inner product function with an appropriate promise can be calculated. The communication complexity of a protocol is the total number of bits that need to be communicated. When n is prime and for our chosen function, we exhibit a quantum protocol (with complexity $(n-1)\log n$ bits) and a classical protocol (with complexity $(n-1)^2(\log n^2)$ bits). In the quantum protocol, the players have access to entangled qudits but the communication is still classical. Furthermore, we present an integer linear programming formulation for determining a lower bound on the classical communication complexity. This demonstrates that our quantum protocol is strictly better than classical protocols.

I. INTRODUCTION

We consider a multi-party function computation scenario in this work. There are a total of n players in the system numbered $1, 2, \ldots, n$. Each player observes her input and players $2, \ldots, n$ (remote parties) communicate an appropriate number of bits that allows player 1 to finally compute the value of the function. Clearly, this can be accomplished if players $2, \ldots, n$ communicate their actual values but in fact in many cases, the function value can be computed with much lesser information. Thus, a natural question is to understand the minimum number of bits the remote parties need to send to player 1.

Such problems are broadly studied under the umbrella of communication complexity [1, 2] in the literature. In this work we consider the zero-error version of this problem. Our main goal is to understand the advantage that the availability of quantum entanglement confers on this problem and comparing it with classical protocols. Such problems have a long history in the literature [3, 4].

Background: Within quantum communication complexity (QCC) problems, there are three kinds of quantum protocols. In the first kind (introduced by Yao [2]) each player communicates via a quantum channel and the metric is the number of qubits transmitted. The second variation assumes that each player can use entanglement as a free resource but the communication is classical; the metric is the number of classical bits transmitted. It was introduced by Cleve and Buhrman [5]. The third kind is a combination of the first two. It allows free usage of entanglement and works with quantum communication. The work of de Wolf [6] shows that, in the two party case, the latter scenario can be reduced to the first scenario with a factor of two penalty using teleportation [7].

Buhrman, Cleve, Wigderson [8] and Cleve, van Dam, Nielsen and Tapp [9] considered the case of the two party function with quantum communication and used reduction techniques to connect problems in QCC to other known problems and derived upper/lower bounds for QCC in this manner. In particular, the second work showed examples, such as set disjointness function, where quantum protocols are strictly better than classical ones. Here, the set-disjointness problem is such that each player has a set and wants to decide if their intersection is empty. Buhrman and de Wolf [10] generalized the two-party "log rank" lower bound of classical communication complexity to QCC where quantum protocols use both shared entanglement and quantum communication. For other two-party upper/lower bound techniques, see [11–15].

Related Work: Now we discuss works in multiparty quantum communication complexity. There are mainly two kinds of models. The number-in-hand (NIH) model assumes each player observes only one variable. The number-on-forehead (NOF) model assumes each player observes all but one variable. François and Shogo[16] considered the NIH model with quantum communication and gave a quantum protocol for a three-party triangle-finding problem; the formulation considers bounded error. This has polynomial advantage with respect to any classical protocol. Here, the triangle-finding problem is such that the edge set of a graph is distributed over each user and the task is to find a triangle of the graph.

The results in next two works hold for both NIH and NOF models. Lee and Schechtman and Shraibman [17] proved a Grothendieck-type inequality and then derived a general lower bound of the multiparty QCC for Boolean function in Yao's model. Following this work, Briet, Buhrman, Lee, Vidick [18] showed a similar inequality of the multiparty XOR game and proved that the discrepancy method lower bounds QCC when the protocol is of the third kind discussed earlier.

Buhrman, van Dam, Høyer, Tapp [19] considered the NIH model with shared entanglement and proposed a three-party problem with a quantum protocol that is better than any classical protocol by a constant factor. Following this work, Xue, Li, Zhang, Guo [20] and Galvão [21] showed similar results under the same function with

* rmeng@iastate.edu
† adityar@iastate.edu

more restrictions. The work most closely related to our work is by Cleve and Buhrman [5]. This paper considered the case of three players denoted Alice, Bob and Carol who have m-bit strings denoted $\vec{x}, \vec{y}$ and $\vec{z}$ respectively. The strings are such that $\vec{x} + \vec{y} + \vec{z} = \mathbb{1}$, i.e., their binary sum is the all-ones vector. The goal is for Alice to compute

$$g(x, y, z) = \sum_{i=}^{m} x_i y_i z_i.$$

We note that the communication from Bob and Carol to Alice is purely classical; however, they can use entanglement in a judicious manner. For this particular function [5] shows that a classical protocol (without entanglement) requires three bits of communication, whereas if the parties share $3m$ entangled qubits, then two bits of communication are sufficient.

Main Contributions: In this work we consider a significant generalization of the original work of [5]. In particular, we consider a scenario with n players that observe values that lie in a higher-order finite field, with a more general promise that is satisfied by the observed values. As we consider more players and higher-order finite fields, the techniques used in the original work are not directly applicable in our setting.

Our work makes the following contributions.

- We demonstrate a quantum protocol that allows for the function to be computed with $(n-1)\log n$ bits. We use the quantum Fourier Transform as a key ingredient in our method.
- On the other hand, we demonstrate a classical protocol that requires the communication of $(n-1)^2(\log n^2)$ bits.
- For obtaining a lower bound on the classical communication complexity, we define an appropriate integer linear programming problem that demonstrates that our quantum protocol is strictly better than any classical protocol.

This paper is organized as follows. Section II discusses the problem formulation and Section III discusses our quantum protocol. Sections IV and V discuss our classical protocol and the lower bound on any classical protocol respectively.

II. PROBLEM FORMULATION

A. Classical/Quantum Communication Scenarios

Let $\mathcal{X}_i, i = 1, \dots, n$ and $\mathcal{Y}$ denote sets in which the inputs and the output lie and $f(x_, \dots, x_n) : \mathcal{X}_1 \times \dots \times \mathcal{X}_n \mapsto \mathcal{Y}$ be a multivariate function. There are n players such that i-th player is given $x_i \in \mathcal{X}_i$. The first player (henceforth, Alice) receives information from each of the players and this communication should allow her to compute $f(x_1, \dots, x_n)$. The players are not allowed to communicate with each other.

In the classical protocol, players 2 to n communicate to Alice via classical channels. In the quantum protocol, we assume that the users have shared entanglement as a free resource; however, the communication is still classical. In both scenarios the classical/quantum communication complexity is the least possible number of classical bits transmitted such that Alice can compute the function among all classical/quantum protocols.

