Electronic Colloquium on Computational Complexity, Report No. 113 (2021)

Tight Bounds for the Randomized and Quantum Communication Complexities of Equality with Small Error

Nikhil S. Mande* Ronald de Wolf†

Abstract

We investigate the randomized and quantum communication complexities of the well-studied Equality function with small error probability ε, getting the optimal constant factors in the leading terms in a number of different models.

The following are our results in the *randomized* model:

- We give a general technique to convert public-coin protocols to private-coin protocols by incurring a small multiplicative error at a small additive cost. This is an improvement over Newman's theorem [Inf. Proc. Let.'91] in the dependence on the error parameter.
- As a consequence we obtain a $(\log(n/\varepsilon^2)+4)$-cost private-coin communication protocol that computes the n-bit Equality function, to error ε. This improves upon the $\log(n/\varepsilon^3)+O(1)$ upper bound implied by Newman's theorem, and matches the best known lower bound, which follows from Alon [Comb. Prob. Comput.'09], up to an additive $\log\log(1/\varepsilon)+O(1)$.

The following are our results in the *quantum* model:

- We exhibit a one-way protocol with $\log(n/\varepsilon)+4$ qubits of communication, that uses only pure states and computes the n-bit Equality function to error ε. This bound was implicitly already shown by Nayak [PhD thesis'99].
- We give a near-matching lower bound, showing that any ε-error one-way protocol for n-bit Equality that uses only pure states communicates at least $\log(n/\varepsilon)-\log\log(1/\varepsilon)-O(1)$ qubits.
- We exhibit a one-way protocol with $\log(\sqrt{n}/\varepsilon)+3$ qubits of communication, that uses *mixed* states and computes the n-bit Equality function to error ε. This is also tight up to an additive $\log\log(1/\varepsilon)+O(1)$, which follows from Alon's result.

Our upper bounds also yield upper bounds on the approximate rank, approximate nonnegative-rank, and approximate psd-rank of the Identity matrix. As a consequence we also obtain improved upper bounds on these measures for the distributed SINK function, which was recently used to refute the randomized and quantum versions of the log-rank conjecture (Chattopadhyay, Mande and Sherif [J. ACM'20], Sinha and de Wolf [FOCS'19], Anshu, Boddu and Touchette [FOCS'19]).

*CWI, Amsterdam. Supported by the Dutch Research Council (NWO) through QuantERA ERA-NET Cofund project QuantAlgo (project number 680-91-034). Nikhil.Mande@cwi.nl

†QuSoft, CWI and University of Amsterdam, the Netherlands. Partially supported by the Dutch Research Council (NWO/OCW), as part of the Quantum Software Consortium programme (project number 024.003.037), and through QuantERA ERA-NET Cofund project QuantAlgo (680-91-034). rdewolf@cwi.nl

ISSN 1433-8092

1 Introduction

Yao [Yao79] introduced the classical model of communication complexity, and also subsequently introduced its quantum analogue [Yao93]. Communication complexity has important applications in several disciplines, such as lower bounds on circuits, data structures, streaming algorithms, and many other areas (see, for example, [KN97, RY20] and the references therein). The basic model of communication complexity involves two parties, usually called Alice and Bob, who wish to jointly compute $F(x, y)$ for a known function $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$, where Alice holds $x \in \{0,1\}^n$ and Bob holds $y \in \{0,1\}^n$. The parties use a communication protocol agreed upon in advance to compute $F(x, y)$. They are individually computationally unbounded and the cost is the amount of communication between the parties on the worst-case input.

Consider the n-bit *Equality* function, denoted $\mathsf{EQ}_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ (or simply EQ when n is clear from context), and defined as $\mathsf{EQ}_n(x, y) = 1$ iff $x = y$. This is arguably the simplest and most basic problem in communication complexity. It is well known that its deterministic communication complexity equals n, which is maximal. However, Yao [Yao79] already showed that if we allow some small constant error probability, then the communication complexity becomes much smaller. In this paper we pin down the small-error communication complexity of *Equality* in various communication models. Our bounds are essentially optimal both in terms of n and in terms of the error. While our optimal upper bounds only give small improvements over known bounds, Equality is such a fundamental communication problem that we feel it is worthwhile to pin down its complexity as precisely as possible and to find protocols that are as efficient as possible.

1.1 Prior work

Given a function $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$, define the $2^n \times 2^n$ *communication matrix* of F, denoted M_F, by $M_F(x, y) = F(x, y)$. Define the *ε-approximate rank* of a matrix M, denoted $\mathsf{rk}_\varepsilon(M)$, to be the minimum number of rank-1 matrices needed such that their sum is ε-close to M entrywise (equivalently, $\mathsf{rk}_\varepsilon(M)$ is the minimum rank among all matrices that are ε-close to M entrywise). If the rank-1 matrices are additionally constrained to be entrywise nonnegative, then the resulting measure is called the *ε-approximate nonnegative-rank* of M, denoted $\mathsf{rk}^+_\varepsilon(M)$. By definition, $\mathsf{rk}^+_\varepsilon(M_F) \geq \mathsf{rk}_\varepsilon(M_F)$. Denote ε-error randomized communication complexity by $\mathsf{R}^{\mathsf{pri}}_\varepsilon(\cdot)$ when the players have access to private randomness, and $\mathsf{R}^{\mathsf{pub}}_\varepsilon(F)$ when the players have access to public randomness (i.e., shared coin flips). Let $\mathsf{Q}^{\mathsf{pri}}_\varepsilon(\cdot)$ denote ε-error quantum communication complexity, assuming private randomness. In all quantum communication models under consideration in this paper, Alice and Bob do not have access to pre-shared entanglement.

Krause [Kra96] showed the following lower bound on the randomized communication complexity of a Boolean function in terms of the approximate nonnegative-rank of its communication matrix.

Theorem 1.1 ([Kra96])**.** *Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ be a Boolean function and $\varepsilon > 0$. Then,*

$$\mathsf{R}^{\mathsf{pri}}_\varepsilon(F) \geq \log \mathsf{rk}^+_\varepsilon(M_F).$$

Analogous to this, the following lower bound is known on the quantum communication complexity of a Boolean function, due to Nielsen [Nie98] and Buhrman and de Wolf [BW01].

Theorem 1.2 ([Nie98, BW01])**.** *Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ be a Boolean function and let $\varepsilon > 0$. Then,*

$$\mathsf{Q}^{\mathsf{pri}}_\varepsilon(F) \geq \frac{1}{2} \log \mathsf{rk}_\varepsilon(M_F).$$

A similar proof as that of [BW01] can be used to show that the quantum communication complexity of a Boolean function is bounded below by the logarithm of its *approximate psd-rank*, which we define below. Let M be a matrix with nonnegative real entries. A rank-d *psd-factorization* of M consists of a set of $d \times d$ complex[1] psd matrices A_i (one for each row of M) and B_j (one for each column of M), such that for all i, j we have $M_{ij} = \mathrm{tr}(A_i B_j)$. The *psd-rank* of M, denoted $\mathsf{rk}^{\mathrm{psd}}(M)$, is the minimal d for which M has such a psd factorization. This notion has gained a lot of interest in areas such as semidefinite optimization, communication complexity, and others. See Fawzi et al. [FGP+15] for an excellent survey. The ε-*approximate psd-rank* of M, which we denote by $\mathsf{rk}_\varepsilon^{\mathrm{psd}}(M)$, is the minimum psd-rank among all matrices that are ε-close to M entrywise.

