Two-Party Direct-Sum Questions Through the Lens of Multiparty Communication Complexity*

Itay Hazan[1] and Eyal Kushilevitz[2]

1 Department of Computer Science, Technion – Israel Institute of Technology, Haifa, Israel
itay.hzn@gmail.com

2 Department of Computer Science, Technion – Israel Institute of Technology, Haifa, Israel
eyalk@cs.technion.ac.il

Abstract

Direct-sum questions in (two-party) communication complexity ask whether two parties, Alice and Bob, can compute the value of a function f on ℓ inputs $(x_1, y_1), \ldots, (x_\ell, y_\ell)$ more efficiently than by applying the best protocol for f, independently on each input (x_i, y_i). In spite of significant efforts to understand these questions (under various communication-complexity measures), the general question is still far from being well understood.

In this paper, we offer a multiparty view of these questions: The direct-sum setting is just a two-player system with Alice having inputs $x_1, \ldots, x_\ell$, Bob having inputs $y_1, \ldots, y_\ell$ and the desired output is $f(x_1, y_1), \ldots, f(x_\ell, y_\ell)$. The naive solution of solving the ℓ problems independently, is modeled by a network with ℓ (disconnected) pairs of players Alice$_i$ and Bob$_i$, with inputs x_i, y_i respectively, and communication only within each pair. Then, we consider an intermediate ("star") model, where there is one Alice having ℓ inputs $x_1, \ldots, x_\ell$ and ℓ players Bob$_1, \ldots,$Bob$_\ell$ holding $y_1, \ldots, y_\ell$, respectively (in fact, we consider few variants of this intermediate model, depending on whether communication between each Bob$_i$ and Alice is point-to-point or whether we allow broadcast). Our goal is to get a better understanding of the relation between the two extreme models (i.e., of the two-party direct-sum question). If, for instance, Alice and Bob can do better (for some complexity measure) than solving the ℓ problems independently, we wish to understand what intermediate model already allows to do so (hereby understanding the "source" of such savings). If, on the other hand, we wish to prove that there is no better solution than solving the ℓ problems independently, then our approach gives a way of breaking the task of proving such a statement into few (hopefully, easier) steps.

We present several results of both types. Namely, for certain complexity measures, communication problems f and certain pairs of models, we can show gaps between the complexity of solving f on ℓ instances in the two models in question; while, for certain other complexity measures and pairs of models, we can show that such gaps do not exist (for any communication problem f). For example, we prove that if only point-to-point communication is allowed in the intermediate "star" model, then significant savings are impossible in the public-coin randomized setting. On the other hand, in the private-coin randomized setting, if Alice is allowed to broadcast messages to all Bobs in the "star" network, then some savings are possible. While this approach does not lead yet to new results on the original two-party direct-sum question, we believe that our work gives new insights on the already-known direct-sum results, and may potentially lead to more such results in the future.

1998 ACM Subject Classification F.1.3 Complexity Measures and Classes, F.2.2 Nonnumerical Algorithms and Problems

* This work was partially supported by ISF grant 1709/14, BSF grant 2012378, and NSF-BSF grant 2015782.

31st International Symposium on Distributed Computing (DISC 2017).
Editor: Andréa W. Richa; Article No. 26; pp. 26:1–26:15
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Keywords and phrases Communication Complexity, Direct Sum, Multiparty Communication

Digital Object Identifier 10.4230/LIPIcs.DISC.2017.26

1 Introduction

Communication complexity, presented by Yao [27], studies computational problems in a distributed model, where the input is split between two parties or more. The parties exchange messages according to a predetermined protocol in order to solve the computational problem in question, e.g. computing a function on their inputs. The complexity of such protocol is measured by the number of bits exchanged, on the worst possible input. The communication complexity of a problem is the cost of the best protocol that solves it. The literature deals with finding both upper and lower bounds for various computational problems, and various types of protocols (deterministic, randomized, etc). In the two-party model, the most extensively studied model in communication complexity, Alice receives an x and Bob receives a y, both n-bit strings. Together they wish to solve the problem $P(x, y)$. For an overview of communication complexity and some of its applications, see [17].

Direct-sum questions ask whether solving several computational problems simultaneously can be done more efficiently than merely solving each problem separately. The direct sum question in two-party communication complexity, first presented in [16], is the following: suppose that Alice and Bob attempt to solve a computational problem $P(x, y)$, and suppose that the cost of the best protocol for solving it is C. Now suppose Alice and Bob are each given a sequence of ℓ inputs for P, i.e. Alice is given $x_1, \dots, x_\ell$ and Bob is given $y_1, \dots, y_\ell$. Alice and Bob wish to find a solution for each of the instances, namely to compute $P(x_i, y_i)$ for every $i \in \{1, \dots, \ell\}$. Clearly, this can be done by running the best protocol that solves the problem ℓ times, using ℓC bits. However, perhaps Alice and Bob can utilize the fact that they are given all ℓ inputs at once, and solve P on all of them with fewer bits of communication. If this is possible, we say that a *saving* occurs. The question of existence of such savings is the direct-sum question, namely: does any protocol for ℓ inputs encapsulates a protocol for a single input whose cost is at most $1/\ell$ the cost of the original protocol?

1.1 Our Multiparty Models of Communication

In an attempt to achieve a better understanding of the source of hardness of direct-sum questions in the two-party case, we consider several "intermediate" *multiparty* communication models with one Alice and ℓ Bobs, denoted Bob$_1$,…,Bob$_\ell$. Alice receives $x_1, \dots, x_\ell$, and Bob$_i$ receives y_i for every $i \in \{1, \dots, \ell\}$. As in the classical direct sum question, they wish to compute $P(x_i, y_i)$ for every i. In our "intermediate" models, the question is whether a saving can be obtained when one party sees ℓ instances at once, and may send messages that are "global", while each of the other parties sees only one instance and sends messages that rely solely on its instance and its view of the communication.

Specifically, we consider five communication models, to which we refer as M_1 to M_5. The first model, M_1, is the classical two-party direct-sum model, and the last one, M_5, represents ℓ independent computations. Ultimately, the direct-sum question aims towards a better understanding of the connection between M_1 and M_5. In order to do so, M_2, M_3, and M_4 are defined, such that each model presents an additional constraint over the previous model. The definitions and motivations of these models are as follows:

- **The Classical Direct-Sum Model (M_1).** In this model, there are two parties, Alice and Bob. Alice receives an ℓ-tuple of n-bit inputs, $(x_1, \dots, x_\ell) \in (\{0, 1\}^n)^\ell$, and Bob receives another ℓ-tuple of n-bit inputs, $(y_1, \ldots, y_\ell) \in (\{0,1\}^n)^\ell$. Together, they wish to compute $P(x_i, y_i)$ for every $i \in [\ell]$, for some computational problem P.