B. Generalized Inner Product Function with a Promise

In this work we consider a specific multivariate function and the setting where $n \geq 3$ (number of players) is prime. Let $\mathbb{F}_n$ denote the finite field of order-n and $[m] \triangleq \{1, \dots, m\}$. The i-th player is given a vector $\vec{x}^i = [x_1^i \dots x_m^i]^T \in \mathbb{F}_n^m$, i.e., each $x_j^i \in \mathbb{F}_n$. The vectors satisfy the following "promise": $\forall j \in [m]$, the j-th component of each player's vector is such that

$$[x_j^1, \dots, x_j^n]^T \in \{a[1, \dots, 1]^T + b[0, \dots, n-1]^T \mid a, b \in \mathbb{F}_n\},$$

i.e., $[x_j^1, \dots, x_j^n]^T$ lies in a two-dimensional vector space spanned by the basis vectors $[1, \dots, 1]^T$ and $[0, 1, \dots, n-1]^T$. In this case, it can be observed that $[x_j^1, \dots, x_j^n]^T$ is either a multiple of the all-ones vector (if $b = 0$) or a permutation of $[0, 1, \dots, n-1]$ (if $b \neq 0$). The function to be computed is the generalized inner product function given by

$$GIP(\vec{x}^1, \dots, \vec{x}^n) = \sum_{i=1}^{m} \left(\prod_{j=1}^{n} x_i^j \right), \tag{1}$$

where the operations are over $\mathbb{F}_n$.

III. PROPOSED QUANTUM PROTOCOL

We first discuss the entangled states and unitary transforms will be used in the proposed quantum protocol in Section III A. In Section III B, we discuss the quantum protocol with a proof of correctness in detail. A word about notation. In what follows for complex vectors $\vec{u}, \vec{v}$, $\langle \vec{u}, \vec{v} \rangle = \sum_i u_i^\dagger v_i$ denotes the usual inner product. On the other hand if $\vec{u}, \vec{v} \in \mathbb{F}_n^m$, then $\langle \vec{u}, \vec{v} \rangle$ denotes the inner product over $\mathbb{F}_n$.

A. Entanglement Resource and Unitary Transforms Used

a. Shared Entangled States. Consider n isomorphic n-dimensional quantum systems, where each system has a computational basis denoted $\mathcal{B}$ =

Algorithm 1: Proposed Quantum protocol

For $i \in \{1, \dots, m\}$, prepare maximally entangled "shared state" $|\Phi_i\rangle$ and distributed corresponding subsystems to all players.
for player $p \in \{1, \dots n\}$ **do**
  for each $i \in \{1, \dots, m\}$ **do**
    Assume $x_i^p = j$, then player p applies P_j (*cf.* (3)) on her part of $|\Phi_i\rangle$.
    Player p performs QFT on her part of the shared state.
    Player p measures her part of the shared state in the computational basis, yielding $s_i^p \in \mathbb{F}_n$
  end for
  $s^p \leftarrow \sum_{i=1}^m s_i^p$
  Player p sends s^p to Alice if $p \neq 1$
end for
$GIP(\vec{x}^1, \dots, \vec{x}^n) = \sum_p s^p$.

$\{|0\rangle, |1\rangle, \dots, |n-1\rangle\}$. There are m entangled states shared among n players. For $i \in [m]$, prepare entangled state $|\Phi_i\rangle := 1/\sqrt{n}\sum_{k=0}^{n-1} |k \dots k\rangle$. The j-th subsystem of this entangled state is given to j-th player for $j = 1, \dots, n$.

b. Quantum Fourier Transform. Let $\omega := e^{\frac{2\pi \mathrm{i}}{n}}$ denote the n-th root of unity. The Quantum Fourier Transform (QFT) is the following unitary map that takes

$$|j\rangle \mapsto \frac{1}{\sqrt{n}}\sum_{k=0}^{n-1} \omega^{jk} |k\rangle\,, \ \forall |j\rangle \in \mathcal{B}. \tag{2}$$

Let $QFT^{\otimes l}$ denote the QFT performed over l isomorphic systems.

c. Phase Shift Map. For $j \in \mathbb{F}_n$, we define

$$P_0 \triangleq \begin{cases} |0\rangle \mapsto \omega^{-\frac{n-1}{2}} |0\rangle \\ |i\rangle \mapsto |i\rangle\,, i \neq 0. \end{cases}$$

$$\text{If } j \neq 0,\ P_j \triangleq |i\rangle \mapsto \omega^{-\frac{1}{n}(ij \bmod n)} |i\rangle\,. \tag{3}$$

B. The Quantum Protocol

Next, we introduce the quantum protocol that uses $(n-1)(\log n)$ bits.

Theorem 1. *There exists a quantum protocol for computing $GIP(\vec{x}^1, \dots, \vec{x}^n)$ that uses $(n-1)\log n$ bits.*

In our protocol (see Alg. 1), for each $i = 1, \dots, m$, each player p examines x_i^p and applies the corresponding phase shift map to her subsystem of $|\Phi_i\rangle$. Following this, she applies the QFT on each of her symbols and then measures in the computational basis; this yields $s_i^p \in \mathbb{F}_n$ for $i = 1, \dots, m$. Player p transmits $\sum_{i=1}^m s_i^p$. As players $2 \leq p \leq n$ transmit a symbol from $\mathbb{F}_n$, it is clear that the total communication in the protocol is $(n-1)(\log n)$.

For showing the proof of correctness of the protocol, we need the following auxiliary lemma. The proof appears in Appendix A.

Lemma 1. *Let $\vec{\alpha} = [1, \dots, 1]^T \in \mathbb{F}_n^n$. Then, for each $x \in \mathbb{F}_n$, we have*

$$QFT^{\otimes n}\left(\frac{1}{\sqrt{n}}\sum_{j=0}^{n-1} \omega^{-jx} |j \cdot \vec{\alpha}\rangle\right) = \frac{1}{n^{\frac{n}{2}}} \sum_{\vec{k} \in \{0,\dots,n-1\}^n} a_{\vec{k}} |\vec{k}\rangle\,. \tag{4}$$

Then the amplitude $a_{\vec{k}} \neq 0$ iff $\sum_{j=1}^n k_j = x$ where $\vec{k} = [k_1, \dots, k_n]^T$.

The proof of correctness of the protocol hinges on the following lemma.

