The Power of One Clean Qubit in Communication Complexity

Hartmut Klauck ✉

Centre for Quantum Technologies, National University of Singapore, Singapore

Debbie Lim ✉

Centre for Quantum Technologies, National University of Singapore, Singapore

──── **Abstract** ────

We study quantum communication protocols, in which the players' storage starts out in a state where one qubit is in a pure state, and all other qubits are totally mixed (i.e. in a random state), and no other storage is available (for messages or internal computations). This restriction on the available quantum memory has been studied extensively in the model of quantum circuits, and it is known that classically simulating quantum circuits operating on such memory is hard when the additive error of the simulation is exponentially small (in the input length), under the assumption that the polynomial hierarchy does not collapse.

We study this setting in communication complexity. The goal is to consider larger additive error for simulation-hardness results, and to not use unproven assumptions.

We define a complexity measure for this model that takes into account that standard error reduction techniques do not work here. We define a clocked and a semi-unclocked model, and describe efficient simulations between those.

We characterize a one-way communication version of the model in terms of weakly unbounded error communication complexity.

Our main result is that there is a quantum protocol using one clean qubit only and using $O(\log n)$ qubits of communication, such that any classical protocol simulating the acceptance behaviour of the quantum protocol within additive error $1/poly(n)$ needs communication $\Omega(n)$.

We also describe a candidate problem, for which an exponential gap between the one-clean-qubit communication complexity and the randomized communication complexity is likely to hold, and hence a classical simulation of the one-clean-qubit model within *constant* additive error might be hard in communication complexity. We describe a geometrical conjecture that implies the lower bound.

1 Introduction

The computational power of quantum models of computation with different memory restrictions has been studied in order to understand the use of imperfectly implemented qubits. Some possible types of memory restrictions include having only few qubits that are in a pure state plus an abundance of qubits that start in the totally mixed state [12], having memory that starts in an incompressible state that needs to be returned unchanged at the end of the computation, plus some limited auxiliary space available [8], or simply having very little

46th International Symposium on Mathematical Foundations of Computer Science (MFCS 2021).
Editors: Filippo Bonchi and Simon J. Puglisi; Article No. 69; pp. 69:1–69:23

Leibniz International Proceedings in Informatics
LIPIcs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

memory for the computation [2, 20, 16, 3]. The underlying idea in these topics is to study the power of models of quantum computing in which the quantum memory is weak, but the control of this memory is good. This is in contrast to the study of models of quantum computation, where the underlying memory is good, but the control is weak, or restricted, such as the Boson-Sampling model [1]. Both are a step towards understanding the power of quantum computing models that are closer to being implementable than the standard circuit model, and eventually to demonstrate quantum supremacy (i.e., to show that for some problem (of possibly small practical interest) quantum computers that can be built outperform classical computers demonstrably).

This paper explores the potential of a model of quantum communication that uses memory containing only a small number of qubits that start in a known pure state, in particular the power of a having only a single clean qubit (plus many qubits that start in the totally mixed state, i.e., start in a random state).

The one-clean-qubit model proposed by Knill and Laflamme [21] is a model of quantum computing where the memory starts in the tensor product of a single qubit in a pure state $|0\rangle$ with the other m qubits that are in the completely-mixed state, with no further storage allowed. This initial state is described by the density matrix $\rho = |0\rangle\langle 0| \otimes \frac{I}{2^m}$.

The model was originally motivated by the nuclear magnetic resonance (NMR) approach to quantum computing, where the initial state may be highly mixed. Quantum circuits operating on such memory are able to perform tasks that look hard classically, such as estimating Jones polynomials, computing Schatten p-norms, spectral density approximation, testing integrability, computation of fidelity decay [21, 34, 9, 30, 31], just to name a few. [12] showed that quantum circuits under the one-clean-qubit restriction cannot be efficiently classically simulated unless the polynomial hierarchy collapses to the second level. In other words, assuming that the polynomial hierarchy does not collapse, polynomial size quantum circuit operating under the one-clean qubits restriction can have acceptance/rejection probabilities such that any classical randomized circuit that has the same acceptance/rejection probabilities up to additive error $1/exp(n)$ must have superpolynomial size. We note here that we will not consider simulations with multiplicative error in this paper, since those pose a much stronger requirement on the simulation, for instance the simulating algorithm must replicate events of tiny probability with approximately the same probability, and hence such simulations are much less interesting.

In this paper, we study the hardness of simulating the one-clean-qubit model classically in the model of communication complexity. We will consider simulations of the one-clean-qubit model with different amounts of additive errors, namely $\frac{1}{poly(n)}$ and $O(1)$.

Organization

After some preliminaries in Section 2, in Section 3 we discuss related work. In Section 4, we sketch our results. In Section 5 we develop our model of quantum communication with one clean qubit. We motivate the main complexity measure and introduce the concepts of clocked and semi-unclocked protocols. Section 6 is about our characterization of one-way communication complexity in our model. Section 8 discusses our main result, which concerns the hardness of classically simulating the one-clean-qubit model with additive error.

2   Preliminaries

Communication Complexity

Yao's [38] model of communication complexity consists of two players, Alice and Bob, who are each given private inputs $x \in X$ and $y \in Y$ respectively. In addition, they both know the function f and agree to a certain communication protocol beforehand. The task they wish to perform is to compute $z = f(x, y)$. Having no knowledge of each others' inputs, they have to communicate with each other in order to obtain the result z. Communication complexity asks the question "how much communication is needed to compute $f(x, y)$?", and assumes that the players have unlimited computational power.

For formal definitions regarding standard types of communication protocols see [24], regarding quantum communication complexity see [11]. We will use the following notations:

▶ **Definition 1.** $Q(f), R(f)$ *denote the quantum (without entanglement) and randomized (with public coin) communication complexities of a function f with error $1/3$. A subscript like $Q_\epsilon(f)$ denotes other errors ϵ.*

3   Related Work

There has been a lot of research focusing on the hardness of classical simulations of restricted models of quantum computing under certain assumptions [5, 1, 37, 29, 14, 26, 36, 6, 35]. That is to say, a reasonable assumption in complexity theory leads to the impossibility of efficient sampling by a classical computer according to an output probability distribution that can be generated by a quantum computation model. For instance, it is proven that classical simulation with multiplicative error of the IQP model [5] and Boson sampling [1] is hard, unless the polynomial-time hierarchy collapses.

It is interesting to ask if such a result holds for the one-clean-qubit model as well. Over the past few years, the one-clean-qubit model has be shown to be capable of efficiently solving problems where no efficient classical algorithm is known, such as estimating Jones polynomials, computing Schatten p-norms, spectral density approximation, testing integrability and computation of fidelity decay [21, 34, 9, 30, 31]. It has been conjectured that the one-clean-qubit model can be more powerful than classical computing for some problems. However, there has been no proof for such a conjecture. In [27], it is showed that if the output probability distribution of the one-clean-qubit model can be classically efficiently approximated (with at most an exponentially small additive error) then $BQP \subseteq BPP$. Although the belief that $BQP \neq BPP$ is equivalent to that of $P \neq NP$ or that the polynomial hierarchy does not collapse, there is still a good case for it and the assumption is necessary for simulation hardness anyway. Therefore the results in [27] suggest that the one-clean-qubit model is unlikely to be classically efficiently simulatable with exponentially small additive error.

[26] introduced $DQC1_k$, a modified version of the one-clean-qubit model where the workspace starts with one clean qubit and k qubits are measured at the end of the computation. They showed that the $DQC1_k$ model cannot be efficiently classically simulated for $k \geqslant 3$ (within constant *multiplicative* error) unless the polynomial hierarchy collapses.

Later on, [26] showed via circuit complexity that the one-clean-qubit model cannot be efficiently classically simulated with $\frac{1}{exp(n)}$ additive error unless the polynomial hierarchy collapses to the second level.

All existing results regarding the efficient classical simulation of the one-clean-qubit model are conditional (e.g. rely on non-collapse of the polynomial hierarchy) and require simulations to have exponentially small additive error.

We also mention work on classical memory-restricted communication complexity (e.g. [7]) in which some similar issues appear as in this work.

4 Overview of Results

- Definition of a complexity measure for the one-clean-qubit model in communication complexity:
  The complexity measure (cost) of a one-clean-qubit protocol is given by $c \cdot \left(\frac{1}{\epsilon^2} \right)$, where c is the communication and ϵ is the bias. We define a clocked and a semi-unclocked version.
- Simulation of a clocked k-clean-qubit models using only one-clean qubit is inexpensive:
  Such simulations cost $(c + 1) \cdot \left(\frac{2^k}{\epsilon} \right)^2$, where c is the communication and ϵ is the bias.
- The clocked k-clean-qubit model can be simulated by the semi-unclocked one-clean-qubit model:
  Such simulations incur a cost of $O(c \log c) \cdot \left(\frac{2^k}{\epsilon} \right)^2$, where c is the communication and ϵ is the bias.
- Upper and lower bounds on the complexity measure of the one-way one-clean-qubit communication complexity model:
  The complexity measure of the one-way one-clean-qubit communication complexity model denoted as $Q_{[1]}^{A \to B}(f)$ is bounded by $2^{\Omega(PP(f)) - O(\log n)} \leqslant Q_{[1]}^{A \to B}(f) \leqslant 2^{O(PP(f))}$. See [17] for the definition of $PP(f)$.
- Classically simulating the one-clean-qubit model with $\frac{1}{poly(n)}$ additive error requires an exponential increase in communication:
  We consider the $MIDDLE$ problem and give a quantum protocol with one-clean qubit that requires $O(\log n)$ communication while any classical simulation with $\frac{1}{poly(n)}$ additive error requires $\Omega(n)$ communication.
  We stress that in previous results about the hardness of simulating the one-clean-qubit model (in circuit complexity) the additive error must be of size at most $1/exp(n)$ for the simulation to be hard, which stems from low probability events being considered that one would never observe realistically. That means that running the one-clean-qubit circuit as an experiment, and observing an outcome that contradicts classicality is an event that happens only with exponentially small probability, and the classical simulation is only hard because of such extremely low probability events. Our result also uses low probability events, but $1/poly(n)$ is much more reasonable, and the events are observable when repeating such a protocol $poly(n)$ times.
- Simulating the one-clean-qubit model with constant additive error:
  We consider a problem ABC as a candidate to show that simulating the one-clean-qubit model with *constant* additive error is hard, and construct a quantum protocol that requires $O(\log n)$ communication using one clean qubit for ABC. We conjecture that any classical simulation with constant additive error requires $\Omega(\sqrt{n})$ communication and give a matching upper bound.