- **The Broadcast Model (M_2).** In this model, there are $(\ell + 1)$ parties; one Alice and ℓ Bobs, denoted $\text{Bob}_1, \ldots, \text{Bob}_\ell$. Alice receives an ℓ-tuple of n-bit inputs, $(x_1, \ldots, x_\ell) \in (\{0,1\}^n)^\ell$, and each Bob_i receives an n-bit input, $y_i \in \{0,1\}^n$. Together, they wish to compute $P(x_i, y_i)$ for every $i \in [\ell]$, such that when the protocol terminates, Alice knows all ℓ outputs. The communication is by broadcast among all parties; namely, every message sent by any party is received by all other parties.
- **The One-Way Broadcast Model (M_3).** This model is similar to M_2, only that the Bobs cannot hear each other; namely, every message Alice sends is heard by all Bobs, but a message sent by one of the Bobs is received by Alice alone. This model might be thought of as a communication between a satellite and ℓ ground stations – whatever the satellite transmits is heard by all ground stations, but messages from the ground stations are received only by the satellite.
- **The Point-to-Point Model (M_4).** As in M_2, M_3, the underlying setting in this model remains the $(\ell + 1)$-star. However, in this case the communication is point-to-point; namely, every message sent by one of the Bobs is received by Alice alone (i.e. the Bobs cannot send messages to each other), and every message Alice sends is sent to a single Bob of her choice.
- **The Independent Computations Model (M_5).** In this model, there are ℓ Alices and ℓ Bobs. For every $i \in [\ell]$, Alice_i is given $x_i \in \{0,1\}^n$ and Bob_i is given $y_i \in \{0,1\}^n$. They communicate over a point-to-point channel, which none of the other Alices or Bobs can hear, in order to compute $P(x_i, y_i)$. When the computation terminates, Alice_i should know $P(x_i, y_i)$. Since each Alice_i and Bob_i hear no other communication but their own, this model represents ℓ independent computations.

1.2 Previous Work

The direct sum question in communication complexity has been studied extensively, with respect to different types of protocols (e.g. deterministic, nondeterministic, and randomized). In spite of significant efforts it is far from being well understood.

The deterministic case was first studied in [16], where it was shown that if a certain two-party direct-sum result holds, then $\text{NC}^1 \neq \text{NC}^2$ and $\text{NC}^1 \neq \text{P}$. In [10] it is proved that for any (full) boolean function f, $\mathcal{D}(f^\ell) \geq \ell \left(\sqrt{\mathcal{D}(f)/2} - O(\log n) \right)$, while there exists a *partial* function f such that $\mathcal{D}(f) = \log n + 1$ but $\mathcal{D}\left(f^\ell\right) = O(\ell + \log n \log \ell) \ll \ell \cdot D(f)$. A setting in which the number of communication rounds is bounded has also been studied. For example, it was shown in [10, 15] that for one-round and two-round (deterministic) protocols, $\mathcal{D}(f^\ell) \geq \ell\,(\mathcal{D}(f) - O(\log n))$ for any (possibly partial) function f. However, the direct-sum question for *full* functions remains open. Formally stated,

▶ **Question 1.** *Does $\mathcal{D}\left(f^\ell\right) \geq \ell(\mathcal{D}(f) - O(1))$, for every full function f?*

In the case of *randomized* protocols, one may consider several types of randomness. In the *private-coin* setting, each party has a private string of random bits that it can utilize in its computation. In the *public-coin* setting, the string of random bits is public, namely seen by both parties. In [10], a concrete (full) function f that satisfies $\mathcal{R}^{\text{priv}}(f) = O(\log n)$ and $\mathcal{R}^{\text{priv}}\left(f^\ell\right) = O(\ell + \log n)$ was shown, thus demonstrating that savings can be obtained in the private-coin randomized setting.

One might also consider a hybrid of the private and public-coin models, in which each party sees both a private and a public string of random bits. This setting arises naturally when applying information theoretic techniques to communication complexity. Such notions were first introduced in [9] (later redefined in [3]), to measure the amount of *information* that must be revealed by the two parties, about their inputs, in order to solve a communication problem. Informally, since the amount of information revealed by the parties in a protocol is at most the number of bits transmitted throughout its execution, then one can obtain lower bounds on the communication complexity of a function by proving lower bounds on its information complexity. In recent years, *information complexity* became a powerful tool for understanding communication complexity and was used to prove many results, e.g. for reproving a lower bound of $\Omega(n)$ on the communication complexity of the set-disjointness function [2] (originally proved in [14, 23]). In fact, the main theorem in [2] is a direct-sum-like theorem for information complexity. Furthermore, it was shown in [6, 3] that $\mathcal{R}\left(f^{\ell}\right)$ approaches $\ell \cdot \mathrm{IC}\left(f\right)$ as ℓ tends to infinity. Therefore, a two-party direct-sum question in which both public- and private-coin randomization are allowed, can also be stated in terms of compression. Informally stated: given a protocol π, can one construct a "compressed" protocol τ such that $|\tau|$ is roughly equal to the information content of π? This was proven to be false in some settings; in [11, 13], a randomized setting in which the inputs are distributed according to some known distribution was studied, and it was shown that there might be an exponential gap between information and communication complexity in this setting. In [12], a randomized *non-distributional* setting was studied, and it was shown that exponential gaps between information and communication complexity can also be found in this setting, when considering search problems. Nonetheless, the question of compression remains open for *functions* in the randomized *non-distributional* setting.

Our proposed models are intended to naturally relate to the two-party direct-sum problem, and for that reason we require that the same function $f(x, y)$ is computed "on every edge". Contrary to our models, in most previous works, e.g. [8, 4, 5, 1], each of the ℓ parties receives an n-bit input, x_i, and together they compute some "global" function $g(x_1, \ldots, x_\ell)$ rather than a "local" function $f(x, y)$ "on every edge", in our case. To the best of our knowledge, a setting in which a function f is computed "on every edge" was only considered in [22] and [7]. In [22], a direct-sum-like theorem in the randomized case was proved, with respect to some communication complexity measure, denoted $ED^{\epsilon}_{\mu}(f)$ (on which we shall not elaborate), and it was shown that in the message passing model $\mathcal{R}^{\mathrm{pub}}\left(f^{\ell}, \epsilon\right) = \Omega\left(\ell \cdot ED^{\epsilon}_{\mu}(f)\right)$, for any function f and error probability ϵ. In [7], *quantum* nondeterministic multiparty communication complexity was considered, with which we do not deal in this work.

1.3 Our Results

In Section 3, public-coin randomized communication complexity is studied. First, we formalize several notions of randomized and distributional communication complexity in Section 3.1, and prove some useful connections between the different measures we present. Afterwards, in Section 3.2, we prove our main result in the public-coin setting (Theorem 12). It states that solving ℓ instances of a function f in M_4 in the public-coin model costs roughly ℓ times the cost of solving a single instance.

In the full version of the paper, a similar result is shown in the *private-coin* randomized setting, for functions f that satisfy a certain constraint. We also present a function for which there is a gap between M_3 and M_4 in this setting. For *nondeterministic* communication complexity, we prove that M_1, M_2, and M_3 are almost equivalent and that M_4 and M_5 are almost equivalent; this is also omitted here, for lack of space, and included in the full version.

Interestingly, the point-to-point model proved to be hard in both the randomized and nondeterministic settings. These results imply that the fact that Alice must send each Bob a separate message makes practically any savings impossible.

In Section 4, we consider the connections between our five models in a setting where the number of *rounds* is bounded. In particular, for one-round protocols, we show that a saving never occurs when solving a computational problem in either M_3, M_4, or M_5 (Observation 18); that saving never occurs in M_2 in the public-coin randomized setting (Claim 20); and we demonstrate a gap between M_2 and M_3 in the deterministic setting. Finally, in Theorem 25, we show a gap between M_1 and M_2 in the deterministic setting, for some relaxed notion of one-round protocols.