Lemma 2.

$$\sum_{p=1}^n s_i^p = \prod_{p=1}^n x_i^p, \mathit{for}\ i = 1, \dots, m. \tag{5}$$

Proof. The state jointly measured by each player is

$$QFT^{\otimes n}\left(\sum_{j=0}^{n-1}\left(\otimes_{p=1}^n P_{x_i^p}\right)\frac{1}{\sqrt{n}} |j \cdot \vec{\alpha}\rangle\right).$$

If $[x_i^1, \dots, x_i^n]^T = [j, \dots, j]^T$, then (see Appendix B for derivation)

$$P_j^{\otimes n}\left(\frac{1}{\sqrt{n}}\sum_{k=0}^{n-1} |k \cdot \vec{\alpha}\rangle\right) \mapsto \frac{1}{\sqrt{n}}\sum_{k=0}^{n-1} \omega^{-kj} |k \cdot \vec{\alpha}\rangle\,. \tag{6}$$

Thus, $QFT^{\otimes n}(\frac{1}{\sqrt{n}}\sum_{k=0}^{n-1} \omega^{-kj} |k \cdot \vec{\alpha}\rangle)$ has non-zero coefficients only for states $|\vec{k}\rangle$ such that $\sum_{l=1}^n k_l = j$ by **Lemma 1**. Therefore, the measurement result $[s_i^1, \dots, s_i^n]^T$ must be one of $\vec{k} = [k_1, \dots, k_n]^T$ s.t.

$$\sum_{l=1}^n k_l = j \overset{(a)}{=} j^n = \prod_{p=1}^n x_i^p$$

where (a) follows from the fact that $j \in \mathbb{F}_n$.

Now assume $[x_j^1, \dots, x_j^n]^T = a[1, \dots, 1]^T + b[0, 1, \dots, n-1]^T$ with $b \neq 0$. We have that (see Appendix B for derivation)

$$P_0 \otimes \dots \otimes P_{n-1}\left(\frac{1}{\sqrt{n}}\sum_{k=0}^{n-1} |k \cdot \vec{\alpha}\rangle\right) \mapsto \frac{1}{\sqrt{n}}\omega^{-\frac{n-1}{2}}\sum_{k=0}^{n-1} |k \cdot \vec{\alpha}\rangle \tag{7}$$

It follows that

$$\begin{aligned} &QFT^{\otimes n}(\frac{1}{\sqrt{n}}\omega^{-\frac{n-1}{2}}\sum_{k=0}^{n-1} |k \cdot \vec{\alpha}\rangle) \\ =&\omega^{-\frac{n-1}{2}} QFT^{\otimes n}(\frac{1}{\sqrt{n}}\sum_{k=0}^{n-1} |k \cdot \vec{\alpha}\rangle) = \frac{1}{n^{\frac{n}{2}}}\omega^{-\frac{n-1}{2}} \sum_{\vec{k} \in \mathbb{F}_n^n} a_{\vec{k}} |\vec{k}\rangle\,. \end{aligned}$$

By **Lemma 1**, $a_{\vec{k}} \neq 0$ iff $\sum_{l=1}^{n} k_l = 0$. Therefore, the measurement result $[s_i^1, \ldots, s_i^n]^T$ must be $\vec{k} = [k_1, \ldots, k_n]^T$ such that

$$\sum_{l=1}^{n} k_l = 0 = \prod_{j=0}^{n-1} j = \prod_{p=1}^{n} x_i^p.$$

$\square$

Now, we show that our protocol computes $GIP(\vec{x}^1, \ldots, \vec{x}^n)$ correctly. Since $s^p = \sum_i s_i^p$, by applying (5), we have that

$$\sum_p s^p = \sum_p \sum_i s_i^p = \sum_i \sum_p s_i^p = \sum_i \prod_{p=1}^{n} x_i^p = GIP(\vec{x}^1, \ldots, \vec{x}^n).$$

IV. PROPOSED CLASSICAL PROTOCOL

We now move on to considering purely classical protocols for our problem, i.e., ones that do not consider entanglement. At the top-level our classical scheme operates by communicating the "number" of different symbols that exist in within each player's vector. We show that this suffices for Alice to recover the function value.

More precisely, let β_k^p be the number of "k" values in the vector of p-th player; recall that player p is assigned $\vec{x}_p = x_1^p \ldots x_m^p$. Note $\sum_{k=0}^{n-1} \beta_k^p = m$.

Theorem 2. *There exists a classical protocol for computing $GIP(\vec{x}^1, \ldots, \vec{x}^n)$ that uses $(n-1)^2(logn^2)$ bits.*

In our protocol (see Alg. 2), for each $i = 1, \ldots, n-1$, each player p transmits $\beta_k^p \pmod{n^2}$. Alice computes each $\beta_0^p \pmod{n^2}$ by using the fact that $\sum_{k=0}^{n-1} \beta_k^p = m$. Finally, Alice computes the value of the function by using $\{\beta_k^p \pmod{n^2} | k \in \mathbb{F}_n, p \in [n]\}$ For each player $p \in \{2, \ldots, n\}$, p transmits $\{\beta_1^p \pmod{n^2}, \ldots, \beta_{n-1}^p \pmod{n^2}\}$. The total number of bits transmitted is $(n-1)^2(\log n^2)$. The proof of the Theorem 2 appears in Appendix C.

Algorithm 2: Proposed Classical protocol

```
for player p ∈ {1, ... n} do
    for each k ∈ F_n do
        β_k^p ← number of ks in x_1^p ... x_m^p
        if p is not Alice and k ≠ 0 then
            p sends β_k^p (mod n^2) to Alice
        end if
    end for
end for
for p ∈ {2, ... n} do
    Alice computes β_0^p (mod n^2) by using
    Σ_{k=0}^{n-1} β_k^p = m.
end for
W ←
Σ_{p=1}^{n} Σ_{k=1}^{n-1} k · β_k^p + ((n^2 − n)/2)(n − 1) Σ_{p=1}^{n} β_0^p (mod n^2)
GIP(x^1, ..., x^n) = W/n
```

V. CLASSICAL COMMUNICATION COMPLEXITY LOWER BOUND

A. ILP Feasibility Problem for Classical Lower Bound

We now present a lower bound on the communication complexity of any classical protocol for our problem. Towards this end we pose this as an integer linear programming problem that can be solved numerically.

