The Strength of Equality Oracles in Communication

Toniann Pitassi
Columbia University, New York, NY, USA

Morgan Shirley ✉
University of Toronto, Canada

Adi Shraibman ✉
The Academic College of Tel Aviv-Yaffo, Israel

Abstract

It is well-known that randomized communication protocols are more powerful than deterministic protocols. In particular the Equality function requires $\Omega(n)$ deterministic communication complexity but has efficient randomized protocols. Previous work of Chattopadhyay, Lovett and Vinyals shows that randomized communication is strictly stronger than what can be solved by deterministic protocols equipped with an Equality oracle. Despite this separation, we are far from understanding the exact strength of Equality oracles in the context of communication complexity.

In this work we focus on nondeterminisic communication equipped with an Equality oracle, which is a subclass of Merlin-Arthur communication. We show that this inclusion is strict by proving that the previously-studied Integer Inner Product function, which can be efficiently computed even with bounded-error randomness, cannot be computed using sublinear communication in the nondeterministic Equality model. To prove this we give a new matrix-theoretic characterization of the nondeterministic Equality model: specifically, there is a tight connection between this model and a covering number based on the blocky matrices of Hambardzumyan, Hatami, and Hatami, as well as a natural variant of the Gamma-2 factorization norm. Similar equivalences are shown for the unambiguous nondeterministic model with Equality oracles. A bonus result arises from these proofs: for the studied communication models, a single Equality oracle call suffices without loss of generality.

Our results allow us to prove a separation between deterministic and unambiguous nondeterminism in the presence of Equality oracles. This stands in contrast to the result of Yannakakis which shows that these models are polynomially-related without oracles. We suggest a number of intriguing open questions along this direction of inquiry, as well as others that arise from our work.

2012 ACM Subject Classification Theory of computation → Communication complexity

Keywords and phrases Factorization norm, blocky rank, Merlin-Arthur

Digital Object Identifier 10.4230/LIPIcs.ITCS.2023.89

Funding *Toniann Pitassi*: Research supported by NSERC and by NSF Award AF: Medium 2212136. *Morgan Shirley*: Research supported by NSERC.

Acknowledgements We thank Arkadev Chattopadhyay, Lianna Hambardzumyan, Aleksandar Nikolov, and Suhail Sherif for helpful discussions.

1 Introduction

Two computationally unbounded parties each hold an n-bit string. Their goal is to compute some function that depends on their inputs. For a given function, how many bits must they exchange? In the paper that introduced this model, Yao proved that computing the Equality function – that is, deciding whether or not the two parties' inputs are equal – requires $\Omega(n)$ bits of communication. This means that Equality is maximally hard in an asymptotic sense, as $n + 1$ bits of communication always suffices [31]. However, if a public source of randomness is available and some bounded probability of error is tolerated, Equality only

requires $O(1)$ bits of communication; a proof can be found in most introductory texts on the subject [19, 29]. This means that *randomized* communication can be exponentially stronger than *deterministic* communication. There has been recent interest in determining the power of EQUALITY in communication. We can sum up this direction of study with the following question:

What total functions can be efficiently computed in a communication model where the only access to randomness is via reduction to EQUALITY*?*

Many known functions where randomization is useful can be solved by an efficient deterministic protocol with access to an EQUALITY oracle – for example, the greater-than function [25]. On the other hand, it was recently shown that EQUALITY alone cannot simulate all randomized protocols [9]. In both of these results, the model under study is deterministic and the oracle access resembles Turing reductions in classical complexity: the EQUALITY oracle may be queried many times and the results may be used however the parties want. In this article we study what happens when these parameters are changed:

- What functions can be efficiently computed when **stronger models of communication** are given EQUALITY oracle access?
- Does restricting to **many-one reductions** change the power of EQUALITY oracles?

Of specific interest to us is *nondeterministic* communication with access to an EQUALITY oracle. This is a natural restriction of Merlin-Arthur communication, an intriguing model against which no linear lower bounds for explicit functions are known (see [1, 11]). Nondeterministic communication with EQUALITY queries has been implicitly studied before; for example, Göös, Pitassi, and Watson showed a separation between this model and zero-error randomized communication with access to a single nondeterministic oracle query [13]. Our main results center around this model.

1.1 Blocky Matrices as Building Blocks

Given a two-party function $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$, its communication matrix M is a $2^n \times 2^n$ matrix that acts as a bipartite truth table for F: each row represents some input x, each column represents some input y, and entry $M[x,y]$ is the value of $F(x,y)$. Nondeterministic flavors of communication complexity can be defined as minimization problems for *covers* of M, using *monochromatic rectangles* as the basic building block (a rectangle is a product set of rows and columns). For example, the nondeterministic communication complexity of M, $\mathsf{NP}^{\mathsf{cc}}(M)$, is characterized by the logarithm of $C_1(M)$, the minimum number of 1-monochromatic rectangles required to cover the ones of M, and co-nondeterministic communication complexity, $\mathsf{coNP}^{\mathsf{cc}}(M)$, is the logarithm of $C_0(M)$, the minimum cover size for the zeroes of M. Similarly the unambiguous complexity of M, $\mathsf{UP}^{\mathsf{cc}}(M)$, is characterized by the logarithm of $\chi_1(M)$, the minimum number of *disjoint* rectangles needed to cover the ones of M, and $\mathsf{coUP}^{\mathsf{cc}}(M)$ is the logarithm of $\chi_0(M)$, the minimum number of disjoint rectangles needed to cover the zeroes of M. This point of view was highly successful in understanding the relationships between deterministic and nondeterministic communication. For example, Aho, Ullman, and Yannakakis showed that $\mathsf{P}^{\mathsf{cc}} = \mathsf{NP}^{\mathsf{cc}} \cap \mathsf{coNP}^{\mathsf{cc}}$ and thus deterministic communication complexity is characterized by the logarithm of $\chi(M)$, the size of the minimum partition of M into disjoint monochromatic rectangles [2]. Moreover, viewing nondeterministic communication as covering problems brings out some equivalent formulations coming from extremal combinatorics and graph theory. For example, the proof of superlogarithmic lower bounds on the $\mathsf{coNP}^{\mathsf{cc}}$ complexity of problems with efficient $\mathsf{UP}^{\mathsf{cc}}$ protocols refuted a polynomial version of the Alon-Saks-Seymour conjecture in graph theory [30, 6, 12].

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

(a) Identity matrices (b) All-ones matrices (c) Direct sums of all-ones matrices (d) Permutations of (a)-(c)

Figure 1 Some examples of blocky matrices.

In this work we focus on communication complexity classes equipped with an Equality oracle and introduce several equivalent characterizations of these classes as covering minimization problems but now using Equality matrices as the basic building block. The communication matrix for Equality is simply the $2^n \times 2^n$ identity matrix. Therefore, the set of inputs on which an Equality oracle call yields the answer 1 has the same basic structure as the identity matrix, potentially with some rearrangements as the players may locally map their inputs to other values in the query to the oracle. We will use the vocabulary of Hambardzumyan, Hatami, and Hatami [15] who call such blowups of the identity matrix *blocky matrices*:

▶ **Definition 1.** *A* blocky matrix *is an identity matrix, perhaps with some rows and columns deleted, duplicated, or permuted, and perhaps with all-zero rows or columns added. Equivalently, a blocky matrix takes value 1 on a set $\mathcal{R}$ of rectangles, where any pair of rectangles in $\mathcal{R}$ have disjoint row and column sets, and value 0 elsewhere.*

See Figure 1 for some examples of blocky matrices.

We define the blocky cover number of M, $C_1^B(M)$, to be the minumum number of blocky matrices that are needed to cover the ones of M, and the blocky partition number of M, $\chi_1^B(M)$, to be the minimum number of blocky matrices that are needed to *disjointly* cover the ones of M. (See Section 2 for formal definitions.) We note that blocky cover number and blocky partition number are a generalization of the standard notions of cover number and partition number, and thus understanding properties of blocky cover and partition number is an important tool for proving lower bounds for models of computation that have access to Equality oracles.

[15] defined the *blocky rank* of M to be the minimum r such that M can be written as a linear combination of r blocky matrices. Our definitions of covering and partition minimization by blocky matrices can be seen as flavors of blocky rank, similar to the various flavors of rank and γ_2 norm (e.g., approximate rank, sign rank, approximate γ_2, etc.) Here again we see that complexity measures based on blocky rank measures are robust and come up naturally in other areas. For example, Hambardzumyan, Hatami, and Hatami [15] observed that blocky rank arises in operator theory where it is connected to idempotents in Schur algebras, and unambiguous blocky complexity is related to covering problems in graph theory. Another recent result is that a blocky version of sign rank essentially characterizes the size of depth-2 linear threshold circuits [3].

1.2 Our Results

New Characterizations

As mentioned above, nondeterministic, co-nondeterministic and deterministic communication complexity are characterized by 1-cover number, 0-cover number and partition number, respectively. We prove similar characterizations for nondeterministic communication classes equipped with an EQUALITY oracle.