Disclaimer: All I's used in this paper are identity matrices whose dimensions are clear from the context.

5 Communication Complexity of the One-Clean-Qubit Model

5.1 The One-Clean-Qubit Model

▶ **Definition 2** (k-Clean-Qubit Model). *In a k-clean-qubit protocol, all storage initially consists of only k qubits in a clean state $|0\rangle$, while the rest (m qubits) are in the totally mixed state. The players communicate as in a standard quantum protocol. Only at the end of the computation, a single, arbitrary projective measurement (not depending on the inputs) is performed.*

By this definition, all storage in the one-clean-qubit model consists of only one qubit in a clean state $|0\rangle$, while the rest (m qubits) are in the totally mixed state. This can be described by the density matrix

$$\rho = |0\rangle\langle 0| \otimes \frac{I}{2^m}. \tag{1}$$

A protocol in this model for a function f communicates c qubits. Assume the protocol has a bias of ϵ and hence an error of $\frac{1}{2} - \epsilon$. In general, it is not possible to improve the error to, say, $\frac{1}{3}$. Analogous to allowing the computation to be repeated $O(\frac{1}{\epsilon^2})$ times until a correctness probability of at least $\frac{2}{3}$ is achieved, we define the cost of the (unrepeated) protocol to be $c \cdot (\frac{1}{\epsilon})^2$ qubits.

▶ **Definition 3** ($Q_{[1]}(f)$). *Let $\mathcal{P}$ denote a one-clean-qubit clocked (explained later) protocol for a function $f : X \times Y \to \{0,1\}$, such that 0-inputs are accepted with probability at most $p - \epsilon$ and 1-inputs are accepted with probability at least $p + \epsilon$ for some constant $p > 0$ and that uses communication c at most on all inputs. The cost of $\mathcal{P}$ is then c/ϵ^2.*

We denote the complexity measure of the clocked one-clean-qubit model by $Q_{[1]}(f) = \inf_{\mathcal{P}} \frac{communication(\mathcal{P})}{bias(\mathcal{P})^2}$, where the infimum is over all protocols $\mathcal{P}$ for f.

The motivation behind Definition 3 is that it seems unlikely that the success probability can always be amplified arbitrarily. Therefore, we allow the protocol to run with an arbitrarily bad bias but include the cost that it would take to bring this bias up by a standard amplification (repeat the computation $O\left(\frac{1}{bias^2}\right)$ times): in the situation described in Definition 3 by a standard Chernoff bound repeating $t = 4/\epsilon^2$ times (and accepting if at least pt runs accepted) would lead to error at most $1/3$.

There is no prior entanglement allowed in this model because the EPR-pairs could be used to create more pure qubits, simply by sending one qubit from one communicating party to another, who can then make the state $|00\rangle$. It is also essential that measurements are performed only at the end of the computation, or a pure state could be obtained by measuring the state (1).

In our paper, we allow arbitrary projective measurements in the one-clean-qubit model. There are papers such as [34] and [27] defining the one-clean-qubit model in a way such that it measures only one qubit at the end of the computation. However, in Theorem 8, we show that there is only negligible difference between these definitions in communication complexity.

5.2 Clocked and Semi-unclocked Models

We consider two types of models: the clocked model and the semi-unclocked model.
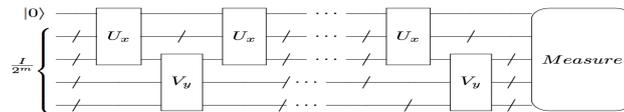
▶ **Definition 4** (Clocked model). *In the clocked model, the message in round i is computed by a unitary that can depend on i. In other words, the protocol knows i without having to store i anywhere. The communication channel of a clocked model is ghosted, i.e. different qubits can be communicated in different rounds.*

Protocols in the clocked model implicitly use a counter to tell the protocol which round it is in. This counter could be considered as extra classical storage, so we define another model that does not allow this. In that model, however, protocols still need to know when to stop, and that in a sense is a counter, just one that cannot be used "inside" the protocol. Since no intermediate measurements are allowed, we simply switch the protocol off after the correct number of rounds, and measure.
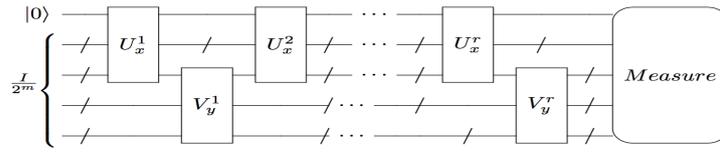
◼ **Figure 1** Clocked model.

▶ **Definition 5** (Semi-unclocked model). *In the semi-unclocked model, the same unitary must be applied in every round. The protocol terminates after a fixed number of rounds. The communication channel of a semi-unclocked model is fixed, i.e., the same qubits have to be communicated in every round.*

◼ **Figure 2** Semi-unclocked model.

▶ **Example 6.** The inner product modulo 2 problem is defined as $IP_2(x, y) = \sum_i x_i y_i$ mod 2, where $x, y \in \{0, 1\}^n$. Under the clocked model $\hat{P}$ shown in Figure 3, let U_x^i be Alice's unitary and let V_y^i be Bob's for $i = 1 \cdots n$. We start with two clean qubits. The first qubit is meant to store Alice's x_i while the second stores $\sum_i x_i y_i$ mod 2. The protocol (informally) goes as follows:

In the first round, Alice stores x_1 in the first qubit and sends the two qubits to Bob, who multiplies x_1 in the first qubit with his y_1 and stores the product in the second qubit. He then sends the first qubit back to Alice. For every round $i = 2, \cdots, n$,

1. U_x^i first XORs $|x_{i-1}\rangle$ on the first qubit with x_{i-1}, thereby restoring the qubit to $|0\rangle$, before storing the value x_i in it.
2. Alice sends the first qubit to Bob.
3. V_y^i multiplies y_i with x_i (stored in the first qubit) and adds the product to the sum stored in the second qubit modulo 2.
4. Bob sends the first qubit back to Alice.

The communication terminates after a total number of $2n - 1$ rounds and the bias is $\frac{1}{2}$ (i.e. zero error). Bob does the measurement, the total communication is $2n$.

◼ **Figure 3** Clocked two-clean-qubit model for computation of inner product modulo 2.

$\hat{P}$ can be simulated with a clocked one-clean-qubit protocol that uses 1 clean qubit and 2 mixed qubits. The unitary $\mathcal{M}$ does the following:

$$\mathcal{M} : \begin{cases} |0\rangle \otimes |0\rangle \otimes |0\rangle \mapsto |1\rangle \otimes |0\rangle \otimes |0\rangle \\ |0\rangle \otimes |z_1\rangle \otimes |z_2\rangle \mapsto |0\rangle \otimes |z_1\rangle \otimes |z_2\rangle \end{cases},$$

where $|z_1\rangle$ or $|z_2\rangle \neq |0\rangle$. Extend to a unitary arbitrarily. In other words, $\mathcal{M}$ flips the first qubit if the next two qubits are both in the $|0\rangle$ state (this happens with probability $\frac{1}{4}$). After applying $\mathcal{M}$, the protocol is carried out as per $\hat{P}$. The measurement is done as follows:

- If the first qubit is $|0\rangle$, a "coin toss" is being performed for the output (e.g. measure yet another mixed qubit).
- If the first qubit is $|1\rangle$, the measurement is done as per $\hat{P}$.

Note that the two measurements can be combined into one.

Therefore, we get an error probability of $\frac{3}{4} \cdot \frac{1}{2} = \frac{3}{8}$, and a bias of $\frac{1}{8}$. The total communication is $2n + 1$ and hence the cost is $64(2n + 1) = O(n)$.

We now compare the k-clean-qubit model with the one-clean-qubit model and also the clocked model with the semi-unclocked model. We prove the following theorems:

▶ **Theorem 7.** *Given a clocked k-clean-qubit protocol $\mathcal{P}$ for a function f that has communication c and a bias of ϵ, there exists a clocked one-clean-qubit protocol $\tilde{\mathcal{P}}$ for f that has communication c (or $c + 1$ depending on which player does the measurement), and a bias of $\frac{\epsilon}{2^k}$.*

Proof. The clocked k-clean-qubit protocol $\mathcal{P}$ illustrated in Figure 4 has communication c and a bias of ϵ. Hence, it has an error probability of $\frac{1}{2} - \epsilon$ and cost $\frac{c}{\epsilon^2}$. Denote by U_x^i Alice's unitaries and by V_y^i Bob's unitaries for $i = 1, \cdots, r$. Note that U_x^i is defined as a unitary on all qubits, but acts only on Alice's qubits.
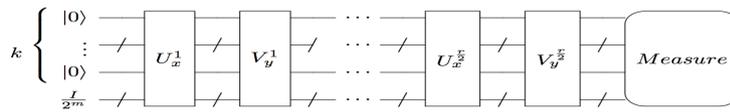
Figure 4 Clocked k-clean-qubits protocol $\mathcal{P}$.