2 Preliminaries

Although most of our results apply to general functions, we focus our discussion on Boolean functions, for simplicity. Thus, unless explicitly stated otherwise, f is a function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. Given such f and a natural non-zero number ℓ, let $f^\ell : \{0,1\}^{n\ell} \times \{0,1\}^{n\ell} \to \{0,1\}^\ell$ denote the following function: for every $(\vec{x}, \vec{y}) = ((x_1, \dots, x_\ell), (y_1, \dots, y_\ell)) \in \{0,1\}^{n\ell} \times \{0,1\}^{n\ell}$, let $f^\ell(\vec{x}, \vec{y}) \triangleq (f(x_1, y_1), \dots, f(x_\ell, y_\ell))$.

Our models, as defined in Section 1.1, aim to naturally relate to the two-party direct-sum question and, hence, throughout this work, we study *asynchronous* protocols whose communication complexity is defined to be the total number of bits sent between the parties. In a protocol π, in all models, the messages each party sends rely solely on its current view of the state of the protocol, i.e. its input (including, possibly, its randomness) and the previous messages it received in the protocol. We further assume that each party knows when it is its turn to speak based on its view of the state of the protocol. Therefore, all messages sent in the protocol are self terminating, e.g. drawn from some prefix code. One may also consider protocols that operate in *synchronous rounds*, as commonly done in the study of distributed computing (see, e.g., [21]). This may seem to be a minor difference but it is, in fact, crucial: In synchronous protocols, parties may exchange information even in rounds in which they do not speak; merely the fact that they remain silent may convey information.

We denote the worst-case communication complexity of π, i.e. the number of bits sent in π on the worst possible input, by $|\pi|$. Given a computational problem P, and a complexity measure $C \in \{\mathcal{D}, \mathcal{N}, \mathcal{R}, \dots\}$ (i.e. Deterministic, Nondeterministic, Randomized, etc.), we denote the communication complexity, with respect to the measure C, of a single instance of P in the two-party model by $C(P)$. Furthermore, given $\ell \geq 1$, we define $C_i(P^\ell)$ to be the communication complexity, w.r.t. the measure C, of computing ℓ instances of P in the model M_i. For example, using this notation, $C_5(P^\ell) = \ell C(P)$.

The models $M_1, \dots, M_5$ were defined such that each model presents an additional constraint over the former models (see Section 1.1). Therefore, intuition suggests that for any $i \in [4]$ and any computational problem P, solving P^ℓ in M_{i+1} is at least as hard as solving it in M_i. This intuition can be easily formalized in a claim that informally states that $C_1 \leq C_2 \leq C_3 \lesssim C_4 \leq C_5$, for any complexity measure C. The formal claim, along with its proof, appear in the full version of the paper.

3 Public-coin Randomized Communication Complexity

In this section, we consider *randomized* communication complexity, in the *public-coin* setting, where the players have access to a common (global) random string. The *private-coin* case, where each player has its own randomness, is deferred, for lack of space, to the full version of the paper.

3.1 Randomized and Distributional Communication Complexity

Several definitions of the randomized and distributional settings, differentiated by the way error is measured, have been considered in the communication complexity literature. This section deals with the various definitions and relates the different measures to one another. The main result of this section, showing that M_4 and M_5 are "close", appears in Subsection 3.2. We note that all the definitions presented hereafter assume ℓ instances for some boolean function f, and the definitions for the two-party setting follow by fixing $\ell = 1$.

▶ **Definition 2** (Public-coin randomized protocols). A protocol π is said to be *public-coin randomized* protocol if at the beginning of every execution of π, each party receives, in addition to its input, the same (public) random string r of unbounded length. Then, the parties communicate according to a predetermined (deterministic) protocol, where the type of communication between the parties is determined by the model in question (i.e. M_1, M_2, M_3, M_4, or M_5). A protocol π is said to compute f^ℓ with ϵ-error if $\Pr_r\left[\pi(\vec{x},\vec{y},r) = f^\ell(\vec{x},\vec{y})\right] \geq 1-\epsilon$ for every $(\vec{x},\vec{y}) \in \{0,1\}^{n\ell} \times \{0,1\}^{n\ell}$. Namely, the error is considered over *all instances simultaneously.* Let $\mathcal{R}_k^{\text{pub}}\left(f^\ell,\epsilon\right)$ denote the cost of the best public-coin randomized protocol that computes f^ℓ with ϵ-error in the model M_k.

▶ **Definition 3** (Distributional protocols). Let ρ be a distribution over $\{0,1\}^{n\ell} \times \{0,1\}^{n\ell}$. A *deterministic* protocol π is said to be (ρ,ϵ)*-distributionally correct* for f^ℓ if it answers correctly on at least a $(1-\epsilon)$-fraction of the inputs, weighted by ρ, i.e. $\Pr_{(\vec{x},\vec{y})\sim\rho}\left[\pi(\vec{x},\vec{y}) = f^\ell(\vec{x},\vec{y})\right] \geq 1-\epsilon$. Let $\mathcal{D}_k^{(\rho,\epsilon)}\left(f^\ell\right)$ denote the cost of the best (ρ,ϵ)-distributional protocol for f^ℓ in M_k.

The following theorem relates the two measures defined above.

▶ **Theorem 4** (Yao's minimax principle). $\mathcal{R}_k^{\text{pub}}\left(f^\ell,\epsilon\right) \geq \mathcal{D}_k^{(\rho,\epsilon)}\left(f^\ell\right)$ *for any distribution ρ over* $\{0,1\}^{n\ell} \times \{0,1\}^{n\ell}$*. Furthermore, if $\ell = 1$, there exists a distribution ρ over* $\{0,1\}^n \times \{0,1\}^n$ *for which* $\mathcal{R}^{\text{pub}}(f,\epsilon) = \mathcal{D}^{(\rho,\epsilon)}(f)$.

Yao's Minimax principle was first proved in [28] for the two-party case, and later generalized for the multiparty case; see, [25, 26]. It relates two settings: in the public-coin randomized setting, error is taken over the choice of randomness, while in the distributional setting, error is taken over the choice of inputs. One may also consider combinations of the two settings, e.g. the *randomized distributional setting* that appears e.g. in [11, 12, 13]. We now define several such measures.

▶ **Definition 5** (Randomized distributional protocols). Let ρ be a distribution over $\{0,1\}^{n\ell} \times \{0,1\}^{n\ell}$. A *public-coin* randomized protocol π is said to be (ρ,ϵ)*-distributionally correct* for f^ℓ in M_k if it produces a correct answer with probability at least $1-\epsilon$, taken over *both* the choice of randomness and the choice of inputs, i.e. $\Pr_{r,(\vec{x},\vec{y})\sim\rho}\left[\pi(\vec{x},\vec{y},r) = f^\ell(\vec{x},\vec{y})\right] \geq 1-\epsilon$. Let $\mathcal{R}_k^\rho\left(f^\ell,\epsilon\right)$ denote the cost of the best public-coin randomized (ρ,ϵ)-distributional protocol for f^ℓ in M_k, and let $\overline{\mathcal{R}}_k^\rho\left(f^\ell,\epsilon\right)$ denote the minimal *expected* cost of any public-coin randomized (ρ,ϵ)-distributional protocol for f^ℓ in M_k, where the expectaion is taken both over the choice of randomness and the choice of input.

Next, we introduce another communication complexity measure for the classical two-party setting – *public-coin randomized communication complexity with (ρ,δ)-promise and ϵ-error.* Although this definition can be easily extended to other communication models, we only need the two-party version for our purposes.