▶ **Theorem 2** (Simplified). *Let F be a communication function on n bits. Let A be its corresponding $2^n \times 2^n$ Boolean communication matrix. Then*

$$\mathsf{UP}^{\mathsf{EQcc}}(F) \leq \log \chi_1^B(A) \leq O\left(\mathsf{UP}^{\mathsf{EQcc}}(F) \cdot \log n\right).$$

Also,

$$\mathsf{NP}^{\mathsf{EQcc}}(F) = \log C_1^B(A) \leq O\left(\mathsf{NP}^{\mathsf{EQcc}}(F) \cdot \log n\right).$$

In order to prove the above theorem, we define matrix-analytic characterizations of these classes by variants of a new *binary* version of the well-studied γ_2 norm. Recall that the γ_2 norm of a matrix M is at most r if M can be decomposed into the product of matrices X and Y such that all rows of X and columns of Y have ℓ_2-norm at most r. This norm and its approximate version are relaxations of the rank and approximate rank of M and have several equivalent characterizations and many applications. (See [21] for a comprehensive survey.) For a Boolean matrix M, we define the *binary* γ_2 of M, $\gamma_{2,B}(M)$, by restricting X and Y to be Boolean matrices. The binary generalization of the measure γ_2^∞, $\gamma_{2,B}^\infty(M)$, is defined similarly. (See Section 2 for formal definitions.) En route to proving Theorem 2, we show that $\gamma_{2,B}$ characterizes $\mathsf{UP}^{\mathsf{EQcc}}$ complexity and $\gamma_{2,B}^\infty$ characterizes $\mathsf{NP}^{\mathsf{EQcc}}$ complexity.

As a byproduct of the above proofs we obtain the following corollary, showing that multiple EQUALITY calls is no more powerful than a single EQUALITY call with respect to $\mathsf{UP}^{\mathsf{EQcc}}$ and $\mathsf{NP}^{\mathsf{EQcc}}$. Note that in contrast this is false with respect to $\mathsf{P}^{\mathsf{EQcc}}$ as [28] exhibited total functions easy for deterministic protocols with k EQUALITY calls but hard for deterministic protocols with less than k EQUALITY calls.

▶ **Corollary 3.** *With respect to unambiguous and nondeterministic communication, Turing-style and many-one style reductions to* EQUALITY *are polynomially equivalent. That is,* $\mathsf{UP}^{\mathsf{EQcc}} = \mathsf{U} \cdot \mathsf{EQ}^{\mathsf{cc}}$ *and* $\mathsf{NP}^{\mathsf{EQcc}} = \exists \cdot \mathsf{EQ}^{\mathsf{cc}}$.

New Separations

In a beautiful paper, Chattopadhyay, Mande, and Sherif disproved the log approximate rank conjecture by exhibiting a total function that has low approximate rank but requires large $\mathsf{BPP}^{\mathsf{cc}}$ complexity [10]. We observe that the same function also has low $\mathsf{UP}^{\mathsf{EQcc}}$ complexity, thereby obtaining the following new separation:

▶ **Theorem 4.** $\mathsf{UP}^{\mathsf{EQcc}} \not\subset \mathsf{coMA}^{\mathsf{cc}}$

As a corollary, we show that $\mathsf{P}^{\mathsf{EQcc}} \neq \mathsf{UP}^{\mathsf{EQcc}}$, and thus Yannakakis' result [30], showing that $\mathsf{P}^{\mathsf{cc}} = \mathsf{UP}^{\mathsf{cc}}$, breaks in the presence of EQUALITY oracles.

Our second separation concerns the strength of deterministic communication equipped with an EQUALITY oracle versus unrestricted randomized communication. As mentioned above, Chattopadhyay, Lovett and Vinyals [9] proved that there is a total function in $\mathsf{BPP}^{\mathsf{cc}}$

but with linear $\mathsf{P}^{\mathsf{EQcc}}$ complexity, thus proving $\mathsf{BPP}^{\mathsf{cc}} \not\subset \mathsf{P}^{\mathsf{EQcc}}$. (In fact their hard function is in $\mathsf{coRP}^{\mathsf{cc}}$, thus proving $\mathsf{coRP}^{\mathsf{cc}} \not\subset \mathsf{P}^{\mathsf{EQcc}}$.) The next theorem strengthens their separation by showing that their function remains hard even for nondeterministic protocols with an Equality oracle.

▶ **Theorem 5** (Simplified). $\mathsf{coRP}^{\mathsf{cc}} \not\subset \mathsf{NP}^{\mathsf{EQcc}}$ *(and therefore* $\mathsf{BPP}^{\mathsf{cc}} \not\subset \mathsf{NP}^{\mathsf{EQcc}}$ *and* $\mathsf{MA}^{\mathsf{cc}} \not\subset \mathsf{NP}^{\mathsf{EQcc}}$*).*

The outline of the remainder of the paper is as follows. Section 2 contains background information, definitions and notation. Section 3 develops basic properties of the new Boolean γ_2 measure, which are used to prove our main equivalences (Theorem 2). In Section 4 we prove our separation theorems (Theorem 4 and Theorem 5). We conclude in Section 5 with a discussion of our results and how they fit into the communication complexity landscape, and highlight several intriguing open questions.

2 Preliminaries

A combinatorial rectangle (or simply "rectangle") is a product set $R = X \times Y$, where X is a set of rows over some universe $\mathcal{X}$ and Y is a set of columns over some universe $\mathcal{Y}$. We say that R *contains* a row x if $x \in X$ (or a column y if $y \in Y$).

A rectangle is often interpreted in this paper as a matrix over $\mathcal{X} \times \mathcal{Y}$ where the entries in $X \times Y$ are given value 1 and the other entries are given value 0. For example, if we say that matrix A is the sum of a set of rectangles, we mean that A is the sum of the matrices based on those rectangles.

For a matrix A, a *monochromatic rectangle of* A is a rectangle whose corresponding entries in A have constant value. Often this value is specified; i.e. a combinatorial rectangle in A that contains only ones is a *1-monochromatic rectangle.*

We say that a set of rectangles $\mathcal{R}$ *covers* a subset $\mathcal{S}$ of coordinates in a matrix A if every coordinate $(i, j) \in \mathcal{S}$ is contained in some $R \in \mathcal{R}$ and no coordinates outside of $\mathcal{S}$ are contained in any $R \in \mathcal{R}$. Such a set is called a *cover* of $\mathcal{S}$. For example, if $\mathcal{R}$ contains exactly the coordinates in A whose entries take value 1, $\mathcal{R}$ is a cover of the ones of A. Furthermore, if the rectangles of $\mathcal{R}$ are disjoint (i.e. they do not overlap), $\mathcal{R}$ is a *partition* and is said to partition $\mathcal{S}$.

For two matrices A, A' of the same size, $A \circ A'$ represents the entry-wise product.

Blocky cover number and blocky partition number

We define matrix measures similar to partition number and cover number, but in terms of blocky matrices instead of combinatorial rectangles.

▶ **Definition 6.** *For a* $\{0,1\}$*-valued matrix* A*, the* blocky partition number *of* A*, denoted* $\chi_1^B(A)$*, is the minimal* r *such that* A *can be expressed as the sum of* r *blocky matrices.*

▶ **Definition 7.** *For a* $\{0,1\}$*-valued matrix* A*, the* blocky cover number *of* A*, denoted* $C_1^B(A)$*, is the minimal* r *such that* A *can be expressed as the entry-wise* Or *of* r *blocky matrices. That is, if* $A[i,j] = 1$ *then the sum of the blocky matrices is at least 1, and otherwise the sum is 0.*

An equivalent way to define these would be that $\chi_1^B(A)$ is the minimum number of blocky matrices such that their constituent rectangles *partition* the ones of A, and $C_1^B(A)$ is the minimum number of blocky matrices such that their constituent rectangles *cover* A – this

definition justifies the names "blocky partition number" and "blocky cover number". It also motivates the definition of two related measures: $\chi_0^B(A)$ is the minimum number of blocky matrices needed to partition the *zeroes* of A, and $C_0^B(A)$ is defined similarly.

2.1 Communication complexity

We assume familiarity with the basics of communication complexity [19, 29]. This paper uses the now-common notation for communication classes and models of Babai, Frankl, and Simon [4]. Denote the complexity of a function F in a given communication model as $\mathcal{C}^{\mathsf{cc}}(F)$, where $\mathcal{C}$ is an analogous class in classical complexity theory. As a slight abuse of notation, "$\mathcal{C}^{\mathsf{cc}}$" is used both to refer to the set of functions with $\mathcal{C}^{\mathsf{cc}}(F) \leq \text{polylog}(n)$ and to the communication model itself.

For most of the standard communication models we reference in this paper – P^{cc}, $\mathsf{BPP}^{\mathsf{cc}}$, $\mathsf{RP}^{\mathsf{cc}}$, $\mathsf{NP}^{\mathsf{cc}}$, and $\mathsf{MA}^{\mathsf{cc}}$ – we point the reader towards Appendix B of the survey by Göös, Pitassi, and Watson for definitions [13]. The only standard model we will need that is not defined in that paper is $\mathsf{UP}^{\mathsf{cc}}$, the model with *unambiguous* nondeterminism.

▶ **Definition 8.** $\mathsf{UP}^{\mathsf{cc}}$ *is the* unambiguous nondeterministic *model, where a prover sends the players a witness string, after which the players proceed deterministically. If the correct output is* 1*, there must always be* exactly one *witness that leads the players to accept; if the correct output is* 0*, there must never be such a witness. The cost of a protocol in the* $\mathsf{UP}^{\mathsf{cc}}$ *model is the number of bits needed to encode the witness plus the maximum depth of the deterministic portion.*

Classes based on equality

We are interested in models of communication that are augmented with the ability to compute the Equality function. To capture this notion, we first define a model of computation that makes a single call to Equality and outputs the answer from that call.