$\mathcal{P}$ can be modified into a clocked one-clean-qubit protocol $\tilde{\mathcal{P}}$ as in Figure 5 with about the same amount of communication.
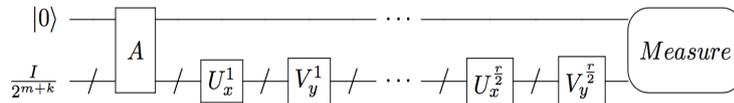
Figure 5 Clocked one-clean-qubit model $\tilde{\mathcal{P}}$.

In $\tilde{\mathcal{P}}$, the unitary A does a bit flip on the first qubit if the next k qubits are in the $|0\rangle$ state, and does nothing otherwise. All the $k + m$ mixed qubits undergo the same series of unitary transformation as in $\mathcal{P}$. The measurement in $\tilde{\mathcal{P}}$ is done as follows:

- If the first qubit is $|0\rangle$, a "coin toss" is being done.
- If the first qubit is $|1\rangle$, the measurement is carried out as per $\mathcal{P}$.

Note that the two measurements can be combined into one.

The communication in $\tilde{\mathcal{P}}$ is c or $c + 1$, depending on which player does the measurement. If the measurement is done by the player who begins the communication, the communication is c. Otherwise, the first qubit has to be sent to the other player for the measurement to be done, causing the communication to be increased to $c + 1$.

The error probability of $\tilde{\mathcal{P}}$ can be computed to be

$$(1 - \frac{1}{2^k}) \cdot \frac{1}{2} + \frac{1}{2^k} \cdot (\frac{1}{2} - \epsilon) = \frac{1}{2} - \frac{\epsilon}{2^k}.$$

Hence, the bias decreases from ϵ to $\frac{\epsilon}{2^k}$.

The cost of $\tilde{\mathcal{P}}$ is given by $c \cdot (\frac{2^k}{\epsilon})^2$ or $(c + 1) \cdot (\frac{2^k}{\epsilon})^2$. ◀

▶ **Theorem 8.** *Given a clocked k-clean-qubit protocol $\tilde{\mathcal{P}}$ for a function $f : X \times Y \to \{0,1\}$ with a ghosted communication channel, that does an arbitrary projective measurement with two outcomes, has communication c and a bias of ϵ, there exists a semi-unclocked one-clean-qubit protocol $\mathcal{P}_f$ for f with a fixed communication channel, that does a measurement on one qubit, has communication $O(c \log c)$ and a bias of $\Omega(\frac{\epsilon}{2^k})$.*

Proof. From Theorem 7, a clocked k-clean qubit protocol $\tilde{\mathcal{P}}$ with a ghosted communication channel that does an arbitrary projective measurement and has communication c and a bias of ϵ, can be modified into a clocked one-clean-qubit protocol $\mathcal{P}$ with a ghosted communication channel, that does an arbitrary projective measurement, has communication $c + 1$ and bias $\frac{\epsilon}{2^k}$. The total number of qubits is $m + k + 1$, with 1 clean qubit.

We would like to turn $\mathcal{P}$ into a protocol $\mathcal{P}'$ that measures only one qubit in the computational basis. This can be done by adding an extra clean qubit and replacing the measurement in $\mathcal{P}$ with a unitary operator U_S and a measurement that measures the newly added qubit in the standard basis. U_S does the following:

$$
U_S : \begin{cases} |a\rangle |b_i\rangle \mapsto |a\rangle |b_i\rangle, \text{ for } b_i \in B \\ |a\rangle |b_i\rangle \mapsto |a \oplus 1\rangle |b_i\rangle, \text{ for } b_i \notin B \end{cases} ,
$$

where $a \in \{0, 1\}$ and $B = \{b_1, \cdots, b_l\}$ is the basis of the subspace $S \subseteq \mathbb{C}^{m+k+1}$, which is a constituent of the observable used to measure the quantum state in $\mathcal{P}$.

In other words, U_S flips the first qubit on any basis vector $b_i \notin B$, and does nothing otherwise. The resulting protocol $\mathcal{P}'$ is as follows:
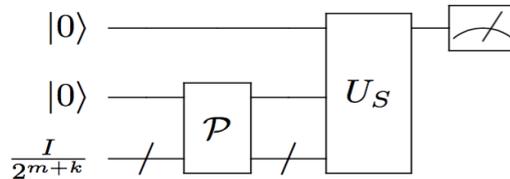
Figure 6 Clocked two-clean-qubit protocol that measures one qubit $\mathcal{P}'$.

▶ **Remark 9.** A clocked protocol with a ghosted communication channel can be easily converted to one with fixed channel in which Alice and Bob take turns to send one qubit each. This at most doubles the communication.

In the new protocol, the communication channel is fixed, the total communication is increased to at most $2(c + 1)$, and the bias remains unchanged.

According to [34], the probability of measuring 0 (which corresponds to acceptance) can be made to depend only on the trace of a unitary operator as shown below.

Consider the following trace estimation protocol $\mathcal{P}_{main}$ illustrated in Figure 7,
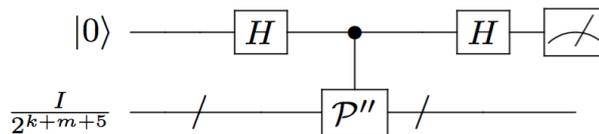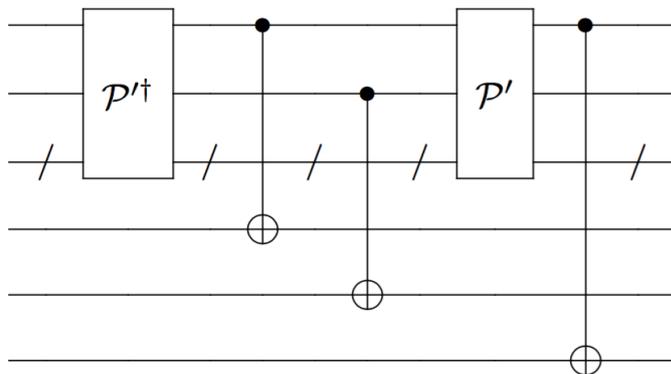
Figure 7 Trace estimation protocol $\mathcal{P}_{main}$.

which contains the unitary operator $\mathcal{P}''$ shown in Figure 8. $\mathcal{P}_{main}$ accepts with probability

$$\frac{1}{2} + \frac{Re(Tr(\mathcal{P}''))}{2^{d+1}},$$

where $d = m + k + 5$ is the number of qubits in $\mathcal{P}''$ and $Re(x)$ is the real part of x.

Figure 8 $\mathcal{P}''$.

Let I_ℓ denote the 2^ℓ-dimensional identity matrix. We have that

$$Tr[(|0\rangle\langle 0| \otimes I_{m+k+1})\mathcal{P}'(|0\rangle^2 \langle 0|^2 \otimes I_{m+k})\mathcal{P}'^\dagger] = \frac{1}{8}Tr[\mathcal{P}''],$$

because $Tr[\mathcal{P}''] = \sum_{x\in\{0,1\}^{m+k+5}} \langle x| \mathcal{P}'' |x\rangle$, and so for instance basis vectors $|x\rangle$ that have a 1 in qubit 1 contribute nothing to the sum due to the rightmost CNOT. Similarly, the other CNOTs correspond to the other projection one the left hand side. This equation also shows that the right-hand-side trace is real: up to scaling the left hand side corresponds to a probability of measuring 0 when running $\mathcal{P}'$ on the two-clean-qubit state.

The acceptance probability of $\mathcal{P}_{main}$ is given by

$$\begin{aligned}
p_0 &= \frac{1}{2} + \frac{Tr[\mathcal{P}'']}{2^{k+m+6}} \\
&= \frac{1}{2} + \frac{8 \cdot Tr[(|0\rangle\langle 0| \otimes I_{m+k+1})\mathcal{P}'(|0\rangle^2 \langle 0|^2 \otimes I_{m+k})\mathcal{P}'^\dagger]}{2^{k+m+6}} \\
&= \frac{1}{2} + \frac{8 \cdot 2^{k+m} \cdot \left(\frac{1}{2} + \frac{\epsilon}{2^k}\right)}{2^{k+m+6}} \\
&= \frac{1}{2} + \frac{1}{16} + \frac{\epsilon}{2^{k+3}}
\end{aligned}$$

▶ **Remark 10.** The factor of 8 instead of 4 as in [34] is due to the presence of three CNOT gates/extra qubits instead of two.
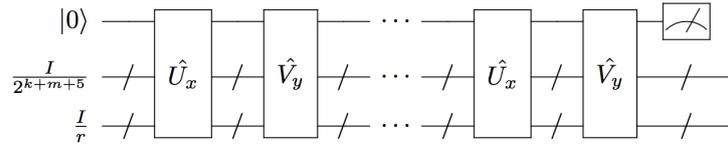
The communication of $\mathcal{P}_{main}$ is four times the communication of $\mathcal{P}'$, since $\mathcal{P}''$ runs $\mathcal{P}'$ backwards and forwards, and because the clean control qubit in $\mathcal{P}_{main}$ must be communicated in every round (every round communicates only one qubit in $\mathcal{P}'$), i.e. the communication becomes $8(c+1)$. The bias decreases to $\frac{\epsilon}{2^{k+3}}$ and is around $\frac{1}{2} + \frac{1}{16}$ instead of $\frac{1}{2}$.