Theorem 1.3. *Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ be a Boolean function and let $\varepsilon > 0$. Then,*

$$\mathsf{Q}_\varepsilon^{\mathsf{pri}}(F) \geq \log \mathsf{rk}_\varepsilon^{\mathrm{psd}}(M_F) + 1.$$

For completeness, we prove this in Appendix A. It is easy to show that $\mathsf{rk}_\varepsilon^{\mathrm{psd}}(M_F) \leq \mathsf{rk}_\varepsilon^{+}(M_F)$. Alon [Alo09] showed the following bounds on the approximate rank of the Identity matrix.

Theorem 1.4 ([Alo09])**.** *There exists a positive constant c such that the following holds for all integers $n > 0$ and $1/2^{n/2} \leq \varepsilon \leq 1/4$. Let I denote the $2^n \times 2^n$ Identity matrix. Then,*

$$\mathsf{rk}_\varepsilon(I) \geq \frac{cn}{\varepsilon^2 \log\left(\frac{1}{\varepsilon}\right)}.$$

Note that the $2^n \times 2^n$ Identity matrix is the communication matrix of the n-bit Equality function. Theorems 1.1 and 1.4 thus imply that for $1/2^{n/2} \leq \varepsilon \leq 1/4$,

$$\mathsf{R}_\varepsilon^{\mathsf{pri}}(\mathsf{EQ}_n) \geq \log\left(\frac{n}{\varepsilon^2}\right) - \log\log\left(\frac{1}{\varepsilon}\right) - O(1). \tag{1}$$

Newman [New91] proved the following theorem that shows that public-coin protocols can be converted to private-coin protocols with an additive error, with a small additive cost. For the following form, see for example, [KN97, Claim 3.14].

Theorem 1.5 (cf. [KN97, Claim 3.14])**.** *Let $F : \{0,1\}^n \times \{0,1\}^n$ be a Boolean function. For every $\delta > 0$ and every $\varepsilon > 0$,*

$$\mathsf{R}_{\varepsilon+\delta}^{\mathsf{pri}}(F) \leq \mathsf{R}_\varepsilon^{\mathsf{pub}}(F) + \log\left(\frac{n}{\delta^2}\right) + O(1).$$

Relabeling variables, Theorem 1.5 is equivalent to

$$\mathsf{R}_{\varepsilon(1+\delta)}^{\mathsf{pri}}(F) \leq \mathsf{R}_\varepsilon^{\mathsf{pub}}(F) + \log\left(\frac{n}{\varepsilon^2\delta^2}\right) + O(1).$$

1.2 Our results

In this section we list our results, first those for randomized communication complexity, and then those for quantum communication complexity.

[1] Often this definition is restricted to real matrices. This can change the psd-rank by a constant factor, but no more than that [LWW17, Section 3.3].

1.2.1 Randomized communication complexity

We give an improved version of Newman's theorem (Theorem 1.5), which allows us to convert a public-coin protocol to a private-coin one with an optimal dependence on the error. Our proof follows along similar lines as that of Newman's. Our key deviation is that we use a multiplicative form of the Chernoff bound, where previously an additive version was used.

Theorem 1.6. *Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ be a Boolean function. For all $\varepsilon \in [0, 1/2)$ and all $\delta \in (0, 1]$,*

$$\mathsf{R}^{\mathsf{pri}}_{\varepsilon(1+\delta)}(F) \leq \mathsf{R}^{\mathsf{pub}}_{\varepsilon}(F) + \log\left(\frac{n}{\varepsilon}\right) + \log\left(\frac{6}{\delta^2}\right).$$

To compare Theorem 1.5 and Theorem 1.6, consider the $(1/n)$-error private-coin randomized communication complexity of EQ_n. The ε-error *public-coin* communication complexity of EQ_n is at most $\log(1/\varepsilon)$ (and this can be shown to be tight up to an additive constant). Thus, Theorem 1.5 can at best give an upper bound of

$$\mathsf{R}^{\mathsf{pri}}_{1/n}(\mathsf{EQ}_n) \leq \log n + \log(n^3) + O(1) = 4\log n + O(1).$$

In contrast, Equation (1) implies $\mathsf{R}^{\mathsf{pri}}_{1/n}(\mathsf{EQ}_n) \geq 3\log n - \log\log n - O(1)$. On the other hand, Theorem 1.6 implies a tight upper bound (up to the additive $\log\log n + O(1)$ term) of $3\log n + O(1)$ on the $(1/n)$-error private-coin communication complexity of EQ_n, by converting the $\log(1/\varepsilon)$-cost public-coin protocol for EQ_n to a private-coin protocol.

Theorem 1.7. *For all positive integers $n > 0$ and for all $\varepsilon \in [0, 1/2)$,*

$$\mathsf{R}^{\mathsf{pri}}_{\varepsilon}(\mathsf{EQ}) \leq \log\left(\frac{n}{\varepsilon^2}\right) + 4.$$

This shows Alon's theorem (Theorem 1.4) is tight up to the $O(\log(1/\varepsilon))$ factor, not only for approximate rank, but also for communication complexity. Theorem 1.7 and Theorem 1.1 also imply that the approximate-rank lower bound in Theorem 1.4 is nearly tight even restricting to *nonnegative* approximations to the Identity matrix.

Corollary 1.8. *Let $n > 0$ be an integer, and let I denote the $2^n \times 2^n$ Identity matrix. Then for all $\varepsilon \in [0, 1/2)$,*

$$\mathsf{rk}^+_{\varepsilon}(I) \leq \frac{16n}{\varepsilon^2}.$$

To compare the performance of Theorem 1.5 with that of Theorem 1.6 in a more general setting, we consider the natural problem of converting a public-coin protocol to a private-coin protocol while allowing the error to double. Setting $\delta = \varepsilon$ in Theorem 1.5 and relabeling parameters, we obtain

$$\mathsf{R}^{\mathsf{pri}}_{\varepsilon}(F) \leq \mathsf{R}^{\mathsf{pub}}_{\varepsilon/2}(F) + \log\left(\frac{n}{\varepsilon^2}\right) + O(1).$$

However, Theorem 1.6 yields the following improved dependence on ε by setting $\delta = 1$ and relabeling parameters.

$$\mathsf{R}^{\mathsf{pri}}_{\varepsilon}(F) \leq \mathsf{R}^{\mathsf{pub}}_{\varepsilon/2}(F) + \log\left(\frac{n}{\varepsilon}\right) + 4.$$