▶ **Definition 9** (Equality-based communication)**.** *A function F has a protocol in the model* $\mathsf{EQ}^{\mathsf{cc}}$ *if there exist some functions f_X and f_Y such that $F(x, y) \equiv f_X(x) = f_Y(y)$. The cost of any such protocol is 1.*

This is a strange definition, as it does not assign a cost to most functions: no suitable f_X and f_Y exist for most F. Indeed, the only functions with a $\mathsf{EQ}^{\mathsf{cc}}$ protocol are those whose communication matrix is a blocky matrix! The restricted nature of $\mathsf{EQ}^{\mathsf{cc}}$ means that it is only truly useful when examining its composition with other models. To this end, we next define an oracle model where Equality may be queried multiple times.

▶ **Definition 10** (Communication with equality oracle queries)**.** *Let $\mathcal{C}^{\mathsf{cc}}$ be any communication model in which the parties can send messages deterministically. The model $\mathcal{C}^{\mathsf{EQcc}}$ is the same as $\mathcal{C}^{\mathsf{cc}}$ except that at any step where a party would send a bit deterministically, the parties locally compute some functions $f_X(x, \pi)$ and $f_Y(y, \pi)$ (where π is the transcript so far) and learn whether or not $f_X(x, \pi) = f_Y(y, \pi)$. The cost for computing this equality is 1, and the cost is otherwise defined the same as in $\mathcal{C}^{\mathsf{cc}}$.*

The three models of most interest to us are $\mathsf{P}^{\mathsf{EQcc}}$, $\mathsf{NP}^{\mathsf{EQcc}}$, and $\mathsf{UP}^{\mathsf{EQcc}}$. To aid in our proofs we will give explicit definitions of these models that highlight the structure of a protocol.

▶ **Definition 11.** *A* $\mathsf{P}^{\mathsf{EQcc}}$ *protocol is a decision tree. Each internal node* v *of the tree corresponds to oracle queries to the* Equality *function: that is, it tests whether* $f_X(x,\pi) = f_Y(y,\pi)$ *where* π *is the transcript that leads to node* v*. The internal nodes each have two children, corresponding to "yes" and "no" answers to the query. Each leaf node* w *of the tree corresponds to an output* o_w*. The output of the protocol is computed by starting at the root node, making the oracle query, traversing to the appropriate child, continuing this process and halting upon reaching a leaf* w*, where we output* o_w*. The cost of the* $\mathsf{P}^{\mathsf{EQcc}}$ *protocol is the depth of the decision tree.*

▶ **Definition 12.** *An* $\mathsf{NP}^{\mathsf{EQcc}}$ *protocol is a collection of* 2^m $\mathsf{P}^{\mathsf{EQcc}}$ *protocols with depth at most* d*. The function computed by this* $\mathsf{NP}^{\mathsf{EQcc}}$ *is the* Or *of the functions computed by the* $\mathsf{P}^{\mathsf{EQcc}}$ *protocols. The cost of the* $\mathsf{NP}^{\mathsf{EQcc}}$ *protocol is* $m + d$*.*

The definition of $\mathsf{UP}^{\mathsf{EQcc}}$ is similar to the above, and only requires the addition of the unambiguity constraint.

▶ **Definition 13.** *A* $\mathsf{UP}^{\mathsf{EQcc}}$ *protocol is a collection of* 2^m $\mathsf{P}^{\mathsf{EQcc}}$ *protocols with depth at most* d *where no two of these* $\mathsf{P}^{\mathsf{EQcc}}$ *protocols have an input on which they both return 1 (that is, their supports are pairwise disjoint). The function computed by this* $\mathsf{UP}^{\mathsf{EQcc}}$ *is the* Or *of the functions computed by the* $\mathsf{P}^{\mathsf{EQcc}}$ *protocols. The cost of the* $\mathsf{UP}^{\mathsf{EQcc}}$ *protocol is* $m + d$*.*

Many-one reduction classes

As discussed in the introduction, the model $\mathcal{C}^{\mathsf{EQcc}}$ represents a *Turing reduction* from the model $\mathcal{C}^{\mathsf{cc}}$ to the Equality function. In order to reason about *many-one reductions* to Equality, we use counting class notation: this notation is standard in classical complexity, see [16].

▶ **Definition 14.** *An* $\exists \cdot \mathsf{EQ}^{\mathsf{cc}}$ *(respectively* $\mathsf{U} \cdot \mathsf{EQ}^{\mathsf{cc}}$*) protocol is an* $\mathsf{NP}^{\mathsf{EQcc}}$ *(respectively* $\mathsf{UP}^{\mathsf{EQcc}}$*) protocol where the constituent* $\mathsf{P}^{\mathsf{EQcc}}$ *protocols have depth 1 and simply return the output of the* Equality *query.*

2.2 The γ_2 norm and variants

Let A be a matrix. The γ_2 norm of A is defined as:

$$\gamma_2(A) = \min_{\substack{X,Y \\ XY^\top = A}} r(X) r(Y)$$

where $r(M)$ is the maximum ℓ_2 norm of any row of M. This is indeed a norm, which can be proven by examining the semidefinite program that computes it [22].

If A is $\{0,1\}$-valued, then $\gamma_2(A) \leq O(\sqrt{\mathrm{rank}(M)})$ – see the book of Lee and Shraibman for more details [21]. The γ_2 norm turns out to be very closely related with other natural generalizations of rank. We can write a real matrix as $\sum_i \alpha_i R_i$, where the α_i are weights and the R_i are rank-one $\{0,1\}$-matrices (i.e. rectangles). The μ-norm of a matrix is the minimum of $\sum_i |\alpha_i|$ over $\{\alpha_i\}, \{R_i\}$ where $\sum_i \alpha_i R_i$ equals the matrix. The ν-norm is defined similarly, but where the rank-one $\{0,1\}$-matrices are replaced with rank-one $\{-1,1\}$-valued matrices. By an application of norm duality and Grothendieck's Inequality, for any real matrix A we have $\gamma_2(A) \leq \nu(A) \leq \mu(A) \leq 4K_G\gamma_2(A)$ where K_G is Grothendieck's constant [23].

The above relationship between γ_2 and rank means that the γ_2 norm can be used to lower bound deterministic communication complexity, as $\log \operatorname{rank}(A)$ lower bounds deterministic communication complexity. This is perhaps uninteresting, as rank itself is a tighter lower bound: for example, the communication matrix of EQUALITY has constant γ_2 but exponentially high rank. The power of γ_2 in currently-known communication lower bounds arises when we consider its *approximate* variant.

Approximate norms

Every matrix measure Φ has an associated α-approximate variant. Let A be a $\{0,1\}$-valued matrix. We say that A' α-approximates A if A' is positive on entries where A is 1, is non-positive on entries where A is 0, and differs entrywise from A by at most α. The α-approximate Φ of A, denoted $\Phi^\alpha(A)$, is the minimum $\Phi(A')$ over all A' that α-approximate A. See the book of Lee and Shraibman [21] for more discussion on this definition.[1]

$$\Phi^\alpha(A) = \min_{\substack{A' \text{ where } \forall x,y: \\ \text{if } A[x,y]=0 \text{ then } A'[x,y]\leq 0 \\ \text{if } A[x,y]=1 \text{ then } A'[x,y]\geq 1 \\ \|A-A'\|_\infty \leq \alpha}} \Phi(A').$$

Let A_F be the communication matrix of some function F. For any constant α, $\log \gamma_2^\alpha(A_F)$ lower bounds randomized communication complexity of F [24]. This can be proven directly or by using $\gamma_2^\alpha(A_F) = \Theta(\operatorname{rank}^\alpha(A_F))$ [20] and the fact that $\log \operatorname{rank}^\alpha(A_F)$ lower bounds randomized communication complexity [18]. This demonstrates the power of γ_2^α in practice: whereas the approximate rank of a matrix is not known to be efficiently computable, $\gamma_2^\alpha(A_F)$ can be computed by a semidefinite program.

Motivated by taking the limit as α approaches infinity, we can also define the associated infinity variant:

$$\Phi^\infty(A) = \min_{\substack{A' \text{ where } \forall x,y: \\ \text{if } A[x,y]=0 \text{ then } A'[x,y]\leq 0 \\ \text{if } A[x,y]=1 \text{ then } A'[x,y]\geq 1}} \Phi(A').$$

Again letting A_F be the communication matrix of some function F, there is an asymptotically tight connection between $\log \gamma_2^\infty(A_F)$ and the discrepancy of combinatorial rectangles in A_F [23], which itself is known to be a tight bound on the so-called weakly-unbounded randomized communication complexity of F (this model is denoted $\mathsf{PP}^{\mathsf{cc}}$) [17].

Binary γ_2

We are interested in a variant of the γ_2 norm obtained by restricting the matrices X and Y in the factorization of A to have entries in $\{0,1\}$.

$$\gamma_{2,B}(A) = \min_{\substack{\{0,1\}\text{-matrices } X,Y \\ XY^\top = A}} r(X)r(Y)$$

This variant is not a norm. In fact, $\gamma_{2,B}(A)$ is only defined if the entries of A are non-negative integers. However, some useful properties of norms still hold for $\gamma_{2,B}$. See Section 3.1 for some of these.