Lastly, we turn $\mathcal{P}_{main}$ into a semi-unclocked protocol $\mathcal{P}_f$ by adding $\log r$ mixed qubits to act as a counter, where r is the number of rounds. The resulting protocol looks as follows:

In $\mathcal{P}_f$, $\hat{U}_x = (H \otimes I) \cdot U_x \cdot (H \otimes I)$, where

$$U_x : |z\rangle |i\rangle \mapsto (U_x^i |z\rangle) |i\rangle$$

Figure 9 Semi-unclocked one-clean-qubit protocol that measure one qubit $\mathcal{P}_f$.

and $\hat{V}_y = (H \otimes I) \cdot V_y \cdot (H \otimes I)$, where

$$V_y : |z\rangle |i\rangle \mapsto (V_y^i |z\rangle) |i+1 \mod r\rangle,$$

for all $z \in \{0,1\}^{k+m+6}$, for all $i \in \{0,1\}^{\log r}$ and where U_x^i and V_y^i are the unitaries from $\mathcal{P}''$.

This means that, starting from a random j on the counter, the unitaries $\hat{V}_y$ and $\hat{U}_x$ apply V_y^i and U_x^i in the correct, but shifted order. Also note that the Hadamard operators cancel out in between consecutive unitaries, and only the first and last have an effect.

▶ **Fact 11** (Cyclic property of matrix trace). *The trace of a product of three or more square matrices is invariant under cyclic permutations of the order of multiplication of the matrices.*

Since the acceptance probability of $\mathcal{P}_{main}$ depends only on the trace of the product of the sequence of unitary operators in $\mathcal{P}''$, it follows from Fact 11 that the counter can start from any arbitrary $j \mod r$ without affecting the acceptance probability of $\mathcal{P}_f$.

The protocol terminates after r rounds of communication. Note that $r = \Theta(c)$, the total communication is now $8(c+1) + O(c \log c) = O(c \log c)$. The bias is remains unchanged from $\mathcal{P}_{main}$, i.e. $\Omega(\frac{\epsilon}{2^k})$.   ◀

Applying Theorem 8 to Example 6 gives the following.

▶ **Corollary 12.** *The semi-unclocked one-clean-qubit quantum communication complexity of IP_2 is $O(n \log n)$.*

6   One-way Complexity with One Clean Qubit

6.1   The Upper Bound on $Q_{[1]}^{A \to B}(f)$

Let $Q_{[1]}^{A \to B}(f)$ denote the complexity measure of a one-way two-player one-clean-qubit protocol. We define a one-way two-player one-clean-qubit protocol as follows:

▶ **Definition 13** (One-way two-player one-clean-qubit protocol). *The computation in the one-way version of one-clean-qubit protocols starts with a single qubit in the clean state and the rest of the qubits in the totally mixed state. The first player applies her unitary on an arbitrary number of qubits, sends some of the qubits to the next player who also applies his unitary on an arbitrary number of qubits, and does a measurement. The cost is defined as for general one-clean qubit protocols. This can be described by the figure below:*
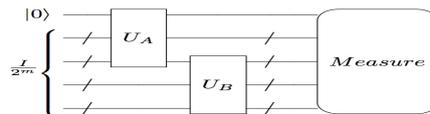
Figure 10 One-round one-clean-qubit protocol.

Note that this type of protocol is semi-unclocked by definition.

We show an upper bound in terms of the weakly unbounded-error communication complexity.

▶ **Definition 14** (Weakly unbounded-error protocol, PP). *In a weakly unbounded-error (randomized) protocol (PP protocol), the function f is computed correctly with probability greater than $\frac{1}{2}$ by a classical private coin protocol. The cost of the protocol with a maximum error (over all inputs) of $\frac{1}{2} - \epsilon$ and a maximum communication of c, is given by $PP(f) = c - \lfloor \log \epsilon \rfloor$. [17]*

We show the following theorem for the upper bound on the communication complexity of the one-clean-qubit one-way protocols (in the appendix):

▶ **Theorem 15.** $Q_{[1]}^{A \to B}(f) \leqslant 2^{O(PP(f))}$.

6.2 The Lower Bound on $Q_{[1]}^{A \to B}(f)$

▶ **Theorem 16.** *For all $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ we have $Q_{[1]}^{A \to B}(f) \geqslant 2^{\Omega(PP(f)) - O(\log n)}$.*

The proof relies only on the fact that an efficient one-way one-clean-qubit protocol needs to achieve a large enough bias. The communication needed to do so is immaterial for our lower bound, which is quite interesting. In other words, there is a threshold to the bias which simply cannot be passed even if we allow more qubits to be sent. This is in sharp contrast to many common modes of communication with error.

The bound on the achievable bias comes from margin complexity, an important concept in learning theory [25].

Before we delve into the proof we need a few definitions. We define the notion of rectangles and two complexity measures: discrepancy and margin complexity.

▶ **Definition 17** (Rectangle [24]). *A rectangle in $X \times Y$ is a subset $R \subseteq X \times Y$ such that $R = A \times B$ for some $A \subseteq X$ and $B \subseteq Y$.*

▶ **Definition 18** (Communication matrix [24]). *The communication matrix M_f of a function $f : X \times Y \to \{0,1\}$ is an $(|X| \times |Y|)$-dimensional matrix, whose rows are indexed by the elements of X and the columns by the elements of Y. The (x, y) entry of M_f is simply defined as $f(x, y)$.*

▶ **Definition 19** (Discrepancy [24]). *Let $f : X \times Y \to \{0,1\}$ be a function, R be any rectangle in the communication matrix, and μ be a probability distribution on $X \times Y$. The discrepancy of f according to μ is*

$$disc_\mu(f) = \max_R |\Pr_\mu[f(x, y) = 0 \text{ and } (x, y) \in R] - \Pr_\mu[f(x, y) = 1 \text{ and } (x, y) \in R]|.$$

Denote $disc(f) = \min_\mu disc_\mu(f)$ as the discrepancy of f over all distributions μ on $X \times Y$.

It is known that $PP(f) \geqslant \Omega(\log(\frac{1}{disc(f)}))$ from Fact 2.8 in [17], and from Theorem 8.1 in [17] we get $PP(f) \leqslant O(\log(\frac{1}{disc(f)})) + \log n)$.

▶ **Definition 20** (Margin [25]). *For a function $f : X \times Y \to \{0,1\}$, let M_f denote the sign matrix where all entries are $M_f(x, y) = (-1)^{f(x,y)}$. The margin of M_f is given by:*

$$m(M_f) = \sup_{\{a_x\}, \{b_y\}} \min_{x,y} \frac{|\langle a_x | b_y \rangle|}{||a_x||_2 ||b_y||_2},$$

where the supremum is over all systems of vectors (of any length) $\{a_x\}_{x \in X}, \{b_y\}_{y \in Y}$ such that $sign(\langle a_x | b_y \rangle) = M_f(x, y)$ for all x, y.

The notion of margin complexity determines the extent to which a given class of functions can be learned by large margin classifiers, which is an important class of machine learning algorithms [25].

The proof of Theorem 16 is in the appendix.

7   The Trivial Lower Bound on $Q_{[1]}(f)$

The lower bound on the two-way one-clean-qubit communication complexity $Q_{[1]}(f) \geqslant \Omega(Q(f))$ is trivial since one-clean-qubit protocols can be turned into standard quantum protocols at their cost. In Appendix C we discuss this lower bound for some well-known functions.

8   Hardness of Classically Simulating the One-Clean-Qubit Model

We now turn to *simulations* of quantum protocols with the one-clean-qubit restriction by randomized protocols. The most demanding definition of simulating a quantum protocol by a randomized protocol is that the randomized protocol must replicate the acceptance probabilities of a given quantum protocol on all inputs, up to some additive error[1].

Our weaker (one-sided) definition of an ϵ-error simulation is:

▶ **Definition 21** (ϵ-error simulation of a quantum protocol). *Given a quantum protocol $\mathcal{P}$ for a function $f : X \times Y \to \{0, 1\}$ such that for all inputs $(x, y) \in X \times Y$, $\mathcal{P}$ accepts 1-inputs with probability at least α and accepts 0-inputs with probability at most β. A classical simulation of $\mathcal{P}$ with additive error of ϵ is one that accepts 1-inputs with probability at least $\alpha - \epsilon$ and accepts 0-inputs with probability at most $\beta + \epsilon$.*

▶ **Remark 22.** The above definition is nontrivial only if $\alpha - \epsilon > \beta + \epsilon$.

8.1   Simulating the One-Clean-Qubit Model with Polynomially Small Additive Error

We show the following lemma (see the appendix):

▶ **Lemma 23.** *Given any two-round (Alice $\to$ Bob $\to$ Alice) k-clean-qubit quantum protocol (with communication $2k$ and where both messages contain only the k clean qubits) for a function f that accepts 0-inputs with probability at most q and accepts 1-inputs with probability at least p, there exists a two-round one-clean qubit protocol (with communication $2k$) for the same function that accepts 0-inputs with probability at most $\frac{q}{2^k}$ and accepts 1-inputs with probability at least $\frac{p}{2^k}$.*

▶ **Theorem 24.** *In communication complexity, there exists a function $f : \{0, 1\}^n \times \{0, 1\}^n \to \{0, 1\}$ and a one-clean-qubit quantum protocol $\mathcal{P}$ with communication $O(\log n)$ such that simulating $\mathcal{P}$ classically with an allowance of $\frac{1}{n^4}$ additive error requires $\Theta(n)$ communication.*

Proof. Consider the function below:

$$MIDDLE(x, y) = 0 \Leftrightarrow \sum_i x_i y_i = \frac{n}{2}, \ MIDDLE(x, y) = 1 \Leftrightarrow \sum_i x_i y_i \neq \frac{n}{2},$$

---

[1] We only consider additive error.

where $x, y \in \{0, 1\}^n$. With Lemma 23 in mind, we design a standard quantum protocol first. We would like to compute the state $\frac{1}{\sqrt{n}} \sum_{i=1}^{n} (-1)^{x_i y_i} |i\rangle$. This can be done by executing the following quantum protocol $\mathcal{P}$:

1. Alice prepares the state $\frac{1}{\sqrt{n}} \sum_{i=1}^{n} |i\rangle |x_i\rangle$ and sends it to Bob.
2. Bob applies his unitary, which maps the state he received from Alice to $\frac{1}{\sqrt{n}} \sum_{i=1}^{n} (-1)^{x_i y_i} |i\rangle |x_i\rangle$ and sends the result to Alice.
3. Alice XORs the last qubit with x_i and then traces out that qubit to obtain $\frac{1}{\sqrt{n}} \sum_{i=1}^{n} (-1)^{x_i y_i} |i\rangle$, applies a Hadamard transformation and does a complete measurement in the computational basis. The protocol outputs 1 if it measures the all-zero string and outputs 0 otherwise.