▶ **Definition 6** (Public-coin randomized protocols with (ρ,δ)-promise and ϵ-error). Let ρ be a distribution on $\{0,1\}^n \times \{0,1\}^n$, and let $\epsilon,\delta \in (0,1)$. A public-coin randomized protocol π is said to compute f *with (ρ,δ)-promise and ϵ-error* if:

Protocol 1 $\tau(x, y, r)$.

```
1: Simulation: Alice and Bob simulate $\pi(x, y, r)$.
2: Early termination: If more than $\frac{1}{\delta^2}|\pi|$ bits were sent, Alice and Bob terminate and
   output '0'. Otherwise, Alice answers like $\pi$.
```

1. On a δ-fraction of the inputs, weighted by ρ, there is no correctness promise, i.e. the protocol may always err. These are called *type-A* inputs of π.
2. On any other input, a $(1-\delta)$-fraction weighted by ρ, there is at most ϵ-error, weighted by the choice of the public random string. These are called *type-B* inputs of π.

Let $\mathcal{R}^{(\rho,\delta)}(f, \epsilon)$ denote the cost of the best public-coin randomized protocol that computes f with (ρ, δ)-promise and ϵ-error.

In the rest of this subsection, we discuss the settings defined above, and show how they relate to one another. We start by the following observation:

▶ **Observation 7.** $\mathcal{R}_k^{\rho}(f^{\ell}, \epsilon) \leq \mathcal{R}_k^{\text{pub}}(f^{\ell}, \epsilon)$ *for any* f, ℓ, $\epsilon \in (0, 1)$ *and distribution* ρ.

This is immediate: suppose π is a public-coin randomized protocol that errs with probability at most ϵ on *every* input (over the choice of randomness). Clearly, π errs with probability at most ϵ if the input is also sampled from some distribution ρ.

▶ **Lemma 8.** $\mathcal{R}^{(\rho,\delta)}(f, \epsilon) \geq \mathcal{D}^{(\rho,\delta+\epsilon)}(f)$, *for any* f, $\epsilon, \delta \in (0, 1)$ *and distribution* ρ.

The proof of Lemma 8 is an immediate generalization of the first part of Theorem 4 and is omitted for lack of space. We conclude this subsection with the following lemma:

▶ **Lemma 9.** $\mathcal{R}^{(\rho,\sqrt{\epsilon}+\delta)}(f, \sqrt{\epsilon}+\delta) \leq \frac{1}{\delta^2}\overline{\mathcal{R}}^{\rho}(f, \epsilon)$ *for any* f*, distribution* ρ*, and* $\epsilon, \delta \in (0, 1)$ *that satisfy* $2(\sqrt{\epsilon}+\delta) \leq 1$.

Proof. Let π be an expected (ρ, ϵ)-distributional randomized protocol for f. For every input pair (x, y) and any public random string r, let $I(x, y, r)$ be the following $\{0, 1\}$-indicator: $I(x, y, r) = 1$ if and only if π errs on (x, y) when the random string is r. Furthermore, let $I(x, y) \triangleq \mathop{\mathbb{E}}_{r}[I(x, y, r)]$. Observe that $I(x, y)$ is exactly $\Pr_r[\pi(x, y, r) \neq f(x, y)]$, and since π is a (ρ, ϵ)-distributional randomized protocol for f, then $\mathop{\mathbb{E}}_{(x,y)\sim\rho}[I(x, y)] \leq \epsilon$.

For every (x, y), let $E(x, y) \triangleq \mathop{\mathbb{E}}_{r}[|\pi(x, y, r)|]$ denote the expected communication complexity of π on (x, y), taken over the choice of public randomness r. By the definition of π, we have that $\mathop{\mathbb{E}}_{(x,y)\sim\rho}[E(x, y)] = |\pi|$, where here $|\pi|$ denotes the expected communication cost of π (since π is an expected randomized distributional protocol).

We construct a protocol τ for f in Protocol 1.

We claim that τ is a public-coin randomized protocol for f with $(\delta + \sqrt{\epsilon})$-promise and $(\delta + \sqrt{\epsilon})$-error. To do so, we separate the input space of π into two sets, type-A inputs and type-B inputs, as follows: an input (x, y) is said to be a type-A input of τ if and only if

$$E(x, y) \geq \frac{1}{\delta}|\pi| \quad \text{or} \quad I(x, y) \geq \sqrt{\epsilon}.$$

▶ **Claim 10.** $\Pr_{(x,y)\sim\rho}[(x, y)$ *is a type-A input of* $\tau] \leq \delta + \sqrt{\epsilon}$.

Proof. First, $\mathop{\mathbb{E}}_{(x,y)\sim\rho}[E(x, y)] = |\pi|$ and, by applying Markov's inequality,

$$\Pr_{(x,y)\sim\rho}\left[E(x, y) \geq \frac{1}{\delta}|\pi|\right] \leq \Pr_{(x,y)\sim\rho}\left[E(x, y) \geq \frac{1}{\delta}\mathop{\mathbb{E}}_{(x,y)\sim\rho}[E(x, y)]\right] \leq \delta.$$

Similarly, $\underset{(x,y)\sim\rho}{\mathbb{E}}[I(x,y)] \leq \epsilon$, and by applying Markov's inequality,

$$\Pr_{(x,y)\sim\rho}\left[I(x,y) \geq \sqrt{\epsilon}\right] \leq \Pr_{(x,y)\sim\rho}\left[I(x,y) \geq \frac{1}{\sqrt{\epsilon}}\underset{(x,y)\sim\rho}{\mathbb{E}}[I(x,y)]\right] \leq \sqrt{\epsilon}.$$

A union bound argument yields that

$$\Pr_{(x,y)\sim\rho}[(x,y) \text{ is a type-A input of } \tau] \leq \delta + \sqrt{\epsilon},$$

and the claim follows. ◀

▶ **Claim 11.** *Given that (x,y) is a type-B input of τ, $\Pr_r[\tau(x,y,r) \neq f(x,y)] \leq \delta + \sqrt{\epsilon}$.*

Proof. Since (x,y) is a type-B input of τ, then $\underset{r}{\mathbb{E}}[|\tau(x,y,r)|] \leq \frac{1}{\delta}|\pi|$ and $\underset{r}{\mathbb{E}}[I(x,y,r)] \leq \sqrt{\epsilon}$. Observe that τ might err in either of two cases: τ was early-terminated, or τ was not early terminated but the simulation of π answered incorrectly. By the union bound, we conclude the following:

$$\begin{aligned}\Pr_r[\tau(x,y,r) \neq f(x,y)] &\leq \Pr_r\left[|\tau(x,y,r)| > \frac{1}{\delta^2}|\pi|\right] + \Pr_r[I(x,y,r) = 1] \\ &\leq \Pr_r\left[|\tau(x,y,r)| > \frac{1}{\delta}\underset{r}{\mathbb{E}}[|\tau(x,y,r)|]\right] + \underset{r}{\mathbb{E}}[I(x,y,r)] \\ &\leq \delta + \sqrt{\epsilon},\end{aligned}$$

where the last inequality follows from Markov's inequality. ◀

In conclusion, Claim 10 proves that there are at most $(\delta + \sqrt{\epsilon})$ type-A inputs of τ, weighed by ρ, and Claim 11 proves that τ has at most $(\delta + \sqrt{\epsilon})$-error on type-B inputs. Therefore, τ is indeed a public-coin randomized protocol that computes f with $(\rho, \sqrt{\epsilon} + \delta)$-promise and $(\sqrt{\epsilon} + \delta)$-error. Step 2 (early termination) assures that $|\tau| \leq \frac{1}{\delta^2}|\pi|$, and that concludes the proof of Lemma 9. ◀

We remark that we have dealt with several communication complexity measures in this subsection and, for conciseness reasons, some of the connections between the different measures were omitted. However, the omitted connections can be shown, either by simply combining the connections we have proved, or by slightly modifying the arguments presented in our proofs. For instance, an argument similar to that of Lemma 9 proves that $\mathcal{R}^{(\rho,\sqrt{\epsilon})}(f,\sqrt{\epsilon}) \leq \mathcal{R}^{\rho}(f,\epsilon)$. For another example, one can prove that there exists a distribution ρ over $\{0,1\}^n \times \{0,1\}^n$ for which $\mathcal{R}^{(\rho,\delta)}(f,\epsilon) \geq \mathcal{R}^{\text{pub}}(f,\delta+\epsilon)$ using Theorem 4 and Theorem 8.