---

[1] Lee and Shraibman define α-approximation for $\{-1,1\}$-valued matrices, and the definition ends up being a bit simpler. However, our results overall are cleaner if we use $\{0,1\}$-valued matrices, so we suffer a bit of mess here.

For our applications we will also use the infinity variant of $\gamma_{2,B}$. Since $\gamma_{2,B}$ is only defined for non-negative integer matrices, the constraint on the zeroes of the approximating matrix must hold with equality. Explicitly:

$$\gamma^{\infty}_{2,B}(A) = \min_{\substack{A' \text{ where } \forall x,y: \\ \text{if } A[x,y]=0 \text{ then } A'[x,y]=0 \\ \text{if } A[x,y]=1 \text{ then } A'[x,y]\geq 1}} \gamma_{2,B}(A').$$

3 Characterizations

In this section we prove the matrix characterizations of nondeterministic communication models with EQUALITY oracles.

3.1 Properties of γ_2 variants

First we will prove some helpful properties of $\gamma_{2,B}$. We begin by giving an alternate definition of $\gamma_{2,B}$ that will be more convenient to work with. Intuitively, optimizing $\gamma_{2,B}$ is equivalent to finding a partition of the ones of a matrix into combinatorial rectangles that minimizes the number of rectangles containing any row or column.

▶ **Lemma 15.** *Let A be a matrix whose values are non-negative integers. Let $\mathcal{R}$ be a set of combinatorial rectangles with $\sum_{R\in\mathcal{R}} R = A$ that minimizes $\sqrt{k_x k_y}$, where k_x (respectively k_y) is the maximum number of rectangles in $\mathcal{R}$ that contain any row (respectively column) of A. Then $\gamma_{2,B}(A) = \sqrt{k_x k_y}$.*

Proof. We begin by rearranging the terms in the definition of $\gamma_{2,B}$ to focus on the columns of the factor matrices X and Y. Letting $\{u\}$ be the columns of X and $\{v\}$ be the columns of Y, it is easy to see that $\gamma_{2,B}$ can be written as:

$$\gamma_{2,B}(A) = \min_{\substack{\{u\},\{v\} \text{ sets of } \{0,1\}\text{-valued vectors} \\ \sum_i u_i v_i^\top = A}} \max_{x,y} \sqrt{\sum_i \langle e_x, u_i\rangle^2} \sqrt{\sum_i \langle e_y, v_i\rangle^2}$$

where e_x is the vector that is 1 at location x and 0 elsewhere.

We can now verify that the characterization in the statement of the lemma is correct. Since all vectors in $\{u\}$ and $\{v\}$ are $\{0,1\}$-valued, the outer products $u_i v_i^\top$ are combinatorial rectangles. The sum of these rectangles is A. The expressions $\sum_i \langle e_x, u_i\rangle^2$ and $\sum_i \langle e_y, v_i\rangle^2$ are exactly k_x and k_y, respectively.[2] Therefore, finding an optimal $\mathcal{R}$ as stated is exactly the same as finding an optimal factorization of A. ◀

The alternate definition given in Lemma 15 allows for particularly simple proofs of the following properties.

▶ **Lemma 16.** *The measure $\gamma_{2,B}$ does not increase if a matrix has its rows or columns deleted, duplicated, or rearranged, or if all-zeros rows or columns are added.*

Proof. All of these operations allow us to keep the same structure of decomposition into rectangles. ◀

[2] Note that the exponents here are unnecessary, as the value of the inner products are always zero or one. We include these only to highlight the equivalence with the ℓ_2-norm in the definition of $\gamma_{2,B}$.

▶ **Lemma 17.** *Any blocky matrix B has $\gamma_{2,B}(B) = 1$.*

Proof. The identity matrix has a $\gamma_{2,B}$ of 1 (the factor matrices are both the identity matrix). Apply Lemma 16. ◀

▶ **Lemma 18.** *Let A_1 and A_2 be two $\{0,1\}$-valued matrices of the same dimensions. Then*

$$\gamma_{2,B}(A_1 \circ A_2) \leq \gamma_{2,B}(A_1)\gamma_{2,B}(A_2).$$

Proof. For $i = 1, 2$, let $\mathcal{R}_i$ be a partition of the ones of A_i into 1-monochromatic rectangles achieving the minimum for $\gamma_{2,B}(A_i)$. Then $\{R \circ R' : R \in \mathcal{R}_1, R' \in \mathcal{R}_2\}$ is a partition of the ones of $A_1 \circ A_2$ into 1-monochromatic rectangles. If a row or column intersect $R \circ R'$ then it intersects both R and R'. ◀

▶ **Lemma 19.** *Let A_1 and A_2 be two $\{0,1\}$-valued matrices of the same dimensions whose sets of 1-entries are disjoint. Then*

$$\gamma_{2,B}(A_1 + A_2) \leq \gamma_{2,B}(A_1) + \gamma_{2,B}(A_2).$$

Proof. For $i = 1, 2$, let $\mathcal{R}_i$ be a partition of A_i achieving the minimum for $\gamma_{2,B}(A_i)$. Then $\mathcal{R}_1 \cup \mathcal{R}_2$ is a partition of the ones of $A_1 + A_2$ into 1-monochromatic rectangles. Every row and column intersect at most $\gamma_{2,B}(A_1) + \gamma_{2,B}(A_2)$ rectangles in this partition. ◀

Note that Lemma 19 does not give us subadditivity in situations where the ones of A_1 and A_2 are not disjoint. In fact, such a property does not hold.

We finish this subsection by proving tight bounds for the $\gamma_{2,B}$ of matrices of a specific form.

▶ **Lemma 20.** *$\gamma_{2,B}(J_n - I_n) = \Theta(\log n)$, where J_n is the $n \times n$ all-ones matrix.*

Proof. Let $E_n = J_n - I_n$. Then the following recursive structure exists:

$$E_{2n} = \begin{pmatrix} E_n & J_n \\ J_n & E_n \end{pmatrix}.$$

It follows that $\gamma_{2,B}(E_{2n}) \leq \gamma_{2,B}(E_n) + 1$, and therefore $\gamma_{2,B}(E_n) \leq O(\log n)$.

The lower bound follows from Claim 7 in [27], which relies of a bound from [5]. The claim says that if $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ are Boolean vectors satisfying that $x_i y_j^t = 0$ if and only if $i = j$, then there is some $i \in [n]$ for which the number of ones in x_i plus the number of ones in y_i is at least $\Omega(\log n)$. ◀

Combining Lemma 16 and Lemma 20 gives us the following useful corollary.

▶ **Corollary 21.** *$\gamma_{2,B}(J_n - B) = O(\log n)$, where J_n is the $n \times n$ all-ones matrix and B is any blocky matrix.*

3.2 Connections between blocky measures and γ_2 variants

Here we prove that blocky partition has a polynomial relationship with $\gamma_{2,B}$ and blocky cover has a polynomial relationship with $\gamma^{\infty}_{2,B}$. Again, Lemma 15 helps us keep things simple.

▶ **Lemma 22.** *Let A be a $\{0,1\}$-valued matrix. Then:*

$$\gamma_{2,B}(A) \leq \chi_1^B(A) \leq (\gamma_{2,B}(A))^2 \qquad \text{and} \qquad \gamma^{\infty}_{2,B}(A) \leq C_1^B(A) \leq (\gamma^{\infty}_{2,B}(A))^2.$$

Proof. In the following, let A' be the matrix that ∞-approximates A in the definition of $\gamma^{\infty}_{2,B}(A)$: that is, $\gamma_{2,B}(A') = \gamma^{\infty}_{2,B}(A)$ and A' is a matrix with non-negative integer values and the same non-zero coordinates as A.

For a matrix M whose entries are non-negative integers let $\mathcal{B}$ be a set of blocky matrices such that $\sum_{B\in\mathcal{B}} B = M$. Then at most a single rectangle from each of these blocky matrices can contain any given row or column of M, as the rectangles of each blocky matrix have pairwise disjoint row and column sets. By Lemma 15, this means that the constituent rectangles of $\mathcal{B}$ give an upper bound of $\gamma_{2,B}(M) \leq \sqrt{|\mathcal{B}| \cdot |\mathcal{B}|} = |\mathcal{B}|$. If $M = A$, then $\mathcal{B}$ is a partition of the ones of A into blocky matrices, and so we can set $\mathcal{B}$ such that $|\mathcal{B}| = \chi^{B}_{1}(A)$. If $M = A'$, then $\mathcal{B}$ is a cover of the ones of A into blocky matrices, and so we can set $\mathcal{B}$ such that $|\mathcal{B}| = C^{B}_{1}(A)$.

We now prove the other direction. Again, let M be a matrix whose entries are non-negative integers. Let $\mathcal{R}$ be the optimal decomposition of M into combinatorial rectangles as in the statement of Lemma 15 and let k_x/k_y be the associated row/column counts. Fix some order on $\mathcal{R}$. Define a set of $k_x k_y$ blocky matrices $\mathcal{B}$ as follows: for integers $0 < i \leq k_x$ and $0 < j \leq k_y$, blocky matrix $B_{i,j} \in \mathcal{B}$ is the set of row-column pairs (x, y) that are in the ith rectangle that contains row x and the jth rectangle that contains column y (according to the order that we fixed previously).