This protocol requires $2 \log n + 2$ communication and uses $\log n + 1$ clean qubits. Finally, we transform the above protocol into a one-clean-qubit protocol according to Lemma 23.

Now we compute the acceptance probabilities of the standard quantum protocol above. Note that $\langle \cdot | \cdot \rangle$ denotes the inner product.

$$\langle H(\frac{1}{\sqrt{n}} \sum_{i=1}^{n} |i\rangle (-1)^{x_i y_i}) | |00 \cdots 0\rangle\rangle = \langle \frac{1}{\sqrt{n}} \sum_{i=1}^{n} |i\rangle (-1)^{x_i y_i} | H(|00 \cdots 0\rangle)\rangle$$

$$= \langle \frac{1}{\sqrt{n}} \sum_{i=1}^{n} |i\rangle (-1)^{x_i y_i} | \frac{1}{\sqrt{n}} \sum_{i=1}^{n} |i\rangle\rangle. \tag{2}$$

For the case where $\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i = \frac{n}{2}$, we have $\frac{n}{2}$ 0's and $\frac{n}{2}$ 1's among the $x_i y_i$ and hence, (2) for this case equals to zero, which implies that the protocol rejects 0-inputs with certainty.

For the case where $\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i = \frac{n}{2} + t$, we have $\frac{n}{2} - t$ 0's and $\frac{n}{2} + t$ 1's and hence, the amplitude from (2) is $\frac{1}{\sqrt{n}} \cdot \left(\frac{n}{2} + t - \left(\frac{n}{2} - t \right) \right) \frac{1}{\sqrt{n}} = \frac{2t}{n}$, which implies an acceptance probability of $(\frac{2t}{n})^2 = \frac{4t^2}{n^2}$.

Notice that the gap between 0- and 1-inputs is $\frac{4t^2}{n^2}$. Now, simulating $\mathcal{P}$ using only one clean qubit does not change the communication but reduces the acceptance probability of 1-inputs from $\frac{4t^2}{n^2}$ to $\frac{2t^2}{n^3}$ and does not change the acceptance probability of 0-inputs. The gap between the acceptance probability of 0-inputs and 1-inputs is now $\frac{2t^2}{n^3} - 0 = \frac{2t^2}{n^3}$.

We will focus on the 1-inputs with $t = -1$.

We then show that classically simulating the one-clean-qubit protocol with $\frac{1}{n^4}$ additive error for the function $MIDDLE(x, y)$ requires $\Omega(n)$ communication. For this, we use Razborov's analysis of the rectangle bound for the Disjointness problem[32] together with a reduction and the fact that the rectangle bound is not sensitive to acceptance probabilities being small. This shows that any classical protocol that simulates the above quantum protocol within additive error $1/n^4$ needs communication $\Omega(n)$. Details are in Appendix E. ◄

8.2 Simulating the One-Clean-Qubit Model with Constant Additive Error

Previous results about the hardness of simulating the one-clean-qubit model (in circuit complexity) require the additive simulation error to be exponentially small. In the previous subsection we have shown that in communication complexity additive error $1/poly(n)$ is already enough to give a separation (which is also not based on unproven assumptions). Here we consider pushing this even further: can the one-clean-qubit model be simulated classically with constant additive error?

Showing hardness of a classical simulation with constant additive error is equivalent to showing a separation between $Q_{[1]}(f)$ and $R(f)$: regarding both complexity measures efficient error reduction is possible[2]. And showing hardness of a simulation of a quantum protocol for f within a small constant error means showing $R(f)$ is large.

The strength of the one-clean-qubit model is trace-estimation. Any communication-like unitary can have its trace estimated by a quantum protocol with only one clean qubit (compare the proof of Theorem 8). So we look for a hard problem along those lines. A two-party one-way quantum protocol is not a good choice, since the trace of the product of unitaries applied by Alice and Bob is a vector inner product and can be estimated well by known randomized protocols with small error, if the gap of acceptance between one-inputs and zero-inputs is large [23].

For technical reasons (cyclic property of matrix trace), looking for the simplest problem that should exhibit a separation we consider the three-player number-in-hand model[3].

We conjecture the following:

▶ **Conjecture 25.** *There exists a function f and a one-clean-qubit quantum protocol $\mathcal{P}$ that computes f exactly with communication $O(\log n)$ such that simulating $\mathcal{P}$ classically with an allowance of constant additive error requires $\Omega(\sqrt{n})$ communication.*

Consider the number-in-hand ABC (promise) problem involving three parties: Alice, Bob and Charlie, who are each given $n \times n$ matrices A, B and C respectively, where $A, B, C \in SO_n$, where SO_n is the special orthogonal group. The ABC problem is described by the following function:

$$ABC(A, B, C) = 1 \iff ABC = I, \quad ABC(A, B, C) = 0 \iff ABC = -I.$$

▶ **Lemma 26.** *There exists a three-player number-in-hand one-clean-qubit protocol that solves ABC exactly with communication $O(\log n)$.*

Proof. The initial state starts off with one qubit in a pure state $|0\rangle$ and $\log n$ totally mixed qubits. The protocol goes as follows:

1. Alice applies a Hadamard transformation to the clean qubit and obtains $\sigma = H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. She then tensors it with an arbitrary state ρ on $\log n$ qubits (for example $\frac{I}{n}$) and we denote the resulting state as ζ. She then applies her controlled-A unitary to ζ and gets ζ'. Alice send ζ' to Bob.
2. Bob applies his controlled-B unitary to ζ' and gets ζ''. Bob sends ζ'' to Charlie.
3. Charlie applies his controlled-C unitary to ζ'' and gets ζ'''. He then applies a Hadamard transformation to the first qubit in ζ''' and does a measurement.

The protocol is illustrated in Figure 11.
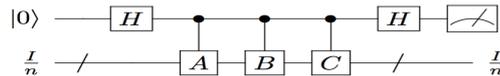
Figure 11 One-clean-qubit protocol for ABC.

If $ABC = I$, the composite of controlled A, B and C is the same as that of a controlled-identity unitary, which does nothing to σ. When σ undergoes a Hadamard transformation before being measured, it becomes the $|0\rangle$ state. The protocol outputs 1 if it measures $|0\rangle$. If $ABC = -I$, the composite of controlled A, B and C is similar to that of a controlled-Z unitary, which does a phase flip on $|1\rangle$ in σ, changing it into $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. We denote the phase-flipped σ as σ'. When σ' undergoes a Hadamard transformation before being measured, it becomes the $|1\rangle$ state. The protocol outputs 0 if it measures $|1\rangle$. ◄

Note that the quantum protocol uses the arbitrary state ρ (here $\rho = I/n$) as a catalyst as in [8]. Regarding the randomized complexity of ABC, we prove the following theorem:

▶ **Theorem 27.** $R(ABC) \leqslant O(\sqrt{n})$.

See the full version [18] for the proof.

Let us note here that with minor modifications, both the quantum and classical protocols for ABC are one-way and can be run in any order among the players, e.g. Charlie to Alice to Bob or Alice to Charlie to Bob.

It remains an open problem to derive a matching lower bound for the randomized communication complexity of ABC.

▶ **Conjecture 28.** $R(ABC) \geqslant \Omega(\sqrt{n})$ *as long as n is even.*

We now consider a geometric conjecture that implies Conjecture 28. This conjecture says that if we take two sufficiently large subsets of SO_n (the special orthogonal group), choose two operators independently from them, and multiply them, we get something similar to the uniform distribution on all of SO_n.

▶ **Conjecture 29.** *There are constants $\delta > 0, \gamma > 1$ such that the following is true:*
Let $M, R \subseteq SO_n$ and, for the Haar measure μ on SO_n, let $\mu(M), \mu(R) \geqslant 2^{-\delta\sqrt{n}}$. Denote by τ the density function of the probability distribution that arises, when $B \in M$ and $C \in R$ are chosen uniformly from these sets independently, and the matrix product BC is formed. Then $Prob_{A \in SO_n}(\tau(A) \notin [1/\gamma, \gamma]) \leqslant 2^{-\delta\sqrt{n}}$.

Conjecture 28 follows from Conjecture 29 by an application of the rectangle bound from communication complexity: A large rectangle/box $L \times M \times R$, where $L, M, R \subseteq SO_n$ leads to a τ that is similar to the uniform distribution. Only an exponentially small subset of matrices $A \in SO_n$ has $\tau(A)$ not constant. This also implies that $E_{A \in L}\tau(A) = \Theta(1)$, if we throw out the small subset of $A \in L$ where $\tau(A)$ is too large (this does not affect size or error much.) Denote by β_C the density function of the distribution where a random $B \in M$ is multiplied to a fixed C. $\tau(A) = E_{C \in R}\beta_C(A^*)$.