Suppose, for $p \in \{2, \ldots, n\}$, the p-th player sends symbols (labels) in $[l^p] := \{1, 2, \ldots, l^p\}$ for some large enough positive integer l^p. Let $c \in [l^p]$ and define $I_{\vec{x}^p, c} \in \{0, 1\}$ to be the indicator that the p-th player sends c when it has the vector $\vec{x}^p \in \mathbb{F}_n^m$. As this mapping is unique, we have $\sum_{c \in [l^p]} I_{\vec{x}^p, c} = 1$. Furthermore, for a given set of vectors $\vec{x}^p$ for $p \in \{2, \ldots, n\}$ if the p-th player sends label c^p, we have $\prod_{p=2}^{n} I_{\vec{x}^p, c^p} = 1$.

Consider two sets of vectors $\{\vec{x}^p \in \mathbb{F}_n^m | p \in \{1, \ldots, n\}\}$, $\{\vec{z}^p \in \mathbb{F}_n^m | p \in \{1, \ldots, n\}\}$. We denote

$$(\vec{x}^1, \ldots, \vec{x}^n) \sim_{GIP} (\vec{z}^1, \ldots, \vec{z}^n)$$

if the following conditions are satisfied.

1. Both $(\vec{x}^1, \ldots, \vec{x}^n)$ and $(\vec{z}^1, \ldots, \vec{z}^n)$ satisfy the promise (*cf.* Sec. II B).
2. $\vec{x}^1 = \vec{z}^1$.
3. $GIP(\vec{x}^1, \ldots, \vec{x}^n) \neq GIP(\vec{z}^1, \ldots, \vec{z}^n)$.

This definition applies to distinct inputs with the "same" Alice vector, but different function evaluations. It can be seen that for two such distinct inputs, the symbols communicated by players 2 to n have to be distinct, otherwise Alice has no way to decode in a zero-error fashion.

Our proposed ILP works with fixed l^p's and a fixed value of m. Owing to complexity reasons m cannot be very large. However, we point out that if the ILP is infeasible for given l^p's and a $\tilde{m}$, then our lower bound holds for arbitrary values $m \geq \tilde{m}$. To see this we note that our lower bound would continue to hold even if Alice was provided the values $x_{\tilde{m}+1}^p, \ldots, x_m^p$ for all players $p = 2, \ldots, n$.

Consider the following $0-1$ integer programming feasibility problem.

$$\begin{aligned} &\min \quad 0 \\ \text{s.t.} \quad & p \in \{2,\ldots,n\}, c \in [l^p], \vec{x}^p \in \mathbb{F}_n^m, \\ & I_{\vec{x}^p,c} \in \{0,1\}, \\ & \sum_{c\in[l^p]} I_{\vec{x}^p,c} = 1,\ \forall\ \vec{x}^p, \\ \sum_{c^2\in[l^2],\ldots,c^n\in[l^n]} & |\prod_{p=2}^n I_{\vec{x}^p,c^p} - \prod_{p=2}^n I_{\vec{z}^p,c^p}| = 2 \\ & \text{for all } (\vec{x}^1,\ldots,\vec{x}^n) \sim_{GIP} (\vec{z}^1,\ldots,\vec{z}^n). \end{aligned} \tag{8}$$

The infeasibility of the above integer programming problem corresponds to a lower bound on the classical communication complexity. The proof of the following theorem appears in Appendix D.

Theorem 3. *There exists a deterministic classical protocol computing $GIP(\cdot)$ where each player sends at most l^p different labels for $p \in \{2,\ldots,n\}$ iff the above integer programming is feasible.*

Remark 1. *The above integer program contains constraints that involve the product of variables and equality constraints with sums of absolute values. We show how these constraints can be linearized in Appendix E. The entire code for our ILP is available at this online repository [22].*

B. Numerical experiments

In our numerical experiments, we considered an instance of the ILP involving $n = 3$ players, namely Alice, Bob, and Carol. Let m represent the length of each vector, while $[l^b], [l^c]$ denote the sets of labels used by Bob and Carol, with l^b, l^c as the sizes of these sets. The experimental results under varying settings of l^b, l^c, m are displayed in TABLE I.

In the case where $n = 3$, we assume that Alice, Bob, and Carol are given vectors $\vec{x}^1$, $\vec{x}^2$, and $\vec{x}^3$, respectively, each of length m. The promise (*cf.* Sec. II B) is equivalent to

$$\vec{x}^1_j + \vec{x}^2_j + \vec{x}^3_j = 0, j = 1,\ldots,m.$$

It can be observed that swapping the vectors of Bob and Carol continues to satisfy the promise. Due to this inherent symmetry, a protocol with communication lengths $l^b = x$ and $l^c = y$ exhibits the same feasibility as one with $l^b = y$ and $l^c = x$. Consequently, we can assume that $l^b \leq l^c$.

TABLE I. Numerical results.

m	l^b	l^c	Feasibility
1	1	3	Feasible
3	1	17	Infeasible
2	2	4	Infeasible
3	3	3	Infeasible
2	2	4	Feasible
3	5	5	Feasible

If a classical protocol exists with $l^b \geq 4$, it follows that $l^c \geq 4$. The number of bits transmitted would then be $\log(l^b) + \log(l^c) \geq 2\log(4)$.

Assuming a classical protocol with $l^b = 1$, and given the infeasibility of the second result, i.e. the case $l^b = 1, l^c = 17$, in TABLE I, it must hold that $l^c \geq 18$. The number of bits transmitted would then be at least $\log(l^b) + \log(l^c) \geq \log(1) + \log(18)$. The ILP is infeasible for the cases $l^b = 2, l^c = 4$ and $l^b = 3, l^c = 3$. For the same reason, a protocol with $l^b = 2$ or $l^b = 3$ necessitates at least $\log(2) + \log(5)$ or $\log(3) + \log(4)$ bits of communication, respectively.

Recalling that our proposed protocol employs $2\log(3)$ bits of communication, we have that

$$\begin{aligned} 2\log(3) < \min\{&2\log(4), \log(1) + \log(18), \\ &\log(3) + \log(4), \log(2) + \log(5)\}, \end{aligned}$$

which demonstrates a strict separation between our quantum protocol and any classical protocol.

VI. CONCLUSIONS

We considered the communication complexity problem of the GIP function with a specific promise. We proposed a quantum protocol utilizing $(n-1)\log(n)$ bits and a classical protocol employing $(n-1)^2(\log n^2)$ bits. By establishing a connection between the integer linear programming feasibility problem and the existence of a classical protocol with a particular communication complexity, we were able to provide numerical evidence supporting the quantum advantage in our model's communication complexity.

It would be interesting to analytically investigate the quantum advantage in the asymptotic limit when n increases.