3.2 Pushing M_4 Towards M_5

In this section, we prove that computing ℓ instances of f in the point-to-point model, M_4, cannot be done much more efficiently than just solving each instance separately, as in the independent computations model, M_5. From a more philosophical point of view, designing protocols in which Alice sends "global" messages is virtually useless in the public-coin randomized setting when only point-to-point communication is allowed. Formally stated:

▶ **Theorem 12.** $\mathcal{R}^{\text{pub}}(f, 2(\sqrt{\epsilon}+\delta)) \leq \frac{1}{\delta^2}\frac{1}{\ell}\mathcal{R}_4^{\text{pub}}(f^\ell,\epsilon)$*, for any f, ℓ, and $\epsilon, \delta \in (0,1)$ such that* $2(\sqrt{\epsilon}+\delta) \leq 1$.

Protocol 2 $\tau(x, y, r)$.

```
1: Preparation: Alice and Bob split the random string $r$ into two independent random
   strings, $r \triangleq (r_1, r_2)$.
2: Augmentation: Alice and Bob construct an input $(\vec{x}, \vec{y})$ for $\pi$ from their $(x, y)$:
   2.1: Alice and Bob sample $i \sim \text{Unif}\{[\ell]\}$ from the randomness $r_1$.
   2.2: Alice samples $(\vec{u}, \vec{v}) = ((u_1, \dots, u_{\ell-1}), (v_1, \dots, v_{\ell-1})) \sim \rho^{\ell-1}$ from $r_1$.
   2.3: Let $\vec{x} \triangleq \text{aug}[\vec{u}, x, i]$, and let $\vec{y} \triangleq \text{aug}[\vec{v}, y, i]$.
3: Simulation: Alice and Bob simulate the $i$'th channel of $\pi(\vec{x}, \vec{y}, r_2)$.
   That is, Bob plays the role of $\text{Dan}_i$, while Alice plays the role of Carol and all other
   Dans. In their simulation, Alice and Bob only send messages that are sent between Carol
   and and $\text{Dan}_i$ in $\pi$. All other messages are simulated by Alice alone, with no additional
   communication.
```

Given a protocol π for f^ℓ in M_4, our proof constructs a protocol τ for f (a single instance in the two-party model) such that $|\tau| \le \frac{1}{\delta^2}\frac{1}{\ell}|\pi|$. The construction of τ is based on the *symmetrization* technique, that was introduced in [22], and was later used in, e.g., [24, 25]. In the core of the symmetrization technique lies an intuitive averaging argument: suppose we fix some input to each of the parties in M_4. In that case, the average number of bits communicated on a uniformly-chosen channel is at most $\frac{1}{\ell}|\pi|$. In τ, Alice and Bob augment their single instance (x, y) to an input $(\vec{x}, \vec{y})$ for π, that contains ℓ instances of f, and then simulate a channel of $\pi(\vec{x}, \vec{y})$. We thus define an *augmentation operator*:

▶ **Definition 13** (The Augmentation operator). Let Q be any set, and $k \in \mathbb{N}$ an integer. Given a k-tuple $\vec{q} = (q_1, \dots, q_k) \in Q^k$, an element p, and an index $i \in [k+1]$, the *augmentation operator* $\text{aug}[\vec{q}, p, i]$ is defined to be the $(k+1)$-tuple obtained by "inserting" p as an i'th element in $\vec{q}$, i.e. $\text{aug}[\vec{q}, p, i] \triangleq (q_1, \dots, q_{i-1}, p, q_i, \dots, q_k)$.

We now prove a central lemma from which we conclude Theorem 12:

▶ **Lemma 14.** $\overline{\mathcal{R}}^{\rho}(f, \epsilon) \le \frac{1}{\ell}\mathcal{R}_4^{\rho^\ell}\left(f^\ell, \epsilon\right)$*, for any* f*,* ℓ*,* $\epsilon \in (0, 1)$*, and* ρ *over* $\{0,1\}^n \times \{0,1\}^n$.

Proof. Let π be a randomized $\left(\rho^\ell, \epsilon\right)$-distributional protocol for f^ℓ in M_4. Given π, we construct a protocol τ for a single instance of f, such that τ is an expected randomized (ρ, ϵ)-distributional protocol. The construction of τ is presented in Protocol 2. To avoid confusion, we refer to the two parties in τ as Alice and Bob, and to the $\ell + 1$ parties in π as Carol and Dans.

For every $(x, y) \in \{0,1\}^n \times \{0,1\}^n$, let $E(x, y) \triangleq \underset{r}{\mathbb{E}}[|\tau(x, y, r)|]$ denote the expected communication complexity of τ on (x, y), over the choice of public randomness.

▶ **Claim 15.** $\underset{(x,y)\sim\rho}{\mathbb{E}}[E(x, y)] \le \frac{1}{\ell}|\pi|$.

Proof of Claim 15. For every $i \in [\ell]$ and every $(\vec{x}, \vec{y}) \in \{0,1\}^{n\ell} \times \{0,1\}^{n\ell}$, let $\left|\pi^i(\vec{x}, \vec{y})\right|$ denote the maximum number of bits communicated between Carol and Dan_i when running π on $(\vec{x}, \vec{y})$. We thus have

$$\underset{(x,y)\sim\rho}{\mathbb{E}}[E(x, y)] = \underset{(x,y)\sim\rho}{\mathbb{E}}\left[\underset{i\sim\text{Unif}\{[\ell]\}}{\mathbb{E}}\left[\underset{(\vec{u},\vec{v})\sim\rho^{\ell-1}}{\mathbb{E}}\left[\left|\pi^i(\vec{x}, \vec{y})\right|\right]\right]\right] \le \underset{(\vec{x},\vec{y})\sim\rho^\ell}{\mathbb{E}}\left[\frac{1}{\ell}|\pi|\right] \le \frac{1}{\ell}|\pi|$$

and the claim follows. ◀

For every $(\vec{x},\vec{y}) \in \{0,1\}^{n\ell} \times \{0,1\}^{n\ell}$ and for every random string r_2, let $J(\vec{x},\vec{y},r_2)$ be the following $\{0,1\}$-indicator: $J(\vec{x},\vec{y},r_2) = 1$ if and only if π errs on $(\vec{x},\vec{y})$ given the random string is r_2. Furthermore, for every $(x,y) \in \{0,1\}^n \times \{0,1\}^n$ and for every possible random string $r = (r_1,r_2)$, where $r_1 = (i,(\vec{u},\vec{v})) \in [\ell] \times \{0,1\}^{n(\ell-1)} \times \{0,1\}^{n(\ell-1)}$ and $r_2 \in \{0,1\}^*$, let $I(x,y,r) = J(\operatorname{aug}[\vec{u},x,i], \operatorname{aug}[\vec{v},y,i], r_2)$. Let $I(x,y) \triangleq \mathop{\mathbb{E}}_{r}[I(x,y,r)]$ for every $(x,y) \in \{0,1\}^n \times \{0,1\}^n$.