Define $H = \{(A, B, C) : A, B, C \in SO_n \text{ and } ABC = I\}$ and $G = \{(A, B, C) : A, B, C \in SO_n \text{ and } ABC = -I\}$. It is easy to show that $E_{A \in L}E_{C \in R}[\beta_C(A)] = \frac{\mu(L \times M \times R|H)}{\mu(L \times M \times R)}$. That means that $\mu(L \times M \times R|H)$ and $\mu(L \times M \times R|G)$ differ by at most a constant factor and $L \times M \times R$ has constant error under the distribution that puts weight $1/2$ on each of G, H. Hence the rectangle/box $L \times M \times R$ has large error. We use that n is even because otherwise $-I \notin SO_n$. Furthermore in the case of odd n Alice, Bob, and Charlie can simply compute $det(ABC) = det(A)det(B)det(C)$ in order to determine whether $ABC = I$ or $ABC = -I$. This does not work in the case of even n of course.

We also note that the corresponding conjecture is wrong for O_n, since SO_n is a subgroup of measure $1/2$ that serves as a counterexample. Note that SO_n does not have any proper subgroups of size larger than 0.

As weaker conjecture, in which the stated probability is upper bounded by a small constant would be sufficient to give a lower bound on one-way protocols and might be much easier to achieve. We note that in [19] we have recently shown a lower bound for the related aBc problem, in which Alice and Charlie receive vectors from the sphere instead of matrices in a generalized one-way setting. Note that the protocol for Theorem 27 really solves the aBc problem.

9 Conclusion

We investigate a communication complexity model in which all storage consist initially of only one clean qubit plus other qubits that start in the totally mixed state, and where only one projective measurement can be done in the end. Since error reduction is not possible efficiently in this model we define an appropriate complexity measure depending on the bias.

We introduce the notions of clocked protocols with ghosted communication channel and semi-unclocked protocols with fixed communication channel for this model. Efficient simulations of clocked k-clean-qubits protocols by clocked one-clean-qubit protocols as well as simulations of clocked k-clean-qubit protocols by semi-unclocked one-clean-qubit protocols are described. Remarkably, the semi-unclocked model is only less efficient by a logarithmic factor compared to the clocked model.

We study one-way protocols in the model and are able to almost pinpoint their complexity in terms of PP-communication complexity: $2^{\Omega(PP(f))-O(\log n)} \leqslant Q_{[1]}^{A \to B}(f) \leqslant 2^{O(PP(f))}$, implying that functions when computed using the one-clean-qubit model have a cost of at most $2^{O(m)}$, where m is the input length, and that this is tight for some functions (one-way).

Classically simulating a certain one-clean-qubit protocol for the $MIDDLE(x, y)$ problem with $\frac{1}{poly(n)}$ additive error is hard, as a classical simulation with such error requires $\Theta(n)$ communication, compared to the $O(\log n)$ communication of the one-clean-qubit protocol.

We conjecture that classically simulating the one-clean-qubit protocol we give for the three-player number-in-hand ABC problem with constant additive error requires $\Omega(\sqrt{n})$ communication, compare to the $O(\log n)$ communication in the one-clean-qubit protocol. We show the corresponding upper bound on $R(ABC)$.

References

1 S. Aaronson and A. Arkhipov. The computational complexity of linear optics. *Theory of Computing*, 9:143–252, 2013.

2 A. Ambainis. Quantum walk algorithm for element distinctness. *SIAM Journal on Computing*, 37(1):210–239, 2007.

3 A. Ambainis, R. Špalek, and R. de Wolf. A new quantum lower bound method, with applications to direct product theorems and time-space tradeoffs. In *Proceedings of 38th ACM STOC*, pages 618–633, 2006. quant-ph/0511200.

4 L. Babai, P. Frankl, and J. Simon. Complexity classes in communication complexity theory.pdf. In *Proceedings FOCS*, 1986.

5 M. J. Bremner, R. Jozsa, and D. J. Shepherd. Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy. In *Proceedings of the Royal Society A*, volume 467, pages 459–472, 2011.

6 D. J. Brod. The complexity of simulating constant-depth boson sampling. *Physical Review A*, 91(4), 2015.

7 J. Brody, S. Chen, P. A. Papakonstantinou, H. Song, and X. Sun. Space-bounded communication complexity. In *Proceedings of the 4th conference on Innovations in Theoretical Computer Science*, ITCS '13, pages 159–172, 2013.

8 H. Buhrman, R. Cleve, M. Koucký, B. Loff, and F. Speelman. Computing with a full memory: Catalytic space. In *Proceedings of the Forty-sixth Annual ACM Symposium on Theory of Computing*, STOC '14, pages 857–866. ACM, 2014.

9 C. Cade and A. Montanaro. The quantum complexity of computing schatten p-norms, 2017. `arXiv:1706.09279v1`.

10 R. Cleve, W. van Dam, M. Nielsen, and A. Tapp. Quantum entanglement and the communication complexity of the inner product function. In *Proceedings of 1st NASA QCQC conference*, volume 1509 of *Lecture Notes in Computer Science*, pages 61–74. Springer, 1998. `arXiv:quant-ph/9708019`.

11 R. de Wolf. Quantum communication and complexity. *Theoretical Computer Science*, 287:337–353, 2002.

12 K. Fujii, H. Kobayashi, T. Morimae, H. Nishimura, S. Tamate, and S. Tani. Power of quantum computation with few clean qubits. *Proceedings of 43rd International Colloquium on Automata, Languages, and Programming (ICALP 2016)*, pages 13:1–13:14, 2016.

13 R. Jain and H. Klauck. The partition bound for classical communication complexity and query complexity. In *25th Annual Conference on Computational Complexity*, pages 247–258, 2010. `arXiv:0910.4266v2`.

14 R. Jozsa and M. V. den Nest. Classical simulation complexity of extended clifford circuits. *Quantum Information and Computation*, 14(7-8):0633–0648„ 2014.

15 B. Klartag and O. Regev. Quantum one-way communication is exponentially stronger than classical communication. In *Proceedings of 43rd ACM STOC*, 2011.

16 H. Klauck. Quantum and classical communication-space tradeoffs from rectangle bounds. In *FSTTCS 2004: Foundations of Software Technology and Theoretical Computer Science, 24th International Conference*, pages 384–395, 2004.

17 H. Klauck. Lower bounds for quantum communication complexity. *SIAM Journal on Computing*, 37(1):20–46, 2007. Earlier version in FOCS'01. quant-ph/0106160.

18 H. Klauck and D. Lim. The power of one clean qubit in communication complexity. *arXiv*, 2018. `arXiv:1807.07762`.

19 H. Klauck and D. Lim. The *abc* problem and equator sampling renyi divergences. *arXiv*, 2019. `arXiv:1912.11275`.

20 H. Klauck, R. Špalek, and R. de Wolf. Quantum and classical strong direct product theorems and optimal time-space tradeoffs. *SIAM Journal on Computing*, 36(5):1472–1493, 2007. Earlier version in FOCS'04. quant-ph/0402123.

21 E. Knill and R. Laflamme. On the power of one bit of quantum information. *Phys.Rev.Lett.*, 81:5672–5675, 1998. `arXiv:quant-ph/9802037v1`.

22 I. Kremer. Quantum communication. Master's Thesis, 1995.

23 I. Kremer, N. Nisan, and D. Ron. On randomized one-round communication complexity. *Computational Complexity*, 8(1):21–49, 1999. Earlier version in STOC'95. Correction at `http://www.eng.tau.ac.il/~danar/Public/KNR-fix.ps`.

24 E. Kushilevitz and N. Nisan. *Communication Complexity*. CUP, 1997.

25 N. Linial and A. Shraibman. Learning complexity vs communication complexity. *Combinatorics, Probability and Computing*, 18:227–245, 2009.

26 T. Morimae, K. Fujii, and J. F. Fitzsimons. On the hardness of classically simulating the one clean qubit model. *Phys. Rev. Lett.*, 112, 130502, 2014.

27 T. Morimae and T. Koshiba. Classical simulatability of the one clean qubit model, 2014. `arXiv:1405.6840v2`.

28 A. Nayak. Optimal lower bounds for quantum automata and random access codes. In *In Proceedings of 40th IEEE FOCS*, 1999.

29 X. Ni and M. V. den Nest. Commuting quantum circuits: Efficient classical simulations versus hardness results. *Quantum Information and Computation*, 13(1-2):0054–0072, 2013.

30   D. Poulin, R. Blume-Kohout, R. Laflamme, and H. Ollivier. Exponential speed-up with a single bit of quantum information: Testing the quantum butterfly effect. *Phys. Rev. Lett.*, 92, 177906, 2004.

31   D. Poulin, R. Laflamme, G. J. Milburn, and J. P. Paz. Testing integrability with a single bit of quantum information. *Phys. Rev. A*, 68(2):022302–1–022302–6, 2003.

32   A. A. Razborov. On the distributional complexity of disjointness. *Theoret. Comput. Sci.*, 106:385–390, 1992.

33   A. A. Razborov. Quantum communication complexity of symmetric predicates. *Izvestiya: Mathematics*, 67(1):145, 2003.

34   P. W. Shor and S. P. Jordan. Estimating jones polynomials is a complete problem for one clean qubit. *Quantum Information and Computation*, 8:681, 2008. `arXiv:0707.2831v3`.