VII. ACKNOWLEDGMENTS

The material in this work was supported in part by NSF grant CIF-1910840 and CIF-2115200.

Appendix A: Proof of Lemma 1

Recall that

$$\vec{\alpha} = [1,\ldots,1]^T.$$

The action of $\mathrm{QFT}^{\otimes n}$ on $\frac{1}{\sqrt{n}}\sum_{j=0}^{n-1}\omega^{-xj}\left|j\cdot\vec{\alpha}\right\rangle$ is

$$\frac{1}{n^{\frac{n}{2}}}\sum_{\vec{k}\in\mathbb{F}_n^n}a_{\vec{k}}\left|\vec{k}\right\rangle = QFT^{\otimes n}\left(\frac{1}{\sqrt{n}}\sum_{j=0}^{n-1}\omega^{-xj}\left|j\cdot\vec{\alpha}\right\rangle\right)$$
$$=\frac{1}{n^{\frac{n}{2}}}\sum_{\vec{k}\in\mathbb{F}_n^n}\left(\frac{1}{\sqrt{n}}\sum_{j=0}^{n-1}\omega^{-xj}\cdot\omega^{\langle\vec{k},j\cdot\vec{\alpha}\rangle}\right)\left|\vec{k}\right\rangle.$$

Write $\vec{k}=[k_1,\dots,k_n]^T$. Therefore,

$$a_{\vec{k}}=\frac{1}{\sqrt{n}}\sum_{j=0}^{n-1}\omega^{-xj}\cdot\omega^{\langle\vec{k},j\cdot\vec{\alpha}\rangle}=\frac{1}{\sqrt{n}}\sum_{j=0}^{n-1}\omega^{-xj+j\sum_{l=1}^{n}k_l}.$$

When $\vec{k}$ satisfies $\sum_{l=1}^{n}k_l=x$, we have that $a_{\vec{k}}=\sqrt{n}\neq 0$. Otherwise, since $-x+\sum_{l=1}^{n}k_l\neq 0$ and n being prime, $1-\omega^{n(-x+\sum_{l=1}^{n}k_l)}=0$ and $1-\omega^{-x+\sum_{l=1}^{n}k_l}\neq 0$. We have

$$\frac{1}{\sqrt{n}}\sum_{j=0}^{n-1}\omega^{-xj+j\sum_{l=1}^{n}k_l}=\frac{1}{\sqrt{n}}\sum_{j=0}^{n-1}\omega^{(-x+\sum_{l=1}^{n}k_l)j}$$
$$=\frac{1}{\sqrt{n}}\frac{1-\omega^{n(-x+\sum_{l=1}^{n}k_l)}}{1-\omega^{-x+\sum_{l=1}^{n}k_l}}=0.$$

Appendix B: Derivation of equation (6) and equation (7)

We derive equation (6) by considering two cases. The first case is that $[x_i^1,\dots,x_i^n]^T=[0,\dots,0]^T$. Then, we have

$$P_0^{\otimes n}\left(\frac{1}{\sqrt{n}}\sum_{k=0}^{n-1}\left|k\cdot\vec{\alpha}\right\rangle\right)\mapsto\frac{1}{\sqrt{n}}\omega^{-\frac{n(n-1)}{2}}\left|0\cdot\vec{\alpha}\right\rangle$$
$$+\frac{1}{\sqrt{n}}\sum_{k=1}^{n-1}\left|k\cdot\vec{\alpha}\right\rangle=\frac{1}{\sqrt{n}}\sum_{k=0}^{n-1}\left|k\cdot\vec{\alpha}\right\rangle=\frac{1}{\sqrt{n}}\sum_{k=0}^{n-1}\omega^{-k\cdot 0}\left|k\cdot\vec{\alpha}\right\rangle. \tag{B1}$$

The second case is that $[x_i^1,\dots,x_i^n]^T=[j,\dots,j]^T$ with $j\neq 0$. Then, we have

$$P_j^{\otimes n}\left(\frac{1}{\sqrt{n}}\sum_{k=0}^{n-1}\left|k\cdot\vec{\alpha}\right\rangle\right)\mapsto\frac{1}{\sqrt{n}}\sum_{k=0}^{n-1}\omega^{-n(\frac{1}{n}(kj \bmod n))}\left|k\cdot\vec{\alpha}\right\rangle$$
$$=\frac{1}{\sqrt{n}}\sum_{k=0}^{n-1}\omega^{-kj}\left|k\cdot\vec{\alpha}\right\rangle \tag{B2}$$

where the last equality holds since $\omega^{-kj}=\omega^{-(kj \bmod n)}$. Thus, in this case collectively, we can express the joint state after phase-shifting as $\frac{1}{\sqrt{n}}\sum_{k=0}^{n-1}\omega^{-kj}\left|k\cdot\vec{\alpha}\right\rangle$.

Now we derive equation (7). Assume $[x_j^1,\dots,x_j^n]^T=a[1,\dots,1]^T+b[0,1,\dots,n-1]^T$ with $b\neq 0$. If a and $b\neq 0$, then $a+b\cdot i\in\mathbb{F}_n$ is distinct for each $i\in\{0,\dots,n\}$. It can be observed that $a[1,\dots,1]+b[0,\dots,n-1]$ is a permutation of $[0,\dots,n-1]$, so it suffices to discuss $[x_i^1,\dots,x_i^p]^T=[0,\dots,n-1]^T$ by symmetry. Thus,

$$P_0\otimes\cdots\otimes P_{n-1}\left(\frac{1}{\sqrt{n}}\sum_{k=0}^{n-1}\left|k\cdot\vec{\alpha}\right\rangle\right)\mapsto$$
$$\frac{1}{\sqrt{n}}\omega^{-\frac{n-1}{2}}\left|0\cdot\vec{\alpha}\right\rangle+\frac{1}{\sqrt{n}}\sum_{k=1}^{n-1}\omega^{-\sum_{j=0}^{n-1}\frac{1}{n}(kj \bmod n)}\left|k\cdot\vec{\alpha}\right\rangle$$
$$\overset{(a)}{=}\frac{1}{\sqrt{n}}\omega^{-\frac{n-1}{2}}\left|0\cdot\vec{\alpha}\right\rangle+\frac{1}{\sqrt{n}}\sum_{k=1}^{n-1}\omega^{-\frac{1}{n}(\sum_{j=0}^{n-1}j)}\left|k\cdot\vec{\alpha}\right\rangle$$
$$=\frac{1}{\sqrt{n}}\omega^{-\frac{n-1}{2}}\left|0\cdot\vec{\alpha}\right\rangle+\frac{1}{\sqrt{n}}\sum_{k=1}^{n-1}\omega^{-\frac{1}{n}[\frac{n(n-1)}{2}]}\left|k\cdot\vec{\alpha}\right\rangle$$
$$=\frac{1}{\sqrt{n}}\omega^{-\frac{n-1}{2}}\sum_{k=0}^{n-1}\left|k\cdot\vec{\alpha}\right\rangle$$