One can see that this definition of $B_{i,j}$ does indeed yield a blocky matrix. Each entry in the support of $B_{i,j}$ is also in the support of some rectangle in $\mathcal{R}$, and for any $R \in \mathcal{R}$, it is easy to see that the portion of R included in $B_{i,j}$ is a product set – inclusion in $B_{i,j}$ relies only on fulfilling the ordering property on both the row and column – and that its rows and columns are not shared with any other rectangle in $B_{i,j}$ – only one rectangle R can be the ith rectangle containing a row or the jth rectangle containing a column. Furthermore, each entry in the support of $R \in \mathcal{R}$ is covered by some blocky matrix in $\mathcal{B}$. Given this, we can see that the sum of the matrices in $\mathcal{B}$ is M.

The size of $\mathcal{B}$ is $k_x k_y = (\gamma_{2,B}(M))^2$. If $M = A$, $\mathcal{B}$ is a blocky partition of the ones of M because $\mathcal{R}$ was a partition, and so $\mathcal{B}$ witnesses $\chi^{B}_{1}(A) \leq (\gamma_{2,B}(A))^2$. If $M = A'$, then $\mathcal{B}$ is a blocky covering of A and so $C^{B}_{1}(A) \leq (\gamma^{\infty}_{2,B}(A))^2$. ◀

3.3 Characterizations of equality-based protocols

We can now move on to proving the characterizations of EQUALITY-based communication classes. The proof techniques are essentially the same between the two theorems. Therefore, we will state the intermediate lemmas in terms of both nondeterminism and unambiguous nondeterminism.

▶ **Lemma 23.** *Let F be a communication function on n bits. Let A be its corresponding $2^n \times 2^n$ Boolean communication matrix. Then*

$$\log \gamma_{2,B}(A) \leq O\left(\mathsf{UP}^{\mathsf{EQcc}}(F) \cdot \log n\right) \qquad \textit{and} \qquad \log \gamma^{\infty}_{2,B}(A) \leq O\left(\mathsf{NP}^{\mathsf{EQcc}}(F) \cdot \log n\right).$$

Proof. Let Π be either a $\mathsf{UP}^{\mathsf{EQcc}}$ or $\mathsf{NP}^{\mathsf{EQcc}}$ protocol for F with 2^m constituent $\mathsf{P}^{\mathsf{EQcc}}$ protocol trees T_i of depth at most d. We can associate any node v of T_i with a Boolean matrix whose set of 1-entries characterizes the subset of entries (x, y) on which the protocol reaches v. Denote this matrix by M_v. As a simple example, for the root of the tree r, the matrix is $M_r = J_{2^n}$.

Let v be any node in T_i, and let u_L and u_R be its children. Recall that u_L will be reached if the EQUALITY query at v returned 0, and u_R will be reached if that query returned 1. Then there is some blocky matrix B such that:

- $M_{u_R} = M_v \circ B$.
- $M_{u_L} = M_v \circ (J_{2^n} - B)$.

Therefore, if v has depth d' in T_i, M_v can be expressed as the entrywise product of d' matrices that are either blocky or J_{2^n} minus a blocky matrix. By Lemma 17, Lemma 18, and Corollary 21, this implies that for every node v in T, $\gamma_{2,B}(M_v) \leq (n)^{d'}$.[3]

Now we can prove the desired bounds. Let $\mathcal{L}$ be the set of all leaves ℓ of the trees T_i where the corresponding $\mathsf{P}^{\mathsf{EQcc}}$ protocol would output 1. There are at most $2^d 2^m$ such leaves.

If Π is a $\mathsf{UP}^{\mathsf{EQcc}}$ protocol, then for $\ell \in \mathcal{L}$ the corresponding matrices M_ℓ have disjoint 1-entries: leaves of a given tree will have disjoint 1-entries, and the inputs on which the trees output 1 are disjoint. Therefore, $A = \sum_{\ell \in \mathcal{L}} M_\ell$, and so by Lemma 19 we have $\gamma_{2,B}(A) \leq (2n)^{d+m}$. Rearranging, we get $\log \gamma_{2,B}(A) \leq O\left((d+m) \cdot \log n\right)$.

If Π is an $\mathsf{NP}^{\mathsf{EQcc}}$ protocol, a similar analysis holds, but we no longer have the property that the inputs on which the trees output 1 are disjoint. Instead, we have that there is some matrix $A' = \sum_{\ell \in \mathcal{L}} M_\ell$ which is non-zero exactly when A is non-zero. As above, by Lemma 19 we have $\gamma_{2,B}(A') \leq (2n)^{d+m}$. By the definition of $\gamma^{\infty}_{2,B}$, this means that $\gamma^{\infty}_{2,B}(A) \leq (2n)^{d+m}$. Again, we can rearrange to yield $\log \gamma^{\infty}_{2,B}(A) \leq O\left((d+m) \cdot \log n\right)$. ◀

▶ **Lemma 24.** *Let F be a communication function on n bits. Let A be its corresponding $2^n \times 2^n$ Boolean communication matrix. Then*

$$\mathsf{U} \cdot \mathsf{EQ}^{\mathsf{cc}}(F) = \log \chi^B_1(A) \qquad \textit{and} \qquad \exists \cdot \mathsf{EQ}^{\mathsf{cc}}(F) = \log C^B_1(A).$$

Proof. If $\mathcal{B}$ is a partition (respectively cover) of the ones of A then in a $\mathsf{U} \cdot \mathsf{EQ}^{\mathsf{cc}}$ (respectively $\exists \cdot \mathsf{EQ}^{\mathsf{cc}}$) protocol the nondeterministic witness can simply specify which blocky matrix in $\mathcal{B}$ has the input in its support, and the parties can determine whether this is correct using a single Equality call.

If Π is a $\mathsf{U} \cdot \mathsf{EQ}^{\mathsf{cc}}$ (respectively $\exists \cdot \mathsf{EQ}^{\mathsf{cc}}$) protocol, then the associated matrices of the constituent $\mathsf{P}^{\mathsf{EQcc}}$ trees are blocky and form a size 2^k partition (respectively covering) of the ones of A, where k is the cost of Π. ◀

▶ **Theorem 2.** *Let F be a communication function on n bits. Let A be its corresponding $2^n \times 2^n$ Boolean communication matrix. Then*

$$\mathsf{UP}^{\mathsf{EQcc}}(F) \leq \mathsf{U} \cdot \mathsf{EQ}^{\mathsf{cc}}(F) = \log \chi^B_1(A) = O(\log \gamma_{2,B}(A)) \leq O\left(\mathsf{UP}^{\mathsf{EQcc}}(F) \cdot \log n\right).$$

Also,

$$\mathsf{NP}^{\mathsf{EQcc}}(F) \leq \exists \cdot \mathsf{EQ}^{\mathsf{cc}}(F) = \log C^B_1(A) = O(\log \gamma^{\infty}_{2,B}(A)) \leq O\left(\mathsf{NP}^{\mathsf{EQcc}}(F) \cdot \log n\right).$$

Proof. The theorem follows from Lemma 22, Lemma 23, Lemma 24, and the facts that $\mathsf{U} \cdot \mathsf{EQ}^{\mathsf{cc}}(F) \geq \mathsf{UP}^{\mathsf{EQcc}}(F)$ and $\exists \cdot \mathsf{EQ}^{\mathsf{cc}}(F) \geq \mathsf{NP}^{\mathsf{EQcc}}(F)$ which follow easily from the definitions. ◀

4 Lower bounds and separations for equality protocols

In this section we prove our two separation results, both concerning the nondeterministic communication classes $\mathsf{UP}^{\mathsf{EQcc}}$ and $\mathsf{NP}^{\mathsf{EQcc}}$. The first separation, Theorem 4, establishes that there is a total function in $\mathsf{UP}^{\mathsf{EQcc}}$ (and thus also in $\mathsf{NP}^{\mathsf{EQcc}}$) that is not in $\mathsf{coMA}^{\mathsf{cc}}$. The second separation, Theorem 5, shows that there is a total function in $\mathsf{coRP}^{\mathsf{cc}}$ (and thus also in $\mathsf{BPP}^{\mathsf{cc}}$ and $\mathsf{MA}^{\mathsf{cc}}$) that is not in $\mathsf{NP}^{\mathsf{EQcc}}$.

[3] Corollary 21 is stated in terms of $n \times n$ matrices, whereas the matrices here are of dimension $2^n \times 2^n$.

4.1 Proof of Theorem 4

In this section we prove Theorem 4, restated below.

▶ **Theorem 4.** $\mathsf{UP}^{\mathsf{EQcc}} \not\subset \mathsf{coMA}^{\mathsf{cc}}$.

The *log rank conjecture* is a long-standing open problem that asks whether the deterministic communication complexity of a function and the rank of its communication matrix are polylogarithmically related. Similarly, the *log approximate rank conjecture* asks a similar question about the connection between *randomized* communication complexity and the *approximate* rank of its communication matrix. Chattopadhyay, Mande, and Sherif give a counterexample showing that the log approximate rank conjecture is false [10]. The function that they use in their separation is called Sink∘XOR.