1.2.2 Quantum communication complexity

Prior to this work, the best known lower bound on the ε-error quantum communication complexity of Equality was $\Omega(\log(n/\varepsilon))$ [BW01, Proposition 3], with a constant hidden in the $\Omega(\cdot)$ that is less than 1/2. Theorem 1.2 and Theorem 1.4 imply that

$$\mathsf{Q}_\varepsilon^{\mathsf{pri}}(\mathsf{EQ}_n) \geq \log\left(\frac{\sqrt{n}}{\varepsilon}\right) - \log\log\left(\frac{1}{\varepsilon}\right) - O(1). \tag{2}$$

In terms of upper bounds, we exhibit a *one-way* quantum communication upper bound with an optimal dependence on ε, that uses only pure-state messages (and hence does not use even private randomness). In particular, by choosing ε to be an arbitrary small polynomial in the input size, this implies that the factor of 1/2 in Theorem 1.2 cannot be improved when $F = \mathsf{EQ}_n$. Let $\mathsf{Q}_\varepsilon^{\mathrm{pure},\rightarrow}(F)$ be the ε-error quantum communication complexity of F, where the protocols are one-way and Alice is only allowed to send a pure state to Bob. We show the following.

Theorem 1.9. *For all positive integers $n > 0$ and for all $\varepsilon \in [0, 1/2)$,*

$$\mathsf{Q}_\varepsilon^{\mathrm{pure},\rightarrow}(\mathsf{EQ}_n) \leq \log\left(\frac{n}{\varepsilon}\right) + 4.$$

The proof uses the probabilistic method to analyze random linear codes. Nayak [Nay99] already used the same upper bound technique to show an upper bound on the bounded-error one-way quantum communication complexity of EQ_n. They did not explicitly derive this error-dependence, but it follows immediately from their construction by plugging in codes with length $O(n/\varepsilon)$ and relative distance $1/2 - \sqrt{\varepsilon}$ in [Nay99, pp.16–17]. We also show that this is nearly tight:

Theorem 1.10. *There exists an absolute constant c such that the following holds. For all positive integers $n > 0$ and for all $\varepsilon \in [1/2^n, 1/4]$,*

$$\mathsf{Q}_\varepsilon^{\mathrm{pure},\rightarrow}(\mathsf{EQ}_n) \geq \log\left(\frac{n}{\varepsilon}\right) - \log\log\left(\frac{1}{\varepsilon}\right) - c.$$

While the pure-state protocol of Theorem 1.9 has optimal dependence on ε (up to the $\log\log(1/\varepsilon)$ term), it does not match the n-dependence of the lower bound of Equation (2); in fact, one-way pure-state protocols cannot match this (Theorem 1.10). However, if we allow one-way *mixed-state* messages, then we can give a better upper bound and close the gap:

Theorem 1.11. *For all positive integers $n > 0$ and for all $\varepsilon \in [0, 1/2)$,*

$$\mathsf{Q}_\varepsilon^{\mathsf{pri}}(\mathsf{EQ}_n) \leq \log\left(\frac{\sqrt{n}}{\varepsilon}\right) + 3.$$

The proof is again probabilistic, using known concentration properties of overlaps of random projectors to allow us to show the existence of appropriate mixed-state messages for Alice and appropriate measurements for Bob. Theorems 1.3 and 1.11 also imply upper bounds on the ε-approximate psd-rank of the Identity matrix.

Corollary 1.12. *Let $n > 0$ be an integer, and let I denote the $2^n \times 2^n$ Identity matrix. Then for all $\varepsilon \in [0, 1/2)$,*

$$\mathsf{rk}_\varepsilon^{\mathrm{psd}}(I) \leq \frac{4\sqrt{n}}{\varepsilon}.$$

As noted by Lee, Wei and de Wolf [LWW17, Theorem 17], Alon's approximate rank lower bound (Theorem 1.4) almost immediately gives a lower bound of $\mathsf{rk}_\varepsilon^{\text{psd}}(I) = \Omega\left(\frac{\sqrt{n}}{\varepsilon\sqrt{\log(1/\varepsilon)}}\right)$. This shows that our upper bound in Corollary 1.12 is tight up to a multiplicative $O(\sqrt{\log(1/\varepsilon)})$ factor.

2 Preliminaries

All logarithms in this paper are taken to base 2. We use $\exp(x)$ to denote e^x, where e denotes Euler's number. For strings $x, y \in \{0,1\}^n$, define their Hamming distance by $d(x,y) := |\{i \in [n] : x_i \neq y_i\}|$. For an event X, let $I(X) \in \{0,1\}$ denote the *indicator* of X, which is 1 iff X occurs.

Definition 2.1 (Linear code)**.** *For integers $N \geq n$, a linear code is a linear function $C : \{0,1\}^n \to \{0,1\}^N$.*

One may view a linear code as an $N \times n$ matrix M over $\mathbb{F}_2$; an input $x \in \{0,1\}^n$ is mapped to N-bit codeword Mx (where the matrix product is taken over $\mathbb{F}_2$). Choosing a random linear code corresponds to choosing an M with uniformly random binary entries.

We use the following well-known multiplicative form of the Chernoff bound [MU05, Theorem 4.4].

Lemma 2.2. *Let $Z_1, \ldots, Z_n$ be independent random variables taking values in $\{0,1\}$. Let $Z = \sum_{i=1}^n Z_i$, and let $\mu = \mathbb{E}[Z]$. Then for all $\delta \in [0,1]$,*

$$\Pr[Z \geq (1+\delta)\mu] \leq \exp(-\delta^2\mu/3),$$
$$\Pr[Z \leq (1-\delta)\mu] \leq \exp(-\delta^2\mu/2).$$

We refer the reader to [KN97, RY20] for the basics of classical communication complexity, and to [Wol02] for an introduction to quantum communication complexity.

3 An improved form of Newman's theorem

Proof of Theorem 1.6. Let Π be a public-coin protocol that computes F with error ε. Assume without loss of generality that all the random coins are tossed at the beginning of the protocol. That is, for every $x, y \in \{0,1\}^n$,

$$\Pr_r[\Pi(x,y,r) \neq F(x,y)] \leq \varepsilon. \tag{3}$$

Set

$$B = \frac{6n}{\delta^2\varepsilon} \tag{4}$$

and independently choose random strings $r_1, \ldots, r_B$ according to the same distribution as used by Π. For two strings $x, y \in \{0,1\}^n$ and an index $j \in [B]$, let $I_{j,x,y}$ denote the indicator event of r_j being a "bad random string" for x, y:

$$I_{j,x,y} := \begin{cases} 1 & \Pi(x,y,r_j) \neq f(x,y) \\ 0 & \text{otherwise.} \end{cases} \tag{5}$$

Fix two arbitrary strings $x, y \in \{0,1\}^n$. Equation (3) implies $\Pr_{r_1,\dots,r_B, j\in[B]}[I_{j,x,y} = 1] \le \varepsilon$. By linearity of expectation and our choice of B in Equation (4),

$$\mathbb{E}_{r_1,\dots,r_B}\left[\sum_{j\in[B]} I_{j,x,y}\right] \le B\varepsilon = \frac{6n}{\delta^2}.$$