where (a) follows from the fact that $\{kj \bmod n|j\in\{0,\dots,n-1\}\}=\{0,\dots,n-1\}$ for $k\neq 0$. It follows that

$$QFT^{\otimes n}\left(\frac{1}{\sqrt{n}}\omega^{-\frac{n-1}{2}}\sum_{k=0}^{n-1}\left|k\cdot\vec{\alpha}\right\rangle\right)$$
$$=\frac{1}{\sqrt{n}}\omega^{-\frac{n-1}{2}}QFT^{\otimes n}\left(\sum_{k=0}^{n-1}\left|k\cdot\vec{\alpha}\right\rangle\right)=\frac{1}{\sqrt{n}}\omega^{-\frac{n-1}{2}}\sum_{\vec{k}\in\mathbb{F}_n^n}a_{\vec{k}}\left|\vec{k}\right\rangle.$$

Appendix C: Proof of Theorem 2

For $a,b\in\mathbb{F}_n$, we define $M_{a,b}=\{i\in[m]|[x_i^1,\dots,x_i^n]^T=a[1,\dots,1]^T+b[0,1,\dots,n-1]^T\}$ and $m_{a,b}=|M_{a,b}|$. Since the promise is that, for each $i\in\{1,\dots,m\}$, there exists $a,b\in\mathbb{F}_n$ s.t. $[x_i^1,\dots,x_i^n]^T=a[1,\dots,1]^T+b[0,1,\dots,n-1]^T\in\mathbb{F}_n^n$, we have that $\{M_{a,b}|a,b\in\mathbb{F}_n\}$ forms a partition of the set $\{1,\dots,m\}$.

When $i\in M_{a,0}$, i.e. $[x_i^1,\dots,x_i^n]^T=a[1,\dots,1]^T$, we have

$$\prod_{p=1}^{n}x_i^p=a^n=a. \tag{C1}$$

Otherwise, we have $i\in M_{a,b}$ for some $b\neq 0$, so $a[1,\dots,1]^T+b[0,\dots,n-1]^T$. Then,

$$\prod_{p=1}^{n}x_i^p=\prod_{i=0}^{n-1}(a+i\cdot b)=0. \tag{C2}$$

By (C1) and (C2), if $i\in M_{a,b}$, then $\prod_{p=1}^{n}x_i^p=\delta_{0b}\cdot a$. Define

$$\mathbb{1}((x_i^1,\dots,x_i^n),M_{a,b})=\begin{cases}1, & i\in M_{a,b}\\ 0, & \text{otherwise},\end{cases}$$

i.e. it is the indicator of $i\in M_{a,b}$. Since $\{M_{a,b}\mid a,b\in\mathbb{F}_n\}$ is a partition of the set $[m]$, $i\in M_{a,b}$ for exactly one choice of (a,b). It follows that

$$\prod_{p=1}^{n} x_i^p = \delta_{0b}\cdot a = \sum_{a,b=0}^{n-1} \delta_{0b}\cdot a\cdot \mathbb{1}((x_i^1,\dots,x_i^n), M_{a,b}). \quad \text{(C3)}$$

We have

$$\begin{aligned}
&\sum_{i=1}^{m}\prod_{p=1}^{n} x_i^p \\
\overset{(*)}{=}&\sum_{i=1}^{m}\sum_{a,b=0}^{n-1} a\cdot\delta_{0b}\cdot \mathbb{1}((x_i^1,\dots,x_i^n), M_{a,b}) \\
=&\sum_{a,b=0}^{n-1}\sum_{i=1}^{m} a\cdot\delta_{0b}\cdot \mathbb{1}((x_i^1,\dots,x_i^n), M_{a,b}) \\
=&\sum_{a,b=0}^{n-1} a\cdot\delta_{0b}\cdot m_{a,b} = \sum_{a=0}^{n-1} a\cdot m_{a,0} \pmod n.
\end{aligned} \quad \text{(C4)}$$

Here, (*) follows from (C3). Our next step is to show $\sum_{a=0}^{n-1} am_{a,0} = W/n \pmod n$; W is defined in Alg. 2.

Suppose $i\in M_{a,b}$, then $(x_i^1,\dots,x_i^n) = a(1,\dots,1)+b(0,\dots,n-1)$. For pth player, $a+(p-1)b$ is the value of its ith coordinate of his vector $\vec{x}^p$. For a fixed $k\in\mathbb{F}_n$, the set of (a,b) s.t. $a+(p-1)b=k$ is $\{(k,0),(k+p-1,-1),(k+2p-2,-2),\dots,(k+(n-1)(p-1),-(n-1)\}$. It follows that $\forall p\in\{1,\dots,n\}, k\in\mathbb{F}_n$,

$$\beta_k^p = \sum_{i=0}^{n-1} m_{k+i(p-1),-i}. \quad \text{(C5)}$$

Consider $\sum_{i=0}^{n-1}\sum_{p=1}^{n} m_{k+i(p-1),-i}$. When $i=0$, $m_{k+i(p-1),-i}$ is counted n times. Denote $S=\{(0,0),\dots,(n-1,0)\}$. For arbitrary $[x,y]^T\in\mathbb{F}_n^2-S$, the equation $\begin{bmatrix}k+i(p-1)\\ -i\end{bmatrix} = \begin{bmatrix}x\\ y\end{bmatrix}$ has a unique solution given by $\begin{cases} i=-y,\\ p=\frac{y-x+k}{y}.\end{cases}$ Then, we have

$$\mathbb{F}_n^2 - S = \{(k+i(p-1),-i)|p\in\{1,\dots,n\}, i\in\{1,\dots,n-1\}\}.$$

Therefore, when $i\neq 0$, $m_{k+i(p-1),-i}$ is counted exactly once. It follows that

$$\begin{aligned}
&\sum_{p=1}^{n}\sum_{i=0}^{n-1} m_{k+i(p-1),-i} \\
=&\sum_{p=1}^{n}\sum_{i=1}^{n-1} m_{k+i(p-1),-i} + \sum_{p=1}^{n} m_{k+0(p-1),0} \\
=&\sum_{a,b\in\mathbb{F}_n^2-S} m_{a,b} + n\cdot m_{k,0}.
\end{aligned} \quad \text{(C6)}$$