▶ **Claim 16.** $\mathop{\mathbb{E}}_{(x,y)\sim\rho}[I(x,y)] \le \epsilon$.

Proof.

$$\begin{aligned}\mathop{\mathbb{E}}_{(x,y)\sim\rho}[I(x,y)] &= \mathop{\mathbb{E}}_{(x,y)\sim\rho}\left[\mathop{\mathbb{E}}_{i\sim\mathrm{Unif}\{[\ell]\}}\left[\mathop{\mathbb{E}}_{(\vec{u},\vec{v})\sim\rho^{\ell-1}}\left[\mathop{\mathbb{E}}_{r_2}[J(\operatorname{aug}[\vec{u},x,i], \operatorname{aug}[\vec{v},y,i], r_2)]\right]\right]\right]\\ &\le \mathop{\mathbb{E}}_{(\vec{x},\vec{y})\sim\rho^{\ell}}\left[\mathop{\mathbb{E}}_{r_2}[J(\vec{x},\vec{y},r_2)]\right] \le \epsilon,\end{aligned}$$

where the last inequality holds since π is an expected randomized (ρ^ℓ,ϵ)-distributional protocol for f^ℓ in M_4. ◀

To conclude, Claim 15 and Claim 16 show that τ is indeed an expected randomized distributional protocol for f with the desired properties, and together they imply Lemma 14. ◀

Proof of Theorem 12. As promised in Theorem 4, let ρ be a distribution on $\{0,1\}^n \times \{0,1\}^n$ that satisfies $\mathcal{D}^{(\rho,2(\delta+\sqrt{\epsilon}))}(f) = \mathcal{R}^{\mathrm{pub}}(f, 2(\delta+\sqrt{\epsilon}))$. We therefore have that

$$\begin{aligned}\mathcal{R}^{\mathrm{pub}}\left(f, 2\left(\delta+\sqrt{\epsilon}\right)\right) &= \mathcal{D}^{\left(\rho,2\left(\sqrt{\epsilon}+\delta\right)\right)}(f) && \text{(by choice of } \rho)\\ &\le \mathcal{R}^{\left(\rho,\sqrt{\epsilon}+\delta\right)}\left(f,\sqrt{\epsilon}+\delta\right) && \text{(Theorem 8)}\\ &\le \frac{1}{\delta^2}\overline{\mathcal{R}}^{\rho}(f,\epsilon) && \text{(Theorem 9)}\\ &\le \frac{1}{\delta^2}\frac{1}{\ell}\mathcal{R}_4^{\rho^\ell}\left(f^\ell,\epsilon\right) && \text{(Theorem 14)}\\ &\le \frac{1}{\delta^2}\frac{1}{\ell}\mathcal{R}_4^{\mathrm{pub}}\left(f^\ell,\epsilon\right), && \text{(Observation 7)}\end{aligned}$$

and the theorem holds. ◀

4 One-Round Communication

In this section, we consider several definitions of *one-round* communication protocols in our models, and examine the connections between them. We prove that savings cannot be obtained in M_3, M_4, and M_5 when considering one-round protocols, for any complexity measure (that is, deterministic, nondeterministic, and randomized). However, we prove that, under a certain definition of one-round protocols in M_2, gaps can be found between M_2 and M_3 in the private-coin randomized setting and, if search problems are taken into account, then gaps can also be found between M_1 and M_2 in the deterministic setting.

4.1 M_3, M_4 and M_5 in the One-Round Setting

▶ **Definition 17.** Let P be a computational problem, $\ell \ge 1$, and $k \in \{3,4,5\}$.
A protocol π in M_k is a *one-round protocol* if Alice does not send a message to any of the Bobs in any execution of the protocol. Given a complexity measure C, let $C_k^1\left(P^\ell\right)$ denote

the cost of the best one-round protocol that solves P^ℓ in M_k with respect to the measure C. Furthermore, let $C^1(P) \triangleq C^1_5(P)$ denote the cost of the best one-round protocol that solves P in the two-party setting with respect to the measure C.

Since the Bobs in M_3, M_4, and M_5 cannot hear each other directly in these models then, when considering one-round protocols, the message sent by each Bob$_i$ is independent of the messages sent by the other Bobs. The following is therefore fairly easy to prove:

▶ **Observation 18.** *$C^1_k(P^\ell) \geq \ell \cdot C^1(P)$, for any $k \in \{3, 4, 5\}$, any computational problem P, any $\ell \geq 1$, and any complexity measure C (i.e. $C \in \{\mathcal{D}, \mathcal{N}, \mathcal{R}, \dots\}$).*

4.2 M_2 in the One-Round Setting

Contrary to the models M_3, M_4, and M_5, the Bobs are able to hear one another in M_2. This property of M_2 allows for several possible variations on one-round protocols:

1. *One-message-each protocols*, where each Bob sends one message to Alice. However, the messages are sent sequentially, as opposed to simultaneous protocols. Namely, each Bob can hear all messages sent by Bobs whose turn preceded his. The identity of the next speaker is determined by the previous messages sent in the protocol and, in the public-coin randomized setting, by the public randomness as well. Therefore, the order in which the Bobs speak may vary between different executions of the protocol.
2. *Bobs-only protocols* where Alice does not send any message but the Bobs are unconstrained, and can exchange as many messages as they wish. We remark that these are not one-round protocols per se, since the speaker may change multiple times. This collective view of the Bobs is reasonable since M_2 is an asymmetric model, in which Alice plays a different role than the Bobs.

▶ **Definition 19.** Let P be a communication problem and let $\ell \in \mathbb{N}$. Let C be any complexity measure. Let $C^1_2\left(P^\ell\right)$ denote the cost of the best one-message-each protocol that solves P^ℓ in M_2 with respect to the measure C, and let $C^B_2\left(P^\ell\right)$ denote the cost of the best Bobs-only protocol that solves P^ℓ in M_2 with respect to the measure C.

4.2.1 The Randomized Case

4.2.1.1 The Public-Coin Setting

The following claim proves that if public-coin randomness is allowed, then M_2 and M_5 are essentially equivalent when considering Bobs-only communication complexity, and significant gaps between them cannot be found with respect to this measure.

▶ **Claim 20.** *$\mathcal{R}^{1,\text{pub}}(f, 2(\sqrt{\epsilon} + \delta)) \leq \frac{1}{\delta^2}\frac{1}{\ell}\mathcal{R}^{B,\text{pub}}_4\left(f^\ell, \epsilon\right)$ for any f, ℓ, and $\epsilon, \delta \in (0, 1)$ that satisfy $2(\sqrt{\epsilon} + \delta) \leq 1$.*

This claim, and its proof, resemble Theorem 12. In the proof of Theorem 12, a protocol τ that computes f in the two-party setting was constructed from a protocol π that computes f^ℓ in M_4. Intuitively, the two parties in τ choose a uniformly random $i \in [\ell]$ and simulate the i'th channel of π. Hence, $|\tau| = O\left(\frac{1}{\ell}|\pi|\right)$ by an averaging argument.