We now give an upper bound on $\Pr_{r_1,\dots,r_B}\left[\sum_{j\in[B]} I_{j,x,y} \ge B\varepsilon(1+\delta)\right]$. Assume without loss of generality that $\Pr_{r_1,\dots,r_B, j\in[B]}[I_{j,x,y} = 1] = \varepsilon$, and hence $\mathbb{E}_{r_1,\dots,r_B}\left[\sum_{j\in[B]} I_{j,x,y}\right] = B\varepsilon$ (since the desired probability could only be smaller otherwise). By a Chernoff bound (Lemma 2.2),

$$\Pr_{r_1,\dots,r_B}\left[\sum_{j\in[B]} I_{j,x,y} \ge B\varepsilon(1+\delta)\right] \le \exp\left(-\frac{\delta^2\cdot 6n}{3\delta^2}\right) = \exp(-2n) < 2^{-2n}.$$

By a union bound over all $x, y \in \{0,1\}^n$,

$$\begin{aligned}\Pr_{r_1,\dots,r_B}\left[\sum_{j\in[B]} I_{j,x,y} \ge B\varepsilon(1+\delta) \text{ for some } x,y\in\{0,1\}^n\right] &\le \sum_{x,y\in\{0,1\}^n} \Pr_{r_1,\dots,r_B}\left[\sum_{j\in[B]} I_{j,x,y} \ge B\varepsilon(1+\delta)\right] \\ &< 2^{2n}\cdot 2^{-2n} = 1.\end{aligned}$$

Hence there exists a choice of $r_1,\dots,r_B$ such that the following holds for all $x, y \in \{0,1\}^n$:

$$\sum_{j\in[B]} I_{j,x,y} < B\varepsilon(1+\delta). \tag{6}$$

Fixing this choice of $r_1,\dots,r_B$, Protocol 1 gives a private-coin protocol for F.

Protocol 1: A private-coin protocol for F

---

1. Alice samples $j \in [B]$ uniformly at random, and sends it to Bob.
2. Alice and Bob perform the public-coin protocol Π assuming r_j was the public random string.

To show the correctness of this protocol, our choice of B (Equation (4)) and Equations (5) and (6) imply that for all $x, y \in \{0,1\}^n$,

$$\Pr_{j\in[B]}[\Pi(x,y,r_j) \ne f(x,y)] < \frac{B\varepsilon(1+\delta)}{B} = \varepsilon(1+\delta).$$

Hence the protocol has error probability less than $\varepsilon(1+\delta)$. The cost of the first step of the protocol is $\log B$, and the cost of the second step is at most $\mathsf{R}^{\mathsf{pub}}_{\varepsilon}(F)$. Thus, we have,

$$\mathsf{R}^{\mathsf{pri}}_{\varepsilon(1+\delta)}(F) \le \mathsf{R}^{\mathsf{pub}}_{\varepsilon}(F) + \log B = \mathsf{R}^{\mathsf{pub}}_{\varepsilon}(F) + \log\frac{6n}{\delta^2\varepsilon} = \mathsf{R}^{\mathsf{pub}}_{\varepsilon}(F) + \log\frac{n}{\varepsilon} + \log\frac{6}{\delta^2}.$$

Note that if Π was a one-way protocol, then Protocol 1 is a one-way private-coin protocol. ☐

4 Communication complexity upper bounds

In this section we show randomized and quantum communication upper bounds for Equality.

4.1 Randomized upper bound

As an application of Theorem 1.6, we recover an optimal small-error private-coin communication complexity upper bound for EQ_n from a naive public-coin protocol of cost $\log(2/\varepsilon)$ and error $\varepsilon/2$:

$$\mathsf{R}^{\mathsf{pri}}_{\varepsilon}(\mathsf{EQ}_n) \leq \log\left(\frac{2}{\varepsilon}\right) + \log\left(\frac{n}{\varepsilon}\right) + 3 = \log\left(\frac{n}{\varepsilon^2}\right) + 4. \tag{7}$$

This proves Theorem 1.7. Newman's theorem (Theorem 1.5) would only give an upper bound of

$$\mathsf{R}^{\mathsf{pri}}_{\varepsilon}(\mathsf{EQ}_n) \leq \log\left(\frac{2}{\varepsilon}\right) + \log\left(\frac{n}{\varepsilon^2}\right) + O(1) = \log\left(\frac{n}{\varepsilon^3}\right) + O(1).$$

In particular, for $\varepsilon = 1/n$ we improve the upper bound from $4\log n + O(1)$ to $3\log n + O(1)$, which turns out to be essentially optimal.

4.2 Quantum upper bound with only pure states

We require the following property of random linear codes.

Claim 4.1. *Let n be a positive integer and let $\delta > 0$. Let $x \neq y \in \{0,1\}^n$ be two arbitrary but fixed strings. Let $N = 4n/\delta^2$. Let $C : \{0,1\}^n \to \{0,1\}^N$ be a random linear code. Then*

$$\Pr_C\left[\frac{d(C(x), C(y))}{N} \notin \left[\frac{1}{2} - \delta, \frac{1}{2} + \delta\right]\right] < 2^{-2n}.$$

Proof of Claim 4.1. For each $i \in [N]$, the random variable $Z_i := I[C(x)_i = C(y)_i]$ equals 1 with probability 1/2 and 0 with probability 1/2. Further, Z_i and Z_j are independent for all $i \neq j \in [N]$. Define $Z = \sum_{i=1}^N Z_i = d(C(x), C(y))$. We have $\mathbb{E}[Z] = N/2$. By a Chernoff bound (Lemma 2.2),

$$\Pr_C\left[\left|\frac{d(C(x), C(y))}{N} - \frac{1}{2}\right| \geq \delta\right] = \Pr_C\left[\left|Z - \frac{N}{2}\right| \geq 2\delta \cdot \frac{N}{2}\right] \leq 2\exp\left(-4\delta^2 N/6\right) < 2^{-2n},$$

where the last inequality holds by our choice of N. □

By a union bound over all $x, y \in \{0,1\}^n$, Claim 4.1 implies the following corollary.

Corollary 4.2. *Let n be a positive integer, let $\delta > 0$ and let $N = 4n/\delta^2$. Then there exists a linear code $C : \{0,1\}^n \to \{0,1\}^N$ such that for all $x \neq y \in \{0,1\}^n$,*

$$\frac{d(C(x), C(y))}{N} \in \left[\frac{1}{2} - \delta, \frac{1}{2} + \delta\right].$$

We now prove Theorem 1.9.

Proof of Theorem 1.9. Set $\delta = \sqrt{\varepsilon}/2$. Let $N = 4n/\delta^2 = 16n/\varepsilon$ and let $C : \{0,1\}^n \to \{0,1\}^{16n/\varepsilon}$ be the code obtained from Corollary 4.2. The following is a protocol for EQ_n.