Now we have

$$\begin{aligned}
&\sum_{p=1}^{n}\sum_{k=1}^{n-1} k\cdot\beta_k^p \\
\overset{\text{(C5)}}{=}&\sum_{k=1}^{n-1} k\sum_{p=1}^{n}\sum_{i=0}^{n-1} m_{k+i\cdot(p-1),-i} \\
\overset{\text{(C6)}}{=}&\sum_{k=1}^{n-1} k\Big[\sum_{a,b\in\mathbb{F}_n^2-S} m_{a,b} + n\cdot m_{k,0}\Big] \\
=&\frac{n^2-n}{2}\sum_{a,b\in\mathbb{F}_n^2-S} m_{a,b} + n\sum_{k=1}^{n-1} k\cdot m_{k,0}
\end{aligned}$$

and that

$$\begin{aligned}
&\sum_{p=1}^{n}\beta_0^p \overset{\text{(C5)}}{=} \sum_{p=1}^{n}\sum_{i=0}^{n-1} m_{i\cdot(p-1),-i} \\
\overset{\text{(C6)}}{=}&\sum_{a,b\in\mathbb{F}_n^2-S} m_{a,b} + n\cdot m_{0,0}.
\end{aligned}$$

Note $n>2$ is prime, so $n-1$ is divisible by 2. It follows that

$$\begin{aligned}
W =&\sum_{p=1}^{n}\sum_{k=1}^{n-1} k\cdot\beta_k^p + \frac{n^2-n}{2}\cdot(n-1)\sum_{p=1}^{n}\beta_0^p \\
=&\frac{n^2-n}{2}\sum_{a,b\in\mathbb{F}_n^2-S} m_{a,b} + n\sum_{k=1}^{n-1} k\cdot m_{k,0} \\
&+\frac{n^2-n}{2}\cdot(n-1)\Big[\sum_{a,b\in\mathbb{F}_n^2-S} m_{a,b} + n\cdot m_{0,0}\Big] \\
=&n\sum_{k=1}^{n-1} k\cdot m_{k,0} + n^2\cdot\frac{(n-1)}{2}\sum_{a,b\in\mathbb{F}_n^2-S} m_{a,b} \\
&+n^2\cdot\frac{(n-1)^2}{2}\cdot m_{0,0} \\
=&n\sum_{k=0}^{n-1} k\cdot m_{k,0} \pmod{n^2}.
\end{aligned}$$

Divide both sides by n and we get $W/n = \sum_{k=1}^{n-1} km_{k,0} \pmod n$. Now we are done because of (C4).

Appendix D: Proof of theorem 3

Suppose we have a protocol that computes the function with zero-error. Our protocol is deterministic, so, for each $\vec{x}^p\in\mathbb{F}_n^m$, it is associated exactly one label $\hat{c}$ s.t. p-th player sends $\hat{c}$ if his vector is $\vec{x}^p$. We set $I_{\vec{x}^p,\hat{c}}=1$ and $I_{\vec{x}^p,c}=0$ for all $c\neq\hat{c}$. Therefore, $I_{\vec{x}^p,c}\in\{0,1\}$ and $\sum_{c\in[l]} I_{\vec{x}^p,c}=1$ are satisfied for all choice of $\vec{x}^p, c$.

Next, suppose we have that $(\vec{x}^1,\dots,\vec{x}^n)\sim_{GIP}(\vec{z}^1,\dots,\vec{z}^n)$. Furthermore, assume that the p-th player sends s^p/t^p for $\vec{x}^p/\vec{z}^p$ for $p=2,\dots,n$. This implies that

$\prod_{p=2}^{n} I_{\vec{x}^p,s^p} = 1$ and that $\prod_{p=2}^{n} I_{\vec{z}^p,t^p} = 1$. In addition, note that $\exists\ p$ such that $s^p \neq t^p$ as for these sequences, the symbols transmitted from users $2,\ldots,n$ have to be distinct.

Thus we have

$$1 = |\prod_{p=2}^{n} I_{\vec{x}^p,s^p} - \prod_{p=2}^{n} I_{\vec{z}^p,s^p}| = |\prod_{p=2}^{n} I_{\vec{x}^p,t^p} - \prod_{p=2}^{n} I_{\vec{z}^p,t^p}|$$

and consequently

$$\sum_{c_2\in[l^2],\ldots,c_n\in[l^n]} |\prod_{p=2}^{n} I_{\vec{x}^p,c^p} - \prod_{p=2}^{n} I_{\vec{z}^p,c^p}| =$$
$$|\prod_{p=2}^{n} I_{\vec{x}^p,\hat{s}^p} - \prod_{p=2}^{n} I_{\vec{z}^p,\hat{s}^p}| + |\prod_{p=2}^{n} I_{\vec{x}^p,\hat{t}^p} - \prod_{p=2}^{n} I_{\vec{z}^p,\hat{t}^p}| = 2.$$

Therefore, the third constraint is satisfied.

Conversely, if we have $\{I_{\vec{x}^p,c}|\vec{x}^p \in \mathbb{F}_n^m, c \in [l^p]\}$ that satisfy the constraints of the ILP, then we construct a classical protocol as follows. Suppose p-th player has vector $\vec{x^p}$ for $p \in \{1,\ldots,n\}$. Since there exists exactly one $s^p \in [l^p]$ s.t. $I_{x^p,s^p} = 1$, then p sends s^p to Alice for $p \in \{2,\ldots,n\}$. When Alice receives the symbols $s^p, p = 2,\ldots,n$ from the other players she picks arbitrary $\{\vec{y}^p \in \mathbb{F}_n^m\}_{i=2}^n$ s.t. $(\vec{x}^1,\vec{y}^2,\ldots,\vec{y}^n)$ satisfies the promise and $\forall p \in \{2,\ldots,n\}, I_{\vec{y}^p,s^p} = 1$.Then she outputs $f(\vec{x}^1,\vec{y}^2,\ldots,\vec{y}^n)$. In what follows we show that

$$GIP(\vec{x}^1,\vec{y}^2,\ldots,\vec{y}^n) = GIP(\vec{x}^1,\vec{x}^2,\ldots,\vec{x}^n).$$