▶ **Definition 25.** *The function* $\textsc{Sink} : \{0,1\}^{\binom{m}{2}} \to \{0,1\}$ *interprets its inputs as assigning directions to edges of the complete graph on* m *vertices and outputs 1 if that directed graph has a sink.*

The function $\textsc{Sink}\circ\textsc{XOR} : \{0,1\}^{\binom{m}{2}} \times \{0,1\}^{\binom{m}{2}} \to \{0,1\}$ *outputs the value of* $\textsc{Sink}(z)$*, where* $z = x \oplus y$ *is the entry-wise* XOR *of the inputs of* Sink∘XOR*.*

The main result of Chattopadhyay, Mande, and Sherif is that Sink∘XOR has logarithmic approximate rank but $\Omega(\sqrt{n})$ randomized communication complexity – here, n is the length of the inputs, so $n = \binom{m}{2}$. Indeed, they show the stronger result that $\mathsf{coMA}^{\mathsf{cc}}(\textsc{Sink}\circ\textsc{XOR}) = \Omega(n^{1/4})$.[4]

▶ **Lemma 26.** $\mathsf{U} \cdot \mathsf{EQ}^{\mathsf{cc}}(\textsc{Sink}\circ\textsc{XOR}) = O(\log n)$.

Proof. The witness indicates which vertex is the sink. As the graph defined in the problem is complete, there is always at most one sink, which means this witness is unambiguous. The parties then confirm that the vertex is a sink using a single Equality call as follows. For a vertex v, let $x[v]$ and $y[v]$ be the inputs x and y restricted to the bits whose XOR will determine the directions of the edges incident to v. Let w be the unique value such that v is a sink if and only if $x[v] \oplus y[v] = w$. The player that knows x can compute $x[v] \oplus w$, and then an Equality call can be used to determine if $x[v] \oplus w = y[v]$, which is the case if and only if v is a sink. ◀

Lemma 26, combined with the main result of [10] that $\mathsf{coMA}^{\mathsf{cc}}(\textsc{Sink}\circ\textsc{XOR}) = \Omega(n^{1/4})$, implies $\mathsf{UP}^{\mathsf{EQcc}} \not\subset \mathsf{coMA}^{\mathsf{cc}}$, thus proving Theorem 4. Of course, this also separates $\mathsf{UP}^{\mathsf{EQcc}}$ from subsets of $\mathsf{coMA}^{\mathsf{cc}}$; of particular interest is $\mathsf{P}^{\mathsf{EQcc}}$. Theorem 4 shows that the result of Yannakakis that $\mathsf{P}^{\mathsf{cc}} = \mathsf{UP}^{\mathsf{cc}}$ [30] does not hold when these classes are augmented with Equality oracles. Theorem 4 also shows that $\mathsf{UP}^{\mathsf{EQcc}}$ is not closed under complement: the negation of Sink∘XOR is in $\mathsf{coUP}^{\mathsf{EQcc}}$ but is not in $\mathsf{MA}^{\mathsf{cc}}$, which is a superset of $\mathsf{UP}^{\mathsf{EQcc}}$.

4.2 Proof of Theorem 5

Our main aim in this section is to prove Theorem 5 (restated below), giving a separation between $\mathsf{NP}^{\mathsf{EQcc}}$ and $\mathsf{MA}^{\mathsf{cc}}$.

[4] Actually, their result is even stronger than this: $\mathsf{coSBP}^{\mathsf{cc}}(\textsc{Sink}\circ\textsc{XOR}) = \Omega(\sqrt{n})$. The class $\mathsf{coSBP}^{\mathsf{cc}}$ represents the small bounded-error model, which tightly characterizes the (0-sided) corruption bound. It is known that $\mathsf{coMA}^{\mathsf{cc}}(F)^2 \geq \mathsf{coSBP}^{\mathsf{cc}}(F)$ for all F [14].

▶ **Theorem 5.** *There is a function F such that* $\mathsf{coRP}^{\mathsf{cc}}(F) = O(\log n)$, *but with* $\mathsf{NP}^{\mathsf{EQcc}}(F) = \Omega(n/\log n)$ *and* $\exists \cdot \mathsf{EQ}^{\mathsf{cc}}(F) = \Omega(n)$. *Therefore* $\mathsf{coRP}^{\mathsf{cc}} \not\subset \mathsf{NP}^{\mathsf{EQcc}}$ *and thus* $\mathsf{MA}^{\mathsf{cc}} \not\subset \mathsf{NP}^{\mathsf{EQcc}}$.

Chattopadhyay, Lovett, and Vinyals defined a lower bound technique that compares the size of the largest 1-monochromatic rectangle of a function's communication matrix with the number of ones of that function [9]. We call the matrix measure used in their proof max-rect.

▶ **Definition 27.** *Let A be a $\{0,1\}$-valued $m \times n$ matrix, where $\alpha(A)$ is the number of ones in A and $\beta(A)$ is the size of the largest 1-monochromatic rectangle in A. The* maximum-rectangle bound *A, denoted* $\mathsf{max\text{-}rect}(A)$, *is defined as:*

$$\mathsf{max\text{-}rect}(A) = \frac{\alpha(A)}{\sqrt{\beta(A)}\left(\frac{m+n}{2}\right)}.$$

Actually, this formulation of max-rect appeared in a preprint version of the aforementioned paper [8] – in the full version [9], a more complicated expression is given. This latter measure is used to give a tight (linear) lower bound on the $\mathsf{P}^{\mathsf{EQcc}}$ complexity of a function in $\mathsf{coRP}^{\mathsf{cc}}$. Using max-rect as defined here and in the preprint, the known techniques only give $\Omega(n/\log n)$ bounds.

▶ **Theorem 28** ([8, 9])**.** *There is a function $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ such that* $\mathsf{coRP}^{\mathsf{cc}}(F) = O(\log n)$ *and whose corresponding $2^n \times 2^n$ Boolean communication matrix A has* $\mathsf{max\text{-}rect}(A) = \Omega(2^n)$.

It turns out that max-rect is stronger than observed by Chattopadhyay, Lovett, and Vinyals, and can be shown to lower bound $\mathsf{NP}^{\mathsf{EQcc}}$ with just a few tweaks of the proof technique in the preprint [8]. This means that the function from Theorem 28 will work for our separation.

▶ **Theorem 29.** *Let A be a $\{0,1\}$-valued $m \times n$ matrix. Then* $C_1^B(A) \geq \Omega(\mathsf{max\text{-}rect}(A))$.

Proof of Theorem 29. Let $\mathcal{B}$ be a cover of the ones of A with $|\mathcal{B}| = C_1^B(A)$ and let $\mathcal{R}$ be the set of combinatorial rectangles in the blocky matrices of $\mathcal{B}$. For a rectangle $R_i \in \mathcal{R}$, we will use the notation $E_x(i)$ (respectively $E_y(i)$) for the event that x (respectively y) is contained in R_i. Because the matrices of $\mathcal{B}$ are blocky, each row or column can only be contained in at most $|\mathcal{B}|$ of these rectangles, i.e. $\sum_i E_x(i) \leq |\mathcal{B}|$ and $\sum_i E_y(i) \leq |\mathcal{B}|$.

Then we have the following relationship between $|\mathcal{B}|$ and these $R_i \in \mathcal{R}$:

$$\begin{aligned}(m+n)|\mathcal{B}| &\geq \sum_x \sum_i E_x(i) + \sum_y \sum_i E_y(i) = \sum_i \left(\sum_x E_x(i) + \sum_y E_y(i) \right) \\ &\geq 2 \sum_i \sqrt{\left(\sum_x E_x(i) \right) \left(\sum_y E_y(i) \right)} = 2 \sum_i \sqrt{\sum_{x,y} (E_x(i) E_y(i))} \\ &= 2 \sum_i \sqrt{|R_i|}.\end{aligned}$$

The second inequality above follows from the AM-GM inequality. Let $\alpha(A)$ and $\beta(A)$ be as in the definition of max-rect. Then, since the rectangles of $\mathcal{R}$ are 1-monochromatic rectangles that cover the ones of A, we have $\sum_i |R_i| \geq \alpha(A)$ and, for all i, $|R_i| \leq \beta(A)$. Together these constraints lower bound $\sum_i \sqrt{|R_i|}$ by the minimum of an optimization problem. This minimum is achieved if $\alpha(A)/\beta(A)$ of the R_i have area $\beta(A)$, which gives $\sum_i \sqrt{|R_i|} \geq \alpha(A)/\sqrt{\beta(A)}$. Combining everything, we get

$$C_1^B(A) \geq \Omega\left(\frac{\alpha(A)}{\sqrt{\beta(A)}\left(\frac{m+n}{2}\right)} \right) = \Omega(\mathsf{max\text{-}rect}(A)). \qquad \blacktriangleleft$$

Proof of Theorem 5. Combining Theorem 29 with our characterizations from Theorem 2:

$$\exists \cdot \mathsf{EQ}^{\mathsf{cc}}(F) = \log C_1^B(A) \text{ and}$$

$$\log C_1^B(A) \leq O\left(\mathsf{NP}^{\mathsf{EQcc}}(F) \cdot \log n\right),$$

we get our desired bounds. ◀

We remark that for $\mathsf{NP}^{\mathsf{EQcc}}$ we get the same $\log n$ term in the denominator as [8], but for $\exists \cdot \mathsf{EQ}^{\mathsf{cc}}$ we get the optimal linear lower bound.