35   Y. Takahashi, S. Tani, T. Yamazaki, and K. Tanaka. Commuting quantum circuits with few outputs are unlikely to be classically simulatable. *Computing and Combinatorics, 21st International Conference, COCOON 2015*, 9198 of Lecture Notes in Computer Science:223–234, 2015.

36   Y. Takahashi, T. Yamazaki, and K. Tanaka. Hardness of classically simulating quantum circuits with unbounded toffoli and fan-out gates. *Quantum Information and Computation*, 14(13-14):1149–1164, 2014.

37   B. M. Terhal and D. P. DiVincenzo. Adaptive quantum computation, constant depth quantum circuits and arthur-merlin games. *Quantum Information and Computation*, 4(2):134–145, 2004.

38   A. 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, pages 209–213. ACM, 1979.

A   Open Problems

- Prove Conjecture 28 or the weaker version mentioned above that establishes a lower bound for one-way protocols.

- What are some nontrivial lower bounds on $Q_{[1]}(f)$, for instance what are $Q_{[1]}(DISJ)$ and $Q_{[1]}(ViS)$ (Vector in Subspace [15])? We conjecture that $Q_{[1]}(DISJ) = \Omega(n)$ based on the difficulty of trying to compute the function in the one-clean-qubit model. Suppose that ViS can computed in the one-clean-qubit communication model efficiently (say with $poly(\log)$ communication), then arbitrary one-way quantum protocols can be simulated with low communication in the one-clean-qubit model. However, we assume that such a supposition seems unlikely and hence we conjecture that $Q_{[1]}(ViS)$ is fairly large, possibly even $Q_{[1]}(ViS) = \Omega(n)$.

- Is $Q_{[1]}(f) > n$ for any function? A candidate for this problem would be a random function chosen from all functions $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. It would be interesting if the one-clean-qubit model can compute all or most $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ with linear cost.

- What are some examples of functions in which $Q_{[1]}(f) >> R(f)$ or $Q_{[1]}(f) << R(f)$? For instance, for the two-player ABC problem, ABC_2, described as follows:

$$ABC_2(A_1, A_2, B_1, B_2) = 1 \Leftrightarrow A_1 B_1 A_2 B_2 = I,$$

$$ABC_2(A_1, A_2, B_1, B_2) = 0 \Leftrightarrow A_1 B_1 A_2 B_2 = -I,$$

where A_1, A_2 are Alice's unitaries and B_1, B_2 are Bob's unitaries, $Q_{[1]}(ABC_2) = O(\log n)$. What is $R(ABC_2)$?

- Are there any specific lower bound methods for the semi-unclocked one-clean-qubit protocol?

B   Proofs Concerning One-Way Protocols

B.1   Proof of Theorem 15

Consider a c-bit PP-communication protocol $\mathcal{P}$ with bias ϵ where Alice sends a message $T(x)$ of length c to Bob[4].

1. We define Alice's unitary U_A^x such that
   - If $z = T(x)$, then $U_A^x : |0\rangle|z_1 \cdots z_c\rangle \mapsto |1\rangle|z_1 \cdots z_c\rangle$
   - If $z \neq T(x)$, then $U_A^x : |0\rangle|z_1 \cdots z_c\rangle \mapsto |0\rangle|z_1 \cdots z_c\rangle$

   and extend to a unitary in any possible way, for all $z \in \{0,1\}^c$. Alice applies U_A^x to the initial state, and computes $U_A^x(|0\rangle\langle 0| \otimes \frac{I}{2^c})U_A^{x\dagger}$.

2. Alice then sends the result σ to Bob. This requires $c + 1$ qubits of communication.

3. Upon receiving σ from Alice, Bob tensors it with $\frac{I}{2}$ and obtains the state $\sigma \otimes \frac{I}{2}$. Bob then applies the unitary V_B^y to the state $\sigma \otimes \frac{I}{2}$, in particular, $V_B^y(\sigma \otimes \frac{I}{2})V_B^{y*}$, as follows

$$V_B^y : \begin{cases} |0\rangle|z_1 \cdots z_{c+1}\rangle \mapsto |0\rangle|z_{c+1}\rangle|z_1 \cdots\ z_c\rangle \\ |1\rangle|z_1 \cdots z_{c+1}\rangle \mapsto |1\rangle U_B^y \otimes I\, |z_1 \cdots z_{c+1}\rangle, \end{cases}$$

   for all $z \in \{0,1\}^{c+1}$. That is to say, if the first qubit of $\sigma \otimes \frac{I}{2}$ is 1, V_B^y will apply the protocol unitary U_B^y. Otherwise, a "coin toss" is done by flipping the last qubit over to the second position.

4. Lastly, he does the measurement on the second qubit.

The probability of the correct message is $\frac{1}{2^c}$. With a protocol of bias ϵ (and hence and error of $\frac{1}{2} - \epsilon$), the acceptance probability of the message is $\frac{1}{2^c}(\frac{1}{2} + \epsilon)$. On the other hand, the acceptance probability of the message in the "coin toss" is given by $\frac{1}{2}(1 - \frac{1}{2^c})$. Therefore, we have the total acceptance probability:

$$\begin{aligned} (1 - \frac{1}{2^c})\frac{1}{2} + \frac{1}{2^c}(\frac{1}{2} + \epsilon) &= \frac{1}{2} - \frac{1}{2^{c+1}} + \frac{1}{2^{c+1}} + \frac{\epsilon}{2^c} \\ &= \frac{1}{2} + \frac{\epsilon}{2^c} \end{aligned} \tag{3}$$

The total cost of the protocol is bounded as follows:

$$Q_{[1]}^{A \to B}(f) \leqslant (c + 1) \cdot \frac{1}{\epsilon'^2} = (c + 1) \cdot 2^{2c} \cdot \frac{1}{\epsilon^2} \leqslant 2^{2PP(f)} \cdot (PP(f) + 1) \leqslant 2^{O(PP(f))}, \tag{4}$$

where $\epsilon' = \frac{\epsilon}{2^c}$ from (3).

B.2   Proof of Theorem 16

Proof. Assume that the protocol measures the first qubit in the computational basis (if not, then a similar construction as in Theorem 8 can be used to make this true). The probability of measuring zero is given by $\frac{1}{2} + \frac{tr(I_A \otimes U_B^y \cdot U_A^x \otimes I_B)}{2^{m+1}}$ [34], where m is the total number of qubits involved and the bias is the term $\frac{tr(I_A \otimes U_B^y \cdot U_A^x \otimes I_B)}{2^{m+1}}$. Note that I_A and I_B act on the private qubits of Alice and Bob respectively. Let $U_A^x \otimes I_B = A_x$ and $I_A \otimes U_B^y = B_y$, and it follows that

$$\frac{tr(I_A \otimes U_B^y \cdot U_A^x \otimes I_B)}{2^{m+1}} = \frac{tr(B_y A_x)}{2^{m+1}} = \frac{\langle b_y | a_x^T \rangle}{2^{m+1}} = \frac{\langle b_y | a_x^T \rangle}{2||a_x||_2||b_y||_2},$$

---

where a_x and b_y are the matrices A_x and B_y viewed as vectors, since A_x and B_y are unitary and hence $||a_x||_2 = ||b_y||_2 = 2^{\frac{m}{2}}$. If the protocol has bias ϵ, then $\frac{\langle b_y|a_x^T\rangle}{2^{m+1}} \geqslant \epsilon$ for $f(x,y) = 1$ and $\frac{\langle b_y|a_x^T\rangle}{2^{m+1}} \leqslant -\epsilon$ for $f(x,y) = 0$.

▶ **Remark 30.** The size of the unitary matrices does not matter, which is good, since there can be an arbitrarily number of private qubits used by the players but never communicated.

We know from the above that the best possible bias satisfies $2\epsilon \leqslant m(f)$. From Theorem 3.1 in [25] which states that $disc(A) = \Theta(m(A))$, and from Theorem 8.1 in [17], which states that $PP(f) \leqslant O(-\log disc(f) + \log n)$ we have

$$Q_{[1]}^{A\rightarrow B}(f) \geqslant \frac{4}{m^2(f)} \geqslant 2^{\Omega(PP(f))-O(\log n)}.$$ ◀

▶ **Remark 31.** This lower bound holds regardless of how much communication is involved: it follows from the fact that one-way one-clean qubit protocols cannot achieve a better bias.

C The Trivial Lower Bound

$Q(f)$ for some functions is given as below [22, 33, 10, 11, 28]:

- The equality function (EQ) defined as

$$EQ(x,y) = 1 \iff x = y \quad , \quad EQ(x,y) = 0 \iff x \neq y,$$

  where $x, y \in \{0,1\}^n$, has $Q(EQ) = \Theta(\log n)$.
  Note: No public coin or entanglement.
- The disjointness function (DISJ) defined as

$$DISJ(x,y) = 1 \iff x \cap y = \varnothing \quad , \quad DISJ(x,y) = 0 \iff x \cap y \neq \varnothing,$$

  where $x, y \in \{0,1\}^n$, has $Q(DISJ) = \Theta(\sqrt{n})$.
  Note: $\Omega(\sqrt{n}) \leqslant Q_{[1]}(DISJ) \leqslant O(n)$.
- The inner product modulo two function (IP_2) defined as

$$IP_2(x,y) = \sum_i x_i y_i \mod 2,$$

  where $x, y \in \{0,1\}^n$, has $Q(IP_2) = \Theta(n)$.
  Note: $Q_{[1]}^{A\rightarrow B}(IP_2) = 2^{\Theta(n)}$ while $Q_{[1]}(IP_2) = \Theta(n)$.
- The vector in subspace function (ViS) defined as

$$ViS(v, H_0) = 1 \iff v \in H_0 \quad , \quad ViS(v, H_0) = 0 \iff v \in H_0^\perp,$$

  where $v \in \mathbb{R}^n$ and $H_0 \subseteq \mathbb{R}^n$ is a subspace with dimension $\frac{n}{2}$, has $Q(ViS) = \Theta(\log n)$.
- The index function (INDEX) defined as

$$INDEX(x,i) = x_i,$$

  where $x \in \{0,1\}^n$ and $1 \leqslant i \leqslant n$ has $Q(INDEX) = \Theta(\log n)$.