Let us try to extend this argument to M_2. As before, to avoid confusion, we refer to the two parties in τ as Alice and Bob, and to the $\ell + 1$ parties in π as Carol and Dans. Assume, then, that π is a protocol for f^ℓ in M_2 (not necessarily a one-round protocol), and suppose that Carol sends at most c bits and that the Dans send at most d bits (combined) in any run of π. Since Carol uses broadcast communication in π, then the average number of bits sent between Carol and Dan$_i$ in π is roughly $c + \frac{1}{\ell}d$, for a uniformly-sampled $i \in [\ell]$. However, c might be very large in general protocols, and hence this averaging argument seems to provide a very weak bound in the general case. However, if $c = 0$, i.e. if π is an Bobs-only protocol, then $|\tau| = O(\frac{1}{\ell}d) = O\left(\frac{1}{\ell}|\pi|\right)$, as desired. Therefore, in the case of Bobs-only protocols, the exact same construction of τ as in Theorem 12 proves Claim 20. The formal proof is almost identical to that of Theorem 12, and is hence omitted.

4.2.1.2 The Private-Coin Setting

In the full version of the paper, we show that the equality function separates M_3 from M_4 in the unbounded-round private-coin setting, and that it also separates M_2 from M_3 in the one-round setting when considering one-message-each protocols, where the lower bound on M_3 follows immediately from Observation 18 and the known fact that $\mathcal{R}^{1,\text{priv}}(\text{EQ}, 1/3) \geq \mathcal{R}^{\text{priv}}(\text{EQ}, 1/3) = \Omega(\log n)$ (see, e.g., [17]). Thus $\mathcal{R}_3^{1,\text{priv}}\left(\text{EQ}^\ell, \epsilon\right) = \Omega(\ell \log n)$. As for the upper bound on M_2, it can be easily obtained using Newman's transformation from the public-coin setting to the private-coin setting [18]; we also show (in the full version) that $\mathcal{R}^{1,\text{pub}}(\text{EQ}, 1/3) = O(1)$ and also that $\mathcal{R}^{1,\text{priv}}\left(f^\ell, 1/3\right) = O\left(\mathcal{R}^{1,\text{pub}}\left(f^\ell, 1/3\right) + \log(n\ell)\right)$ for any function f and natural number ℓ. Using amplification, we have that $\mathcal{R}^{1,\text{pub}}\left(\text{EQ}^\ell, 1/3\right) = O(\ell \log \ell)$, and conclude that $\mathcal{R}_2^{1,\text{priv}}\left(\text{EQ}^\ell, 1/3\right) = O\left(\ell \log \ell + \log(n\ell)\right)$.

We remark that since Bobs-only protocols in M_2 are stronger than one-message-each protocols, then the gap presented also holds for Bobs-only protocols in M_2.

4.2.2 The Deterministic Case

The previous subsection shows a gap between M_2 and M_3 when considering one-message-each protocols in the private-coin setting. However, M_2 seems to behave differently in the deterministic setting, as suggested by the following claim:

▶ **Claim 21.** *$\mathcal{D}_2^1\left(P^\ell\right) \geq \ell \cdot \mathcal{D}^1(P)$, for any computational problem P and any $\ell \in \mathbb{N}$.*

Proof sketch. By induction on ℓ. The claim is clearly true for $\ell = 1$. Let $\ell \geq 2$, and let π be an optimal one-message-each protocol that solves P^ℓ in M_2. For every $i \in [\ell]$, let m_i denote the i'th message in π. We separate into cases:

Case 1. Suppose there exists a valid prefix of the transcript $m_1, \ldots, m_{\ell-1}$ such that $\sum_{i=1}^{\ell-1} |m_i| \geq \frac{\ell-1}{\ell}|\pi|$. In that case, we construct a protocol τ for P in the two-party setting by fixing these messages and letting Bob play the role of the last party in π. The communication complexity of τ is at most $\frac{1}{\ell}|\pi|$, and hence $|\pi| \geq \ell C(P)$.

Case 2. Suppose that every valid prefix of the transcript $m_1, \ldots, m_{\ell-1}$ satisfies $\sum_{i=1}^{\ell-1} |m_i| < \frac{\ell-1}{\ell}|\pi|$. In that case, we construct a protocol τ for $P^{\ell-1}$ in M_2 (with one Alice and $\ell - 1$ Bobs) by letting the Bobs play the roles of the first $\ell - 1$ parties of π, and letting Alice simulate the last Bob (with no communication). We therefore have that $|\tau| < \frac{\ell-1}{\ell}|\pi|$. Since we assumed π to be optimal, then clearly $|\pi| \leq \ell C(P)$, and we thus get $|\tau| < (\ell - 1)C(P)$, in contradiction to the induction hypothesis. ◀

Claim 21 shows that no gaps can be found between M_2 and M_3 when considering one-message-each protocols in the deterministic setting. We ask whether this is true for Bobs-only protocols as well; namely,

▶ **Question 22.** *Is it true that $\mathcal{D}_2^B\left(P^\ell\right) \geq \ell \cdot \mathcal{D}^1(P)$ for any P and any $\ell \geq 1$?*

4.2.2.1 Separating M_1 from M_2 for One-Message-Each Protocols

When considering the deterministic communication complexity of direct-sum problems, no saving is known to be achievable for full functions in the two-party setting. However, some saving can be achieved in the case of partial functions. In the rest of this section, we study such an example in our models.

▶ **Definition 23** (The NBA problem)**.** Let $n \in \mathbb{N}$. For every $x = (u, v) \in \{0,1\}^n \times \{0,1\}^n$ and for every $y \in \{0,1\}^n$, the *NBA* function is defined as follows:

$$\mathrm{NBA}(x,y) \triangleq \begin{cases} \text{undefined} & y \notin \{u,v\} \vee u = v \\ 1 & y = u \\ 0 & y = v \end{cases}$$

Intuitively, Alice knows the names of two NBA teams, u and v, that played against each other last night. However, she does not know which of the teams had won the game. Bob, on the other hand, knows the name of the winning team, $y \in \{u, v\}$, but not the name of its opponent. The goal is for Alice to know which team had won the match.

The NBA problem was first studied in [19, 20], where it was called *The League Problem*, and it was proved that $\mathcal{D}\left(\mathrm{NBA}\right) = \log n + 1$. Then, in [10], it was proved that some saving can be achieved for its direct-sum version. In particular, an upper bound of $O(\ell + \log n \log \ell)$ was shown. The protocol can also be run in M_2 and M_3, and seems to heavily rely on Alice's ability to see all ℓ instances together. Therefore, intuition would suggest that switching the roles of Alice and Bob would put their ability to design a clever protocol for M_2 in question. We therefore define the *Inverted*-NBA problem:

▶ **Definition 24** (The INBA problem)**.** For every $x \in \{0,1\}^n$ and $y \in \{0,1\}^n \times \{0,1\}^n$, the *Inverted-NBA* function is defined to be $\mathrm{INBA}(x, y) \triangleq \mathrm{NBA}(y, x)$.

▶ **Example 25.** Consider the INBA partial function. We claim that it presents a deterministic gap between M_1 and M_2 in the one-round setting. In particular, we examine one-message-each protocols in M_2. The lower bound in M_2 follows from Claim 21 and the fact that $\mathcal{D}\left(\mathrm{NBA}\right) = \log n + 1$, which together prove that $\mathcal{D}_2^B\left(\mathrm{INBA}^\ell\right) \geq \ell \log n$. For the upper bound on M_1, we first claim that any protocol that computes NBA^ℓ in M_1 can also be used to compute INBA^ℓ in M_1, simply by switching the roles of Alice and Bob. Furthermore, we claim (without proof) that the protocol presented in [10] can be easily turned into a one-round protocol for INBA^ℓ in M_1, and thus conclude that $\mathcal{D}_1^1\left(\mathrm{INBA}^\ell\right) = O(\ell + \log \ell \log n)$. The argument appears at length and in greater detail in the full version of the paper.