1. Alice, on input $x \in \{0,1\}^n$ prepares state $|\phi_x\rangle := \frac{1}{\sqrt{N}} \sum_{i \in [N]} (-1)^{C(x)_i} |i\rangle$, and sends Bob $|\phi_x\rangle$.

2. Define $|\phi_y\rangle := \frac{1}{\sqrt{N}} \sum_{i \in [N]} (-1)^{C(y)_i} |i\rangle$. Bob measures with respect to the projectors $|\phi_y\rangle\langle\phi_y|$ and $I - |\phi_y\rangle\langle\phi_y|$, and outputs 1 on observing the first measurement outcome, and 0 otherwise.

This protocol succeeds with probability 1 when $x = y$. The only error arises when $x \neq y$ and Bob observes the first measurement outcome. Thus, the error probability of this protocol equals

$$\begin{aligned}\max_{x \neq y \in \{0,1\}^n} |\langle \phi_x | \phi_y \rangle|^2 &= \max_{x \neq y \in \{0,1\}^n} \left(\frac{1}{N} \sum_{i \in [N]} (-1)^{C(x)_i + C(y)_i} \right)^2 \\ &= \max_{x \neq y \in \{0,1\}^n} \left(1 - \frac{2d(C(x), C(y))}{N} \right)^2 \\ &\leq 4\delta^2 = \varepsilon,\end{aligned}$$

where the last inequality follows from Corollary 4.2 and the last equality follows from our choice of δ. The number of qubits sent from Alice to Bob is $\log N = \log(16n/\varepsilon) = \log(n/\varepsilon) + 4$. □

We show in Section 5 that the protocol in the previous proof is nearly optimal if one restricts to one-way communication with only pure states.

4.3 Quantum upper bound with mixed states

In the last section we gave a $\log(n/\varepsilon) + O(1)$ quantum upper bound on the ε-error communication complexity of EQ_n, where Alice was only allowed to send a pure state to Bob. In this section we show that allowing Alice to send a *mixed* state to Bob gives a communication upper bound with a better (in fact optimal) n-dependence. Our protocol is based on concentration properties of overlaps of random projectors.

Consider two rank-r projectors P and Q acting on $\mathbb{C}^d$. The largest possible inner product $\mathrm{tr}(PQ)$ between them is r, which occurs iff $P = Q$. However, when one or both of the projectors are Haar-random, then we expect their inner product to be much smaller, namely only r^2/d. This is because if we take the spectral decompositions $P = \sum_{i=1}^r |u_i\rangle\langle u_i|$ and $Q = \sum_{j=1}^r |v_j\rangle\langle v_j|$, then

$$\mathrm{tr}(PQ) = \sum_{i,j=1}^r |\langle u_i, v_j \rangle|^2,$$

and the expected squared inner product between a random d-dimensional unit vector u_i and any fixed unit vector v_j, is $1/d$. Hayden, Leung and Winter [HLW06, Lemma III.5] showed that this inner product is very tightly concentrated around its expectation.

Claim 4.3 ([HLW06, Lemma III.5]). *Let P and Q be rank-r projectors on $\mathbb{C}^d$, where P is random*[2] *and Q is fixed. Let $\delta \in [0,1]$. Then*

$$\Pr\left[\mathrm{tr}(PQ) \geq \frac{(1+\delta)r^2}{d}\right] \leq \exp\left(\frac{-r^2\delta^2}{5}\right) < 2^{-r^2\delta^2/5}.$$

[2] More precisely, P is a projection onto a uniformly chosen r-dimensional subspace from all r-dimensional subspaces of $\mathbb{C}^d$. We do not elaborate more on this here since it is not relevant for us.

The following corollary then follows by setting parameters suitably.

Corollary 4.4. *For every integer $n > 0$ and all $\varepsilon \in [0, 1/2)$, there exists a set $\{P_x : x \in \{0,1\}^n\}$ of 2^n rank-r projectors on $\mathbb{C}^d$, with $r = \sqrt{10n}$ and $d = 2r/\varepsilon$, such that $\mathrm{tr}(P_x P_y) < \varepsilon r$ for all $x \neq y \in \{0,1\}^n$.*

Proof. Fix $\delta = 1$ and choose rank-r projectors $\{P_x : x \in \{0,1\}^n\}$ independently and uniformly at random. Claim 4.3 and our choice of parameters implies that for all $x \neq y \in \{0,1\}^n$,

$$\Pr\left[\mathrm{tr}(P_x P_y) \geq \frac{2r^2}{d}\right] = \Pr\left[\mathrm{tr}(P_x P_y) \geq \varepsilon r\right] < 2^{-r^2\delta^2/5} = 2^{-2n}.$$

The corollary now follows by applying a union bound over all distinct $x, y \in \{0,1\}^n$. □

We now prove Theorem 1.11.

Proof. Let $\{P_x : x \in \{0,1\}^n\}$ be projectors on $\mathbb{C}^d$ as guaranteed by Corollary 4.4, each of rank $r = \sqrt{10n}$, with $d = 2\sqrt{10n}/\varepsilon$. The following is our protocol for EQ_n.

Protocol 2: A mixed-state protocol Π for F

---

1. Alice, on input $x \in \{0,1\}^n$, sends the $\log d$-qubit mixed state $\rho_x := P_x/r$ to Bob.
2. Bob, on input $y \in \{0,1\}^n$, measures w.r.t. projectors $P_y, I - P_y$, and outputs 1 on observing the first measurement outcome, and 0 otherwise.

To see the correctness of this protocol, first observe that the protocol outputs the correct answer with probability 1 if $x = y$, because $\mathrm{tr}(P_x \rho_x) = \mathrm{tr}(P_x)/r = 1$. If $x \neq y$, then the error probability is the probability of Bob observing the first measurement outcome, which is

$$\Pr[\Pi(x, y) \neq \mathsf{EQ}_n(x, y)] = \mathrm{tr}(P_y \rho_x) = \mathrm{tr}(P_y P_x)/r < \varepsilon,$$

from Corollary 4.4. The cost is $\log d = \log(2\sqrt{10n}/\varepsilon) \leq \log(\sqrt{n}/\varepsilon) + 3$ qubits of communication. □

5 Quantum one-way lower bound

In this section we prove lower bounds on the one-way quantum communication complexity of any function whose communication matrix has a large number of distinct rows. As a consequence we obtain our lower bound for EQ_n of Theorem 1.10.

Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ be a Boolean function. We consider the model where communication is one-way, and Alice is only allowed to send a pure state to Bob. Suppose there exists a protocol of cost $\log d$ that computes F to error ε. Any such protocol looks like the following.

- Alice, on input $x \in \{0,1\}^n$, sends a message $|\phi_x\rangle$ to Bob, where $|\phi_x\rangle$ is a unit vector in $\mathbb{C}^d$.
- Bob, on input y, measures with respect to projectors $P_y, I - P_y$.