To see this assume otherwise. Then, we have $GIP(\vec{x}^1,\vec{y}^2,\ldots,\vec{y}^n) \neq GIP(\vec{x}^1,\vec{x}^2,\ldots,\vec{x}^n)$. It follows that

$$(\vec{x}^1,\vec{x}^2,\ldots,\vec{x}^n) \sim_{GIP} (\vec{x}^1,\vec{y}^2,\ldots,\vec{y}^n).$$

Because of the third constraint, we have that

$$\sum_{c^2,\ldots,c^n\in[l]} |\prod_{p=2}^{n} I_{\vec{x}^p,c^p} - \prod_{p=2}^{n} I_{\vec{y}^p,c^p}| = 2.$$

However, we have that $I_{\vec{x}^i,s^i} = I_{\vec{y}^i,s^i} = 1$ for all $i \in \{2,\ldots,n\}$. By the first and second constraint, we have that $I_{\vec{x}^i,c^i} = I_{\vec{y}^i,c^i} = 0$ for all $i \in \{2,\ldots,n\}$ and $c^i \neq s^i$. Therefore,

$$\sum_{c^2,\ldots,c^n\in[l]} |\prod_{p=2}^{n} I_{\vec{x}^p,c^p} - \prod_{p=2}^{n} I_{\vec{y}^p,c^p}| = 0.$$

This gives the desired contradiction.

Appendix E: Linearizing constraints in the integer programming problem

The problem of the optimization problem (8) is that the third constraint has multiple absolute value and products of variables. Here we transform the constraints and add extra variable in (8) to get the desired ILP.

Our first step is to introduce auxiliary 0-1 variables that correspond to the product of other 0-1 variables. For instance, it can be verified that we can set $\prod_{i=1}^{k} x_i = x'$ as follows.

$$x' \leq x_i, \text{ for } i = 1,\ldots,k \tag{E1}$$

$$x' \geq \sum_{i=1}^{k} x_i - (k-1). \tag{E2}$$

As a first step we introduce such auxiliary variable for all terms that involve products of our indicator function in (8).

Following this step, we are left with handling constraints that involve sums of absolute values of differences. For this step we show how to replace each absolute value difference by another auxiliary variable. In particular, we can replace $|x-y|$ by z as follows.

$$\begin{aligned} |x-y| &= |x-y|^2 \\ &= x^2 + y^2 - 2xy \\ &= x + y - 2xy \end{aligned}$$

where the last step follows from the fact that the variables are of type $0-1$. The product term $2xy$ can be linearized as described previously. Following these steps, all constraints in the integer programming problem are linear.

[1] A. C.-C. Yao, Some complexity questions related to distributive computing(preliminary report), in *Proceedings of the Eleventh Annual ACM Symposium on Theory of Computing*, STOC '79 (Association for Computing Machinery, New York, NY, USA, 1979) p. 209–213.

[2] A. Chi-Chih Yao, Quantum circuit complexity, in *Proceedings of 1993 IEEE 34th Annual Foundations of Computer Science* (1993) pp. 352–361.

[3] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, Rev. Mod. Phys. **81**, 865 (2009).

[4] H. Buhrman, R. Cleve, S. Massar, and R. de Wolf, Nonlocality and communication complexity, Rev. Mod. Phys. **82**, 665 (2010).

[5] R. Cleve and H. Buhrman, Substituting quantum entanglement for communication, Phys. Rev. A **56**, 1201 (1997).

[6] R. de Wolf, Quantum communication and complex-

ity, Theoretical Computer Science **287**, 337 (2002), natural Computing.

[7] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels, Phys. Rev. Lett. **70**, 1895 (1993).

[8] H. Buhrman, R. Cleve, and A. Wigderson, Quantum vs. classical communication and computation, in *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*, STOC '98 (Association for Computing Machinery, New York, NY, USA, 1998) p. 63–68.

[9] R. Cleve, W. van Dam, M. Nielsen, and A. Tapp, Quantum entanglement and the communication complexity of the inner product function, Theoretical Computer Science **486**, 11 (2013), theory of Quantum Communication Complexity and Non-locality.

[10] H. Buhrman and R. de Wolf, Communication complexity lower bounds by polynomials, in *Proceedings of Computational Complexity. Sixteenth Annual IEEE Conference* (IEEE Computer Society, Los Alamitos, CA, USA, 2001) p. 0120.

[11] A. A. Razborov, Quantum communication complexity of symmetric predicates, Izvestiya: Mathematics **67**, 145 (2003).

[12] H. Klauck, Lower bounds for quantum communication complexity, SIAM Journal on Computing **37**, 20 (2007), https://doi.org/10.1137/S0097539702405620.

[13] W. van Dam and P. Hayden, Renyi-entropic bounds on quantum communication (2002), arXiv:quant-ph/0204093 [quant-ph].

[14] A. Marwah and D. Touchette, Optical quantum communication complexity in the simultaneous-message-passing model, Phys. Rev. A **102**, 062608 (2020).

[15] F. Le Gall and D. Suruga, Bounds on oblivious multiparty quantum communication complexity, in *LATIN 2022: Theoretical Informatics*, edited by A. Castañeda and F. Rodríguez-Henríquez (Springer International Publishing, Cham, 2022) pp. 641–657.

[16] F. Le Gall and S. Nakajima, Multiparty Quantum Communication Complexity of Triangle Finding, in *12th Conference on the Theory of Quantum Computation, Communi* Leibniz International Proceedings in Informatics (LIPIcs), Vol. 73, edited by M. M. Wilde (Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany, 2018) pp. 6:1–6:11.

[17] T. Lee, G. Schechtman, and A. Shraibman, Lower bounds on quantum multiparty communication complexity, in *2009 24th Annual IEEE Conference on Computational Complexity* (2009) pp. 254–262.

[18] J. Briët, H. Buhrman, T. Lee, and T. Vidick, Multiplayer xor games and quantum communication complexity with (2009).

[19] H. Buhrman, W. van Dam, P. Høyer, and A. Tapp, Multiparty quantum communication complexity, Phys. Rev. A **60**, 2737 (1999).

[20] P. Xue, C.-F. Li, Y.-S. Zhang, and G.-C. Guo, Three-party quantum communication complexity via entangled tripartite pure states, Journal of Optics B: Quantum and Semiclassical Optics **3**, 219 (2001

[21] E. F. Galvão, Feasible quantum communication complexity protocol, Phys. Rev. A **65**, 012318 (2001).

[22] Python code for ILP in Sec. V.