Proving that $D_2^B\left(\mathrm{INBA}^\ell\right) = \Omega\left(\ell \log n\right)$ would strengthen the gap presented in the example above. We conjecture that the INBA problem remains hard in M_2 even in the unbounded-round setting. That is: $D_2\left(\mathrm{INBA}^\ell\right) = \Omega\left(\ell \log n\right)$.

5 Conclusions and Future Work

In this work, we suggest a new approach to the study of two-party direct-sum questions in communication complexity. Future work may extend our approach in several directions.

One such direction would be to try and find more gaps and equivalences between the models we proposed with respect to various complexity measures; for instance, one may try to extend Theorem 12 and prove that savings cannot be obtained in M_4 with respect to other measures, e.g. deterministic communication complexity. This would support our intuition that "point-to-point communication is hard". Another example is to try and separate M_1 and M_2 with respect to private-coin randomized setting. To the best of our knowledge, all currently known savings in this setting utilize Newman's transformation which also applies to the models M_2 and M_3. Therefore, the current techniques cannot be used to separate M_1 and M_2. Another interesting direction, that would require devising new functions for which savings can be obtained in the classical two-party direct-sum setting, would be to try to separate M_1 from M_2 with respect to private-coin randomized communication complexity. One may also consider a variant of the public coin randomized setting in which there is a common random string on each communication line, that is, Alice and Bob_i share a random string r_i. It may be interesting to study the connection between our five models in this setting, and compare it to other settings, e.g. to the public coin setting we discuss in the paper (in which there is one global random string, shared by all parties).

Finally, one can examine the two-party direct-sum question through the lens of other multiparty models, such as more complicated bipartite communication graphs (where one side has k Alices and the other side has t Bobs) or the clique network. Understanding these questions may also shed new light on the source of hardness of classical direct-sum questions in two-party communication complexity.

References

1 Noga Alon, Klim Efremenko, and Benny Sudakov. Testing equality in communication graphs. *arXiv preprint arXiv:1605.01658*, 2016.

2 Ziv Bar-Yossef, Thathachar S Jayram, Ravi Kumar, and D Sivakumar. An information statistics approach to data stream and communication complexity. In *Foundations of Computer Science, 2002. Proceedings. The 43rd Annual IEEE Symposium on*, pages 209–218. IEEE, 2002.

3 Mark Braverman. Interactive information complexity. *SIAM Journal on Computing*, 44(6):1698–1739, 2015.

4 Mark Braverman, Faith Ellen, Rotem Oshman, Toniann Pitassi, and Vinod Vaikuntanathan. A tight bound for set disjointness in the message-passing model. In *Foundations of Computer Science (FOCS), 2013 IEEE 54th Annual Symposium on*, pages 668–677. IEEE, 2013.

5 Mark Braverman and Rotem Oshman. The communication complexity of number-in-hand set disjointness with no promise. In *Electronic Colloquium on Computational Complexity (ECCC)*, volume 22, 2015.

6 Mark Braverman and Anup Rao. Information equals amortized communication. *IEEE Transactions on Information Theory*, 60(10):6058–6069, 2014.

7 Harry Buhrman, Matthias Christandl, and Jeroen Zuiddam. Nondeterministic quantum communication complexity: the cyclic equality game and iterated matrix multiplication. *arXiv preprint arXiv:1603.03757*, 2016.

8 Amit Chakrabarti, Subhash Khot, and Xiaodong Sun. Near-optimal lower bounds on the multi-party communication complexity of set disjointness. In *Computational Complexity, 2003. Proceedings. 18th IEEE Annual Conference on*, pages 107–117. IEEE, 2003.

9 Amit Chakrabarti, Yaoyun Shi, Anthony Wirth, and Andrew Yao. Informational complexity and the direct sum problem for simultaneous message complexity. In *Foundations of Computer Science, 2001. Proceedings. 42nd IEEE Symposium on*, pages 270–278. IEEE, 2001.

10 Tomas Feder, Eyal Kushilevitz, Moni Naor, and Noam Nisan. Amortized communication complexity. *SIAM Journal on computing*, 24(4):736–750, 1995.

11 Anat Ganor, Gillat Kol, and Ran Raz. Exponential separation of information and communication. In *Foundations of Computer Science (FOCS), 2014 IEEE 55th Annual Symposium on*, pages 176–185. IEEE, 2014.

12 Anat Ganor, Gillat Kol, and Ran Raz. Exponential separation of communication and external information. In *STOC*, pages 977–986, 2016.

13 Anat Ganor, Gillat Kol, and Ran Raz. Exponential separation of information and communication for boolean functions. *Journal of the ACM (JACM)*, 63(5):46, 2016.

14 Bala Kalyanasundaram and Georg Schintger. The probabilistic communication complexity of set intersection. *SIAM Journal on Discrete Mathematics*, 5(4):545–557, 1992.

15 Mauricio Karchmer, Eyal Kushilevitz, and Noam Nisan. Fractional covers and communication complexity. In *Structure in Complexity Theory Conference, 1992., Proceedings of the Seventh Annual*, pages 262–274. IEEE, 1992.

16 Mauricio Karchmer, Ran Raz, and Avi Wigderson. Super-logarithmic depth lower bounds via the direct sum in communication complexity. *Computational Complexity*, 5(3-4):191–204, 1995. Early version in CCC 1991.

17 Eyal Kushilevitz and Noam Nisan. *Communication Complexity*. Cambridge University Press, Cambridge, 1997.

18 Ilan Newman. Private vs. common random bits in communication complexity. *Information processing letters*, 39(2):67–71, 1991.

19 Alon Orlitsky. Worst-case interactive communication. i. two messages are almost optimal. *IEEE Transactions on Information Theory*, 36(5):1111–1126, 1990.

20 Alon Orlitsky. Worst-case interactive communication. ii. two messages are not optimal. *IEEE Transactions on Information Theory*, 37(4):995–1005, 1991.

21 David Peleg. *Distributed computing: a locality-sensitive approach*. SIAM, 2000.

22 Jeff M Phillips, Elad Verbin, and Qin Zhang. Lower bounds for number-in-hand multiparty communication complexity, made easy. In *Proceedings of the twenty-third annual ACM-SIAM symposium on Discrete Algorithms*, pages 486–501. SIAM, 2012.

23 Alexander A. Razborov. On the distributional complexity of disjointness. *Theoretical Computer Science*, 106(2):385–390, 1992.

24 David P Woodruff and Qin Zhang. Tight bounds for distributed functional monitoring. In *Proceedings of the forty-fourth annual ACM symposium on Theory of computing*, pages 941–960. ACM, 2012.

25 David P Woodruff and Qin Zhang. When distributed computation is communication expensive. In *International Symposium on Distributed Computing*, pages 16–30. Springer, 2013.

26 David P Woodruff and Qin Zhang. An optimal lower bound for distinct elements in the message passing model. In *Proceedings of the Twenty-Fifth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 718–733. Society for Industrial and Applied Mathematics, 2014.

27 Andrew Yao. Some complexity questions related to distributed computing. In *Proc. 11th STOC*, pages 209–213, 1979.

28 Andrew C Yao. Lower bounds by probabilistic arguments. In *Foundations of Computer Science, 1983., 24th Annual Symposium on*, pages 420–428. IEEE, 1983.