The acceptance probability of the protocol is $\|P_y|\phi_x\rangle\|^2$. Thus, we have

$$\|P_y|\phi_x\rangle\|^2 \geq 1-\varepsilon, \quad \|(I-P_y)|\phi_x\rangle\|^2 \leq \varepsilon \quad \text{for all } x,y \in F^{-1}(1), \tag{8}$$

and

$$\|P_y|\phi_x\rangle\|^2 \leq \varepsilon, \quad \|(I-P_y)|\phi_x\rangle\|^2 \geq 1-\varepsilon \quad \text{for all } x,y \in F^{-1}(0). \tag{9}$$

Claim 5.1. *Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ be a Boolean function with N distinct rows in M_F. Let $X \subseteq \{0,1\}^n$ be an arbitrary subset of size N that indexes distinct rows in M_F. For a one-way quantum communication protocol as above that computes F to error $\varepsilon \leq 1/2$, we have*

$$2 - 2\sqrt{\varepsilon(1-\varepsilon)} \leq \||\phi_{x_1}\rangle - |\phi_{x_2}\rangle\|^2 \leq 2 + 4\sqrt{\varepsilon}$$

for all distinct $x_1, x_2 \in X$.

Proof. Fix any two distinct $x_1, x_2 \in X$, and let $|\phi_{x_1}\rangle, |\phi_{x_2}\rangle \in \mathbb{C}^d$ be the messages sent by Alice on inputs x_1, x_2, respectively. Recall that $\||\phi_{x_1}\rangle\| = \||\phi_{x_2}\rangle\| = 1$. Because of the assumption that the rows of M_F indexed by X are all distinct, there is a $y \in \{0,1\}^n$ such that $F(x_1,y) \neq F(x_2,y)$. Without loss of generality assume $F(x_1,y) = 1$ and $F(x_2,y) = 0$. Write

$$\begin{aligned} |\phi_{x_1}\rangle &= P_y|\phi_{x_1}\rangle + (I-P_y)|\phi_{x_1}\rangle, \\ |\phi_{x_2}\rangle &= P_y|\phi_{x_2}\rangle + (I-P_y)|\phi_{x_2}\rangle. \end{aligned}$$

Thus,

$$\begin{aligned} \||\phi_{x_1}\rangle - |\phi_{x_2}\rangle\|^2 &= \|P_y(|\phi_{x_1}\rangle - |\phi_{x_2}\rangle)\|^2 + \|(I-P_y)(|\phi_{x_1}\rangle - |\phi_{x_2}\rangle)\|^2 \\ &\qquad \text{since } P_y \text{ and } I-P_y \text{ are orthogonal projectors} \\ &\geq (\|P_y|\phi_{x_1}\rangle\| - \|P_y|\phi_{x_2}\rangle)\|)^2 + (\|(I-P_y)|\phi_{x_1}\rangle\| - \|(I-P_y)|\phi_{x_2}\rangle\|)^2 \\ &\qquad \text{by the triangle inequality} \\ &\geq 2(\sqrt{1-\varepsilon} - \sqrt{\varepsilon})^2 \\ &\qquad \text{by Equations (8) and (9), and since } F(x_1,y)=1 \text{ and } F(x_2,y)=0 \\ &= 2 - 2\sqrt{\varepsilon(1-\varepsilon)}. \end{aligned}$$

For the upper bound, first define $p := \|P_y|\phi_{x_1}\rangle\|^2 \geq 1-\varepsilon$, and $q := \|(I-P_y)|\phi_{x_2}\rangle\|^2 \geq 1-\varepsilon$.

$$\begin{aligned} \||\phi_{x_1}\rangle - |\phi_{x_2}\rangle\|^2 &= \|P_y(|\phi_{x_1}\rangle - |\phi_{x_2}\rangle)\|^2 + \|(I-P_y)(|\phi_{x_1}\rangle - |\phi_{x_2}\rangle)\|^2 \\ &\leq (\|P_y|\phi_{x_1}\rangle\| + \|P_y|\phi_{x_2}\rangle\|)^2 + (\|(I-P_y)|\phi_{x_1}\rangle\| + \|(I-P_y)|\phi_{x_2}\rangle\|)^2 \\ &\qquad \text{by the triangle inequality} \\ &= (\sqrt{p} + \sqrt{1-q})^2 + (\sqrt{1-p} + \sqrt{q})^2 \\ &= 2 + 2\sqrt{p(1-q)} + 2\sqrt{(1-p)q} \leq 2 + 4\sqrt{\varepsilon}. \end{aligned}$$

□

We now state our main result of this section.

Theorem 5.2. *There exists an absolute constant c such that the following holds. Let $F : \{0,1\}^n \times \{0,1\}^n$ be a Boolean function with N distinct rows in M_F. Then for all $\varepsilon \in [1/N, 1/4]$,*

$$\mathsf{Q}_\varepsilon^{\mathrm{pure},\to}(F) \geq \log\left(\frac{\log N}{\varepsilon}\right) - \log\log\left(\frac{1}{\varepsilon}\right) - c.$$

Proof. Let $X \subseteq \{0,1\}^n$ be an arbitrary set of N elements that index distinct rows in M_F. Consider a protocol of cost $\log d$, as described in the beginning of this section, that computes F to error ε. Claim 5.1 implies existence of vectors $|\phi_x\rangle \in \mathbb{C}^d$ for all $x \in X$, such that

$$2 - 2\sqrt{\varepsilon(1-\varepsilon)} \leq \||\phi_{x_1}\rangle - |\phi_{x_2}\rangle\|^2 \leq 2 + 4\sqrt{\varepsilon} \tag{10}$$

for all distinct $x_1, x_2 \in X$. For each $x \in X$, define a real vector $|\phi_x^R\rangle \in \mathbb{R}^{2d}$ by

$$|\phi_x^R\rangle = \sum_{j \in [d]} |j\rangle \left(R(|\phi_x\rangle_j)|0\rangle + C(|\phi_x\rangle_j)|1\rangle\right),$$

where $R(|\phi_x\rangle_j)$ and $C(|\phi_x\rangle_j)$ denote the real and complex components of the j'th coordinate of $|\phi_x\rangle$, respectively. Note that each $|\phi_x^R\rangle$ is a unit vector, since the $|\phi_x\rangle$ are unit vectors. For all distinct $x_1, x_2 \in X$, we have

$$\begin{aligned} |\phi_{x_1}\rangle - |\phi_{x_2}\rangle &= \sum_{j \in [d]} |j\rangle(R(|\phi_{x_1}\rangle_j - |\phi_{x_2}\rangle_j) + i \cdot C(|\phi_{x_1}\rangle_j - |\phi_{x_2}\rangle_j)), \\ |\phi_{x_1}^R\rangle - |\phi_{x_2}^R\rangle &= \sum_{j \in [d]} |j\rangle((R(|\phi_{x_1}\rangle_j - |\phi_{x_2}\rangle_j)|0\rangle) + (C(|\phi_{x_1}\rangle_j - |\phi_{x_2}\rangle_j)|1\rangle)). \end{aligned}$$