5 Conclusion and open questions

Hambardzumyan, Hatami, and Hatami [15] initiated the study of blocky matrices and blocky rank. They showed that it is a robust notion that is not only relevant to the study of communication complexity, but also connected to central questions in operator theory. Avraham and Yehudayoff [3] prove additional connections to circuit complexity, combinatorics, and learning theory. Taken together, it seems clear that rank-like measures for blocky matrices are a fundamental and robust notion, and deserving of further study.

In this paper, we continued this investigation by studying restrictions of blocky rank, and show that they are equivalent to natural nondeterministic communication models equipped with Equality, and moreover, have a dual characterization in terms of a variant of the well-studied γ_2 norm. Our new characterizations of these communication classes in turn led to further understanding and new separation results.

This new line of inquiry has opened up several exciting new questions/directions, and could potentially shed new light on key open problems in the area, such as the log rank conjecture, and developing more tools and intuition for the poorly understood communication classes $\mathsf{MA}^{\mathsf{cc}}$ and $\mathsf{AM}^{\mathsf{cc}}$. Below we briefly discuss how these communication classes (and blocky rank measures) are related to the communication landscape, and mention a few specific open problems.

Figure 2 shows known relationships between the matrix measures and communication classes that are under study in this paper. A box containing a matrix measure in this diagram should be interpreted as the set of functions for which the value of that measure is polylogarithmic on their communication matrices. For example, the box with "log rank" includes all problems whose communication matrix has rank $2^{(\log n)^{O(1)}}$.

All of the relationships in Figure 2 are discussed in previous sections or follow straightforwardly from the definitions. In the remainder of this section, we will talk about a few of the gaps in this diagram, as well as some other intriguing open questions that naturally follow from our work.

$\mathsf{BPP}^{\mathsf{cc}}$ vs. $\mathsf{P}^{\mathsf{RPcc}}$

Two-sided randomness can simulate a deterministic protocol oracle calls to one-sided randomized protocols, but is the other way true? This question has received some interest in recent years, and separations are known between $\mathsf{BPP}^{\mathsf{cc}}$ and certain subsets of $\mathsf{P}^{\mathsf{RPcc}}$: the paper of Chattopadhyay, Lovett, and Vinyals discussed earlier shows that $\mathsf{BPP}^{\mathsf{cc}} \not\subset \mathsf{P}^{\mathsf{EQcc}}$ [9] and Pitassi, Shirley, and Watson show that limiting the number of RP calls allowed in $\mathsf{P}^{\mathsf{RPcc}}$ to a constant gives a weaker complexity class [28]. The ultimate goal of such research would be not only to resolve $\mathsf{BPP}^{\mathsf{cc}}$ vs. $\mathsf{P}^{\mathsf{RPcc}}$, but also understand $\mathsf{BPP}^{\mathsf{cc}}$ vs. $\mathsf{P}^{\mathsf{NPcc}}$. This latter question was explicitly raised by Göös, Pitassi and Watson [13]. Recall that we focus on total functions here – the relationship is already known when partial functions are allowed [26].

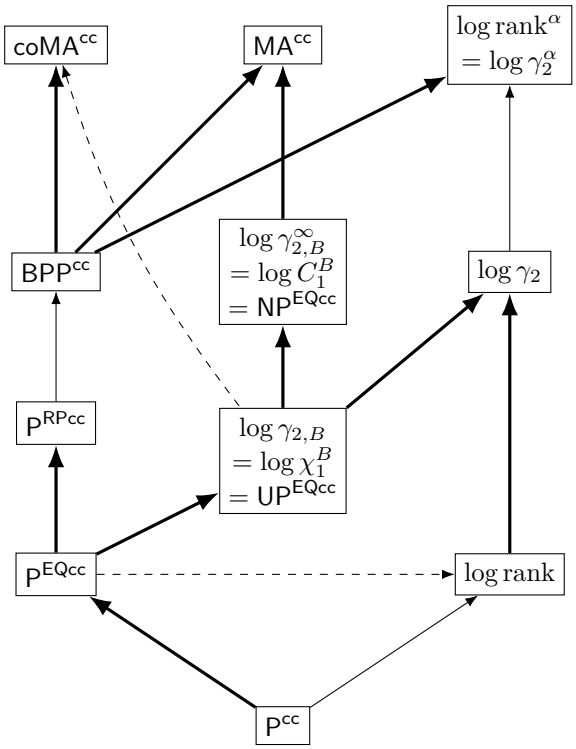

Figure 2 Relationships between the communication complexity measures. We consider total functions only. $\mathcal{A} \to \mathcal{B}$ with a normal arrow represents $\mathcal{A} \subseteq \mathcal{B}$. The arrow is bold if that inclusion is known to be strict ($\mathcal{A} \subsetneq \mathcal{B}$). The arrow is dashed if a separation is known ($\mathcal{A} \not\subset \mathcal{B}$). Some relationships are omitted if they can be derived from the others shown here.

Our work finds tight matrix-analytic characterizations of some EQUALITY-oracle-based communication models. If our understanding of $\mathsf{RP}^{\mathsf{cc}}$ oracles was similarly developed it would represent tremendous progress towards resolving $\mathsf{BPP}^{\mathsf{cc}}$ vs. $\mathsf{P}^{\mathsf{RPcc}}$.

▶ **Open Question 1.** *Find a matrix-analytic technique that characterizes* $\mathsf{RP}^{\mathsf{cc}}$ *oracles in communication complexity.*

This problem seems difficult – one-sided randomness is hardly understood at all! For example, we know that $\mathsf{coRP}^{\mathsf{cc}} \not\subset \mathsf{UP}^{\mathsf{EQcc}}$. However, the max-rect technique is itself one-sided, and so is silent on $\mathsf{RP}^{\mathsf{cc}}$ vs $\mathsf{UP}^{\mathsf{EQcc}}$. Resolving this seems like a concrete first step towards understanding $\mathsf{RP}^{\mathsf{cc}}$.

▶ **Open Question 2.** *Is* $\mathsf{RP}^{\mathsf{cc}} \subset \mathsf{UP}^{\mathsf{EQcc}}$*?*

We remark that the reverse is false (SINK∘XOR $\notin \mathsf{RP}^{\mathsf{cc}}$) and that the situation is easily resolved without the unambiguity in the nondeterminism ($\mathsf{RP}^{\mathsf{cc}} \subset \mathsf{NP}^{\mathsf{cc}} \subset \mathsf{NP}^{\mathsf{EQcc}}$).

How strong is γ_2 in communication?

In the paper where it was introduced, SINK∘XOR was shown to have polynomial approximate rank by analyzing the Fourier decomposition of SINK and lifting these properties to communication complexity [10]. The results in this paper give another way to show this upper bound on approximate rank. From Lemma 26, the $\mathsf{U} \cdot \mathsf{EQ}^{\mathsf{cc}}$ complexity of SINK∘XOR

is logarithmic; Theorem 2 then gives us that its communication matrix has polynomial $\gamma_{2,B}$, and for any matrix A, $\gamma_{2,B}(A) \geq \gamma_2(A) \geq \gamma_2^\alpha(A)$. As mentioned in Section 2, approximate γ_2 and approximate rank are essentially equivalent [20].

This chain of inequalities highlights a huge gap in our understanding of the strength of approximate rank in communication complexity: a very weak variant of approximate rank is sufficient to upper bound Sink∘XOR! A better understanding of the power of γ_2 and its variants in communication complexity may lead us to a richer landscape of functions that refute the log approximate rank conjecture. (For another paper about the search for stronger counterexample that takes a different approach, see [7].) Here are a couple of concrete questions in this direction:

▶ **Open Question 3.** *Is there a function whose communication matrix would be lower bounded by* $\log \gamma_2$ *but not* $\log \gamma_2^\alpha$*?*

Separations between these measures are known outside the realm of communication complexity. However, we are specifically searching for a function with quasipolynomial (or better) approximate γ_2 but exponential γ_2, which appears to still be an unsolved problem.

Another inequality in the chain above is $\gamma_{2,B}(A) \geq \gamma_2(A)$. In a communication complexity sense, these measures are exponentially separated because $\gamma_{2,B}$ is not closed under complement but γ_2 is. However, we find this argument somewhat unsatisfying, as it does not capture many of the differences between $\gamma_{2,B}$ and γ_2. We would like to consider a closure of $\gamma_{2,B}$ – a minimal set that is lower bounded by $\gamma_{2,B}$ and is closed under complement and other simple operations.

▶ **Open Question 4.** *Is there a reasonable closure of* $\gamma_{2,B}$ *that is equivalent to* γ_2 *in terms of its ability to bound functions in communication complexity?*

Perhaps the blocky rank measure of Hambardzumyan, Hatami, and Hatami is the right place to look for such a closure. See their paper for a discussion about how blocky rank relates to communication complexity [15].