$Q_{[1]}(EQ)$, $Q_{[1]}(ViS)$ and $Q_{[1]}(INDEX)$ are basically unknown: the lower bounds we know are $\Omega(\log n)$, but the upper bounds we have are $O(n)$ for $INDEX$ and EQ, while Theorem 7 implies $Q_{[1]}(ViS) = O(n^2 \log n)$.

D Proof of Lemma 23

In the quantum protocol, Alice prepares the first message $|\phi_x\rangle$ by applying a protocol unitary $W_x^{(1)}$ to the all-zero state on the k clean qubits, and sends it to Bob. Bob then applies the protocol unitary $V_y'^{(1)}$ to the message sent by Alice and sends the result back to her. Alice then applies her second unitary $W_x'^{(2)}$ and does a measurement. This protocol has communication $2k$ and accepts 0-inputs with probability at most q and accepts 1-inputs with probability at least p, where $p > q$.

Given any state $|\phi_x\rangle$, we can find an orthonormal basis $\beta_x = \{|\beta_1\rangle \cdots |\beta_{2^k}\rangle\}$ that includes $|\phi_x\rangle$ so that $|\phi_x\rangle$ is a member of the basis and $\sum_{i=1}^{2^k} \frac{|\beta_i\rangle\langle\beta_i|}{2^k} = \frac{I}{2^k}$, such that the state $I/2^k$ is the uniform distribution on the elements in the basis. Consider a one-clean-qubit protocol that simulates the above quantum protocol and goes as follows:

1. We define Alice's unitary $W_x'^{(1)}$ such that
   - If $|\beta_i\rangle = |\phi_x\rangle$, then $W_x'^{(1)} : |0\rangle|\beta_i\rangle \mapsto |1\rangle|\beta_i\rangle$
   - If $|\beta_i\rangle \neq |\phi_x\rangle$, then $W_x'^{(1)} : |0\rangle|\beta_i\rangle \mapsto |0\rangle|\beta_i\rangle$

   and extend to a unitary in any possible way.

   where $|\beta_i\rangle \in \beta_x$. Alice applies $W_x'^{(1)}$ to the initial state, in particular, computes $\sigma_x = W_x'^{(1)}(|0\rangle\langle 0| \otimes \frac{I}{2^c})W_x'^{(1)\dagger}$.

2. Alice then sends the last k qubits to Bob.

3. Bob applies the unitary $V_y'^{(1)}$ to the qubits he received from Alice, in particular computes $\sigma_y = I \otimes V_y'^{(1)}(\sigma_x)I \otimes V_y'^{(1)\dagger}$, where $\dim(I)=2$. Bob sends the qubits back to Alice.

4. Alice applies her unitary $W_x'^{(2)}$ (tensored with identity on the first qubit) to σ_y and measures the first qubit. She outputs 0 if she obtains a measurement result of $|0\rangle$. On the other hand, if she obtains a measurement of $|1\rangle$, she proceeds to execute the measurement of the original quantum protocol. In this case, the acceptance probability of 0-inputs is at most $\frac{q}{2^k}$ and the acceptance probability for 1-inputs is at least $\frac{p}{2^k}$. Note that the two measurements can be combined into one.

The simulation of a k-clean-qubit quantum protocol by a one-clean-qubit protocol is shown in Figure 12:
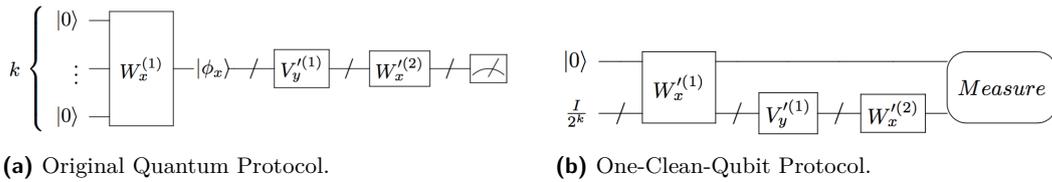

(a) Original Quantum Protocol.

(b) One-Clean-Qubit Protocol.

Figure 12 Simulation by a one-clean-qubit protocol.

E The Simulation Lower Bound

First, we insert dummies into the first $\frac{n}{2} - 1$ entries of each string (set all to 1) and the remaining entries are drawn according to a distribution defined in [32].

Consider the linear program (LP) for the rectangle bound (see [13]) as follows, where we set the acceptance probability for 1-inputs to be at least $\alpha = \frac{1}{n^3}$. We consider an additive error of $\frac{1}{n^4}$ and the simulation is required to accept 0-inputs with probability at most $\frac{1}{n^4}$ and accept 1-inputs with probability at least $\frac{2}{n^3} - \frac{1}{n^4} \geqslant \frac{1}{n^3} = \alpha$. Recall that we consider as 1-inputs only those x, y with $\sum_i x_i y_i = \frac{n}{2} - 1$, and as 0-inputs those with $\sum_i x_i y_i = \frac{n}{2}$.

Denote by $\mathcal{R}$ the set of all rectangles in the communication matrix.

<u>Primal</u>

$$
\begin{aligned}
\text{minimize} \quad & \sum_{R \in \mathcal{R}} W_R \\
\text{subject to} \quad & \sum_{\{R \in \mathcal{R} \mid x,y \in R\}} W_R \geqslant \alpha, && \text{for all } x, y : \sum_i x_i y_i = \tfrac{n}{2} - 1 \\
& \sum_{\{R \in \mathcal{R} \mid x,y \in R\}} -W_R \geqslant -\tfrac{1}{n^4}, && \text{for all } x, y : \sum_i x_i y_i = \tfrac{n}{2} \\
& W_R \geqslant 0
\end{aligned}
$$

<u>Dual</u>

$$
\begin{aligned}
\text{maximize} \quad & \sum_{\{x,y \mid \sum_i x_i y_i = \frac{n}{2} - 1\}} \alpha \gamma_{xy} - \sum_{\{x,y \mid \sum_i x_i y_i = \frac{n}{2}\}} \frac{1}{n^4} \sigma_{xy} \\
\text{subject to} \quad & \sum_{\{x,y \in R \mid \sum_i x_i y_i = \frac{n}{2} - 1\}} \gamma_{xy} - \sum_{\{x,y \in R \mid \sum_i x_i y_i = \frac{n}{2}\}} \sigma_{xy} \leqslant 1 \quad \text{for all } R \in \mathcal{R} \\
& \sigma_{xy}, \gamma_{x,y} \geqslant 0
\end{aligned}
$$

A protocol $\mathcal{P}$ that accepts 1-inputs with probability at least $\frac{1}{n^3}$ and accepts 0-inputs with probability at most $\frac{1}{n^4}$ can be viewed as a probability distribution on deterministic protocols. Each deterministic protocol (in a randomized public-coin protocol) can be represented by a protocol tree. The probabilities of decision trees are given as $p_1, p_2, \ldots, p_t$. Every leaf in each decision tree has an attached rectangle, and a decision: accept or reject. We consider only the rectangles which lead to acceptance, and we assign weight 0 to those rectangles that do not appear in any protocol tree at an accepting leaf and weight $W_R = \sum\limits_{\{i \mid R \text{ accepted in tree } i\}} p_i$

for rectangles appearing in protocol trees i.

▷ **Claim 32.** The constraints in the primal LP hold.

Proof.
- Let (x, y) be a 1-input. Summing up all the probabilities of the decision trees where (x, y) is in a 1-rectangle, we get the LHS of the first inequality constraint, which also corresponds to the acceptance probability, which must exceed α on the RHS.
- Let (x, y) be a 0-input. Adding up the probabilities of decision trees where (x, y) appears in a 1-rectangle will give the LHS of the second inequality constraints, which is at most $1/n^4$ because that is the maximum additive error allowed.
- The nonnegativity constraint is automatically fulfilled since W_R's are sums of probabilities which must be at least zero.   ◁

▷ **Claim 33.** If there is a classical protocol that accepts 1-inputs with probability $\geqslant \alpha$ and 0-inputs with probability $\leqslant 1/n^4$ and communication c then there exists a solution of cost 2^c for the primal LP.

Proof. The contribution of each decision tree to W_R is at most $2^c \cdot p_i$, since there are at most 2^c leaves in each decision tree. Therefore,

$$
\sum_{R \in \mathcal{R}} W_R \leqslant \sum_{i=1}^{t} 2^c \cdot p_i = 2^c. \qquad\qquad ◁
$$

Therefore, in a $\frac{1}{n^4}$-error simulation of a quantum protocol (that accepts 1-inputs with probability at least $\frac{2}{n^3}$ and accepts 0-inputs with probability 0), the simulating randomized protocol (with communication c) must accept 1-inputs with probability at least $\frac{2}{n^3} - \frac{1}{n^4} \geqslant \frac{1}{n^3}$ and accept 0-inputs with probability at most $\frac{1}{n^4}$, and hence yield a solution to the primal LP of cost at most 2^c. By LP duality the primal and its dual have the same cost, and we want to show the lower bound for the cost. Hence, we work with the dual.

▷ **Claim 34.** The cost of the LP is $2^{\Omega(n)}$.

See the full version [18] for the proof.