Hence, Equation (10) implies

$$\||\phi_{x_1}^R\rangle - |\phi_{x_2}^R\rangle\|^2 = \||\phi_{x_1}\rangle - |\phi_{x_2}\rangle\|^2 \in [2 - 2\sqrt{\varepsilon(1-\varepsilon)}, 2 + 4\sqrt{\varepsilon}] \tag{11}$$

for all distinct $x_1, x_2 \in X$. Since $\|v - w\|^2 = \|v\|^2 + \|w\|^2 - 2\langle v, w\rangle$ for real vectors v, w, we obtain

$$|\langle \phi_{x_1}^R | \phi_{x_2}^R \rangle| \leq 2\sqrt{\varepsilon}$$

for all distinct $x_1, x_2 \in X$. Now consider the $N \times N$ matrix M whose rows and columns are indexed by strings in X, defined by

$$M_{x,y} = \langle \phi_x^R | \phi_y^R \rangle.$$

Since each $\phi_x^R \in \mathbb{R}^{2d}$, this matrix has rank at most $2d$. Since $\langle \phi_x^R | \phi_x^R \rangle = 1$ for all $x \in \{0,1\}^n$ and $|\langle \phi_x^R | \phi_y^R \rangle| \leq 2\sqrt{\varepsilon}$ for all $x \neq y \in X$, this M is a $2\sqrt{\varepsilon}$-approximation to the $N \times N$ Identity matrix I. Theorem 1.4 implies existence of an absolute constant $c_1 > 0$ such that

$$2d \geq \mathsf{rk}(M) \geq \mathsf{rk}_{2\sqrt{\varepsilon}}(I) \geq \frac{c_1 \log N}{\varepsilon \log(1/\sqrt{\varepsilon})}.$$

Hence,

$$\log d \geq \log\left(\frac{\log N}{\varepsilon}\right) - \log\log\left(\frac{1}{\varepsilon}\right) - \log(1/c_1),$$

concluding the proof. □

Theorem 1.10 immediately follows from Theorem 5.2 since all 2^n rows in M_{EQ_n} are distinct.

6 Approximate-rank upper bounds for distributed SINK function

In this section we show improved upper bounds on the approximate nonnegative-rank and approximate psd-rank of $M_{\mathsf{SINK}\circ\mathsf{XOR}}$, where SINK is defined as follows.

Definition 6.1. *Define the function* $\mathsf{SINK}_n : \{0,1\}^n \to \{0,1\}$ *on* $n = \binom{m}{2}$ *inputs as follows. The inputs are viewed as orientations of edges on a complete graph with* m *vertices. The function outputs 1 if there is a sink in the graph, and 0 otherwise.*

Consider the function $\mathsf{SINK}_n \circ \mathsf{XOR} : \{0,1\}^{2n} \to \{0,1\}$. This function was recently used to refute the randomized and quantum versions of the log-rank conjecture [CMS20, SW19, ABT19]. Chattopadhyay, Mande and Sherif [CMS20, Theorem 1.10] showed that the 1/3-approximate rank of $M_{\mathsf{SINK}_n\circ\mathsf{XOR}}$ is $O(m^4)$ and the 1/3-approximate nonnegative-rank of $M_{\mathsf{SINK}_n\circ\mathsf{XOR}}$ is $O(m^5)$. As a consequence of our improved upper bounds for the ε-approximate nonnegative-rank of the Identity matrix (Corollary 1.8), we are able to use the same proof idea as theirs to obtain an $O(m^4)$ upper bound on the 1/3-approximate nonnegative-rank of $M_{\mathsf{SINK}_n\circ\mathsf{XOR}}$, matching the approximate rank upper bound. We also obtain approximate psd-rank upper bounds for $\mathsf{SINK}_n \circ \mathsf{XOR}$.

Claim 6.2. *Let* m *be a positive integer, let* $n = \binom{m}{2}$. *Then,*

$$\mathsf{rk}^{+}_{1/3}(M_{\mathsf{SINK}_n\circ\mathsf{XOR}}) = O(m^4)$$
$$\mathsf{rk}^{\mathrm{psd}}_{1/3}(M_{\mathsf{SINK}_n\circ\mathsf{XOR}}) = O(m^{2.5}).$$

Proof. Note that $\mathsf{SINK}_n \circ \mathsf{XOR}$ can be expressed as a *sum* of m Equalities, each with $2(m-1)$ inputs, one corresponding to each vertex in the underlying graph for SINK. Recall that the communication matrix of Equality is the Identity matrix. We require sub-additivity of nonnegative-rank and psd-rank, which are both easy to verify.

- Corollary 1.8 implies that each of these Equalities have $(1/3m)$-approximate nonnegative-rank $O(m^3)$. Summing up these m matrices, we conclude that the $(1/3)$-approximate nonnegative-rank of $\mathsf{SINK}_n \circ \mathsf{XOR}$ equals $O(m^4)$.
- Corollary 1.12 implies that each of these Equalities have $(1/3m)$-approximate psd-rank $O(m^{1.5})$. Summing up these m matrices, we conclude that the $(1/3)$-approximate psd-rank of $\mathsf{SINK}_n \circ \mathsf{XOR}$ equals $O(m^{2.5})$.

□

7 Future work

We mention some possible directions for future work:

- Those of our lower bounds that use Alon's approximate-rank bound (Theorem 1.4) lose an additive $\log\log(1/\varepsilon)$. This term is necessary in some regimes, in particular when ε is very small ($\sim 2^{-n}$) and n/ε gets bigger than the trivial dimension upper bound 2^n. However, in some regimes it may be avoidable. Also Alon's bound itself might be slightly improvable.

- We leave open the optimal quantum communication complexity of Equality with small error in the *simultaneous message passing* (SMP) model, where Alice and Bob each send a message to a "referee" who has to decide the output. With public randomness $\log(1/\varepsilon) \pm O(1)$ classical bits of communication are necessary and sufficient, but with private randomness it is not clear. In the classical case, $\Theta(\sqrt{n})$ bits of communication are necessary [NS96] and sufficient [Amb96] for constant error. In the quantum case, $\Theta(\log n)$ qubits are necessary and sufficient [BCWW01] for constant error. One can get an $O(\log(n)\log(1/\varepsilon))$ ε-error upper bound by repeating the quantum fingerprinting protocol of Buhrman et al. [BCWW01] $O(\log(1/\varepsilon))$ times, but that is much worse than the $\log(\sqrt{n}/\varepsilon)$ and $\log(n/\varepsilon)$ upper bounds that we have in the one-way mixed-state and pure-state scenarios (Theorems 1.11 and 1.9). In neither the randomized nor the quantum SMP settings do we have tight bounds for small ε.

Acknowledgements. We thank Troy Lee, Ignacio Villanueva, and Zhaohui Wei for early discussions related to the result of Section 4.3. We thank Swagato Sanyal for discussions at an early stage of this work, from which the question of pinning down the exact communication complexity of Equality for small ε arose.