$\mathsf{P}^{\mathsf{EQcc}}$ vs. $\mathsf{NP}^{\mathsf{EQcc}} \cap \mathsf{coNP}^{\mathsf{EQcc}}$

As mentioned in Section 4, $\mathsf{P}^{\mathsf{cc}} = \mathsf{UP}^{\mathsf{cc}}$ [30] but $\mathsf{P}^{\mathsf{EQcc}} \neq \mathsf{UP}^{\mathsf{EQcc}}$. There is another known collapse of limited nondeterminism to determinism in communication complexity: $\mathsf{P}^{\mathsf{cc}} = \mathsf{NP}^{\mathsf{cc}} \cap \mathsf{coNP}^{\mathsf{cc}}$ [2]. Does this hold with Equality oracles present?

▶ **Open Question 5.** *Is* $\mathsf{P}^{\mathsf{EQcc}} = \mathsf{NP}^{\mathsf{EQcc}} \cap \mathsf{coNP}^{\mathsf{EQcc}}$*?*

This is still open even if we restrict to unambiguous nondeterminism.

▶ **Open Question 6.** *Is* $\mathsf{P}^{\mathsf{EQcc}} = \mathsf{UP}^{\mathsf{EQcc}} \cap \mathsf{coUP}^{\mathsf{EQcc}}$*?*

Our results provide tools that may be helpful for solving this problem. To illustrate, let us observe a couple of properties of these intersection classes. Theorem 2 and Lemma 15 imply that any function in $\mathsf{UP}^{\mathsf{EQcc}} \cap \mathsf{coUP}^{\mathsf{EQcc}}$ has a communication matrix that can be fully partitioned into monochromatic rectangles where any row or column is contained in only a few of these rectangles (in the case of $\mathsf{NP}^{\mathsf{EQcc}} \cap \mathsf{coNP}^{\mathsf{EQcc}}$, replace the partition with a cover). Furthermore, since max-rect lower bounds $\mathsf{NP}^{\mathsf{EQcc}}$, a zero-sided version of max-rect (which compares the number of *zeroes* with the largest *0-monochromatic* rectangle) lower bounds $\mathsf{coNP}^{\mathsf{EQcc}}$. We can use the contrapositives of these lower bounds to show that any function in $\mathsf{NP}^{\mathsf{EQcc}} \cap \mathsf{coNP}^{\mathsf{EQcc}}$ has a large monochromatic rectangle: either it has many ones and therefore has a large 1-monochromatic rectangle or it has many zeroes and therefore has a large 0-monochromatic rectangle.

References

1 Scott Aaronson and Avi Wigderson. Algebrization: A New Barrier in Complexity Theory. *ACM Trans. Comput. Theory*, 1(1):2:1–2:54, February 2009. doi:10.1145/1490270.1490272.

2 Alfred V. Aho, Jeffrey D. Ullman, and Mihalis Yannakakis. On notions of information transfer in VLSI circuits. In *Proceedings of the Fifteenth Annual ACM Symposium on Theory of Computing*, STOC '83, pages 133–139, New York, NY, USA, December 1983. Association for Computing Machinery. doi:10.1145/800061.808742.

3 Daniel Avraham and Amir Yehudayoff. On blocky ranks of matrices. Technical Report 137, Electronic Colloquium on Computational Complexity, 2022. URL: https://eccc.weizmann.ac.il/report/2022/137/.

4 Laszlo Babai, Peter Frankl, and Janos Simon. Complexity classes in communication complexity theory. In *27th Annual Symposium on Foundations of Computer Science (Sfcs 1986)*, pages 337–347, October 1986. doi:10.1109/SFCS.1986.15.

5 Béla Bollobás. On generalized graphs. *Acta Mathematica Academiae Scientiarum Hungaricae*, 16(3):447–452, September 1965. doi:10.1007/BF01904851.

6 Nicolas Bousquet, Aurélie Lagoutte, and Stéphan Thomassé. Clique versus independent set. *European Journal of Combinatorics*, 40:73–92, August 2014. doi:10.1016/j.ejc.2014.02.003.

7 Arkadev Chattopadhyay, Ankit Garg, and Suhail Sherif. Towards Stronger Counterexamples to the Log-Approximate-Rank Conjecture. In Mikołaj Bojańczy and Chandra Chekuri, editors, *41st IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2021)*, volume 213 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 13:1–13:16, Dagstuhl, Germany, 2021. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.FSTTCS.2021.13.

8 Arkadev Chattopadhyay, Shachar Lovett, and Marc Vinyals. Equality Alone Does Not Simulate Randomness. Technical Report 206, Electronic Colloquium on Computational Complexity, 2018. URL: https://eccc.weizmann.ac.il/report/2018/206/.

9 Arkadev Chattopadhyay, Shachar Lovett, and Marc Vinyals. Equality Alone Does not Simulate Randomness. In Amir Shpilka, editor, *34th Computational Complexity Conference (CCC 2019)*, volume 137 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 14:1–14:11, Dagstuhl, Germany, 2019. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. doi:10.4230/LIPIcs.CCC.2019.14.

10 Arkadev Chattopadhyay, Nikhil S. Mande, and Suhail Sherif. The Log-Approximate-Rank Conjecture Is False. *J. ACM*, 67(4):23:1–23:28, June 2020. doi:10.1145/3396695.

11 Dmitry Gavinsky. The Layer Complexity of Arthur-Merlin-like Communication. *Theory of Computing*, 17(8):1–28, September 2021. doi:10.4086/toc.2021.v017a008.

12 Mika Göös. Lower Bounds for Clique vs. Independent Set. In *2015 IEEE 56th Annual Symposium on Foundations of Computer Science*, pages 1066–1076, October 2015. doi:10.1109/FOCS.2015.69.

13 Mika Göös, Toniann Pitassi, and Thomas Watson. The Landscape of Communication Complexity Classes. *comput. complex.*, 27(2):245–304, June 2018. doi:10.1007/s00037-018-0166-6.

14 Mika Göös and Thomas Watson. Communication Complexity of Set-Disjointness for All Probabilities. *Theory of Computing*, 12(1):1–23, August 2016. doi:10.4086/toc.2016.v012a009.

15 Lianna Hambardzumyan, Hamed Hatami, and Pooya Hatami. Dimension-free bounds and structural results in communication complexity. *Isr. J. Math.*, October 2022. doi:10.1007/s11856-022-2365-8.

16 Lane A. Hemaspaandra and Heribert Vollmer. The satanic notations: Counting classes beyond #P and other definitional adventures. *SIGACT News*, 26(1):2–13, March 1995. doi:10.1145/203610.203611.

17 Hartmut Klauck. Lower Bounds for Quantum Communication Complexity. *SIAM J. Comput.*, 37(1):20–46, January 2007. doi:10.1137/S0097539702405620.

18 Matthias Krause. Geometric arguments yield better bounds for threshold circuits and distributed computing. *Theoretical Computer Science*, 156(1):99–117, March 1996. doi:10.1016/0304-3975(95)00005-4.

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

20 Troy Lee and Adi Shraibman. An Approximation Algorithm for Approximation Rank. In *2009 24th Annual IEEE Conference on Computational Complexity*, pages 351–357, July 2009. doi:10.1109/CCC.2009.25.

21 Troy Lee and Adi Shraibman. Lower Bounds in Communication Complexity. *Found. Trends Theor. Comput. Sci.*, 3(4):263–399, October 2009. doi:10.1561/0400000040.

22 Troy Lee, Adi Shraibman, and Robert Špalek. A Direct Product Theorem for Discrepancy. In *2008 23rd Annual IEEE Conference on Computational Complexity*, pages 71–80, June 2008. doi:10.1109/CCC.2008.25.

23 Nati Linial and Adi Shraibman. Learning Complexity vs Communication Complexity. *Combinatorics, Probability and Computing*, 18(1-2):227–245, March 2009. doi:10.1017/S0963548308009656.

24 Nati Linial and Adi Shraibman. Lower bounds in communication complexity based on factorization norms. *Random Structures & Algorithms*, 34(3):368–394, 2009. doi:10.1002/rsa.20232.

25 Noam Nisan. The Communication Complexity of Threshold Gates. In *Combinatorics, Paul Erdős Is Eighty*, pages 301–315, 1994.

26 Periklis Papakonstantinou, Dominik Scheder, and Hao Song. Overlays and Limited Memory Communication. In *2014 IEEE 29th Conference on Computational Complexity (CCC)*, pages 298–308, June 2014. doi:10.1109/CCC.2014.37.

27 Michal Parnas, Dana Ron, and Adi Shraibman. The Boolean rank of the uniform intersection matrix and a family of its submatrices. *Linear Algebra and its Applications*, 574:67–83, August 2019. doi:10.1016/j.laa.2019.03.027.

28 Toniann Pitassi, Morgan Shirley, and Thomas Watson. Nondeterministic and Randomized Boolean Hierarchies in Communication Complexity. *comput. complex.*, 30(2):1–48, July 2021. doi:10.1007/s00037-021-00210-5.

29 Anup Rao and Amir Yehudayoff. *Communication Complexity and Applications*. Cambridge University Press, Cambridge, 2020. doi:10.1017/9781108671644.

30 Mihalis Yannakakis. Expressing combinatorial optimization problems by Linear Programs. *Journal of Computer and System Sciences*, 43(3):441–466, December 1991. doi:10.1016/0022-0000(91)90024-Y.

31 Andrew Chi-Chih 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, New York, NY, USA, April 1979. Association for Computing Machinery. doi:10.1145/800135.804414.