References

[ABT19] Anurag Anshu, Naresh Goud Boddu, and Dave Touchette. Quantum log-approximate-rank conjecture is also false. In *Proceedings of the 60th IEEE Annual Symposium on Foundations of Computer Science (FOCS)*, pages 982–994, 2019.

[Alo09] Noga Alon. Perturbed identity matrices have high rank: Proof and applications. *Combinatorics, Probability and Computing*, 18(1-2):3–15, 2009.

[Amb96] Andris Ambainis. Communication complexity in a 3-computer model. *Algorithmica*, 16(3):298–301, 1996.

[BCWW01] Harry Buhrman, Richard Cleve, John Watrous, and Ronald de Wolf. Quantum fingerprinting. *Physical Review Letters*, 87(16), September 26, 2001. quant-ph/0102001.

[BW01] Harry Buhrman and Ronald de Wolf. Communication complexity lower bounds by polynomials. In *Proceedings of the 16th Annual IEEE Conference on Computational Complexity (CCC)*, pages 120–130, 2001.

[CMS20] Arkadev Chattopadhyay, Nikhil S. Mande, and Suhail Sherif. The log-approximate-rank conjecture is false. *Journal of the ACM*, 67(4):23:1–23:28, 2020. Earlier version in STOC, 2019.

[FGP+15] Hamza Fawzi, João Gouveia, Pablo A. Parrilo, Richard Z. Robinson, and Rekha R. Thomas. Positive semidefinite rank. *Mathematical Programming*, 153(1):133–177, 2015.

[HLW06] Patrick Hayden, Debbie W. Leung, and Andreas Winter. Aspects of generic entanglement. *Communications in Mathematical Physics*, 265(1):95–117, 2006.

[KN97] Eyal Kushilevitz and Noam Nisan. *Communication Complexity*. Cambridge University Press, 1997.

[Kra96] Matthias Krause. Geometric arguments yield better bounds for threshold circuits and distributed computing. *Theoretical Computer Science*, 156(1&2):99–117, 1996.

[Kre95] Ilan Kremer. Quantum communication. Master's thesis, Hebrew University, Computer Science Department, 1995.

[LWW17] Troy Lee, Zhaohui Wei, and Ronald de Wolf. Some upper and lower bounds on psd-rank. *Mathematical Programming, Series A*, 162(1–2):495–521, 2017.

[MU05] Michael Mitzenmacher and Eli Upfal. *Probability and Computing: Randomized Algorithms and Probabilistic Analysis*. Cambridge University Press, 2005.

[Nay99] Ashwin Nayak. *Lower bounds for Quantum Computation and Communication*. PhD thesis, University of California, Berkeley, 1999.

[New91] Ilan Newman. Private vs. common random bits in communication complexity. *Information Processing Letters*, 39(2):67–71, 1991.

[Nie98] Michael A. Nielsen. *Quantum Information Theory*. PhD thesis, University of New Mexico, Albuquerque, 1998.

[NS96] Ilan Newman and Mario Szegedy. Public vs. private coin flips in one round communication games. In *Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC)*, pages 561–570, 1996.

[RY20] Anup Rao and Amir Yehudayoff. *Communication Complexity and Applications*. Cambridge University Press, 2020.

[SW19] Makrand Sinha and Ronald de Wolf. Exponential separation between quantum communication and logarithm of approximate rank. In *Proceedings of the 60th IEEE Annual Symposium on Foundations of Computer Science (FOCS)*, pages 966–981, 2019.

[Wol02] Ronald de Wolf. Quantum communication and complexity. *Theoretical Computer Science*, 287(1):337–353, 2002.

[Yao79] Andrew Chi-Chih Yao. Some complexity questions related to distributive computing (preliminary report). In *Proceedings of the 11h Annual ACM Symposium on Theory of Computing (STOC)*, pages 209–213, 1979.

[Yao93] Andrew Chi-Chih Yao. Quantum circuit complexity. In *Proceedings of the 34th IEEE Annual Symposium on Foundations of Computer Science (FOCS)*, pages 352–361, 1993.

A Quantum communication complexity and psd-rank

In this section, we prove Theorem 1.3, restated below.

Theorem A.1 (Restatement of Theorem 1.3)**.** *Let* $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ *be a Boolean function and let* $\varepsilon > 0$*. Then,*

$$\mathsf{Q}^{\mathsf{pri}}_{\varepsilon}(F) \geq \log \mathsf{rk}^{\mathrm{psd}}_{\varepsilon}(M_F) + 1.$$

Proof. Consider an ℓ-qubit protocol for F, without public randomness. Because private randomness can be generated using Hadamard gates, we will assume the protocol is unitary, with only a measurement of the output qubit at the end. Let the starting state of the protocol be $|x0^s\rangle_A|y0^s\rangle_B|0\rangle_C$, where the first and second parts are Alice and Bob's register, respectively (containing their input and s workspace qubits each), and the third part is the channel qubit. It is easy to prove by induction that after ℓ qubits of communication, the final state of a protocol has the following form (first observed by Kremer [Kre95] and Yao [Yao93]):

$$\sum_{i\in\{0,1\}^\ell} |a_i(x)\rangle|b_i(y)\rangle|i_\ell\rangle,$$

where $|a_i(x)\rangle, |b_i(y)\rangle$ are subnormalized quantum states. Let P denote the acceptance probability matrix, i.e., $P(x,y)$ is the probability that the protocol outputs 1 on input (x,y). We assume without loss of generality that the output qubit is the last qubit put on the channel. We have

$$P(x,y) = \left\| \sum_{i\in\{0,1\}^\ell : i_\ell=1} |a_i(x)\rangle|b_i(y)\rangle|i_\ell\rangle \right\|^2 = \sum_{i,i'\in\{0,1\}^\ell : i_\ell = i'_\ell = 1} \langle a_i(x)|a_{i'}(x)\rangle \cdot \langle b_i(y)|b_{i'}(y)\rangle.$$

For each $x \in \{0,1\}^n$ define a $2^{\ell-1} \times 2^{\ell-1}$ matrix A_x with rows and columns indexed by strings $i, i' \in \{0,1\}^{\ell-1} \times \{1\}$:

$$A_x(i,i') = \langle a_i(x)|a_{i'}(x)\rangle.$$

Similarly, for each $y \in \{0,1\}^n$ define a $2^{\ell-1} \times 2^{\ell-1}$ matrix B_y by

$$B_y(j,j') = \langle b_j(y)|b_{j'}(y)\rangle.$$

These A_x and B_y are Gram matrices and hence psd. Moreover it is easy to verify that $P(x,y) = \mathrm{tr}(A_x B_y)$. Since the protocol makes error at most ε on each input, the matrix P entrywise approximates M_F up to ε. Hence $\mathsf{rk}^{\mathrm{psd}}_{\varepsilon}(M_F) \leq 2^{\ell-1}$. Taking logarithms gives the theorem. □

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il