THEORY OF COMPUTING, Volume 22 (2272), 2025, pp. 1–18
www.theoryofcomputing.org

SPECIAL ISSUE: APPROX-RANDOM 2025

Equality is Far Weaker than Constant-Cost Communication

Mika Göös Nathaniel Harms Artur Riazanov

Received September 30, 2025; Revised April 19, 2026; Published July 20, 2026

Abstract. We exhibit an n-bit communication problem with a constant-cost randomized protocol but which requires $n^{\Omega(1)}$ deterministic (or even non-deterministic) queries to an EQUALITY oracle. Therefore, even *constant-cost* randomized protocols cannot be efficiently "derandomized" using EQUALITY oracles. This improves on several recent results and answers a question from the survey of Hatami and Hatami (SIGACT News 2024). It also gives a significantly simpler and quantitatively superior proof of the main result of Fang, Göös, Harms, and Hatami (STOC 2025), that constant-cost communication does not reduce to the k-HAMMING DISTANCE hierarchy.

1 Introduction

In this paper we prove strong limits on the power of "simple hashing" for the purpose of communication. In communication complexity, simple hashing, i. e.the EQUALITY communication problem, is the most dramatic example of the power of randomness. Alice and Bob each have

A preliminary version of this paper appeared as [9].

ACM Classification: F.1.3

AMS Classification: 68Q17

Key words and phrases: communication complexity, equality oracle, randomized communication

© 2025 Mika Göös, Nathaniel Harms, and Artur Riazanov
Licensed under a Creative Commons Attribution License (CC-BY)
DOI: 10.4086/toc.2025.v022a2272

binary strings $x, y \in \{0,1\}^n$ and their goal is to decide whether $x = y$. With public randomness, they can generate a random 2-bit hash $\boldsymbol{h}(z)$ for every z and check if $\boldsymbol{h}(x) = \boldsymbol{h}(y)$. This succeeds with probability at least 3/4 and requires only 2 bits of communication regardless of the size of the input n [16, 19].

Randomized communication can often be "derandomized" by allowing Alice and Bob access to an oracle which (deterministically) computes EQUALITY. Write $\mathsf{D}^{\mathrm{EQ}}(F)$ for the minimum cost of a deterministic protocol computing F with access to this oracle, and $\mathsf{R}(F)$ for the public-coin randomized communication cost (with error probability 1/3). Here are three examples covering a range of complexities:

Example 1.1 (Greater Than)**.** Alice and Bob are given n-bit integers x, y and their goal is to decide whether $x > y$. They can perform binary search to find the highest-order bit where x and y differ, by querying the EQUALITY oracle (check if the first half of their bits are equal, etc.), so $\mathsf{D}^{\mathrm{EQ}}(\mathrm{GT}_n) = O(\log n)$, where GT_n denotes the GREATER-THAN problem on n bits. Randomized communication satisfies $\mathsf{R}(F) = O(\mathsf{D}^{\mathrm{EQ}}(F))$ [17, 12], which in this case gives the optimal randomized protocol: $\mathsf{R}(\mathrm{GT}_n) = \Theta(\log n)$ [17, 1, 24, 22].

Example 1.2 (Planar Adjacency [11, 13])**.** Alice and Bob are given vertices x, y in a (shared) planar graph P and wish to decide if they are adjacent. A planar graph is the edge union of 3 forests, so they can check adjacency in P by checking adjacency in each forest: x is equal to the parent of y or vice versa. So $\mathsf{D}^{\mathrm{EQ}} \leq 6$ for this problem and therefore its randomized cost is *constant* (independent of the input size), which is clearly optimal.

Example 1.3 (1-Hamming Distance)**.** Alice and Bob are given $x, y \in \{0,1\}^n$ and their goal is to decide if x, y differ on at most 1 bit. Using binary search with the EQUALITY oracle, we get $\mathsf{D}^{\mathrm{EQ}}(\mathrm{HD}_1^n) = O(\log n)$, where HD_1^n denotes the 1-HAMMING DISTANCE problem on n bits. This protocol is *not* optimal, since $\mathsf{R}(\mathrm{HD}_1^n) = O(1)$, but it is still *efficient*, i. e.$\mathsf{D}^{\mathrm{EQ}}(\mathrm{HD}_1^n) = \operatorname{poly}\log n$.

Can *every* efficient randomized protocol be replaced with an EQUALITY oracle protocol? This is especially interesting for problems like PLANAR ADJACENCY and 1-HAMMING DISTANCE that have *constant* randomized cost, because one may reasonably expect the answer to be *yes*, i. e.any constant-cost randomized protocol can be replaced with $\operatorname{poly}\log n$ EQUALITY queries, as in Theorem 1.3. On the contrary, we show:

Theorem 1.4. *There exists a communication problem* $F\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ *with*

$$\mathsf{R}(F) = O(1) \qquad \textit{and} \qquad \mathsf{D}^{EQ}(F) = \Theta(\sqrt{n}).$$

In terms of complexity classes, this implies $\mathsf{BPP}_0 \not\subseteq \mathsf{P}^{\mathrm{EQ}}$, where BPP_0 is the class of randomized constant-cost problems and P^{EQ} is the class of problems with EQUALITY oracle cost $\operatorname{poly}\log n$.

Communication oracles including EQUALITY, HD_1, and others, are well studied [2, 10, 13, 6, 18, 4, 5, 14, 8, 7, 3]. Theorem 1.4 improves on results from several of these works and our proof answers a number of open questions.

Separation of $\mathsf{R}(F)$ and $\mathsf{D}^{\mathrm{Eq}}(F)$. Whether EQUALITY oracles can efficiently derandomize communication was first asked in [2], who showed that there exists a problem F with

$$\mathsf{R}(F) = O(\log n) \qquad \text{and} \qquad \mathsf{D}^{\mathrm{Eq}}(F) = \Theta(n).$$

This established that $\mathsf{BPP} \not\subseteq \mathsf{P}^{\mathrm{Eq}}$, where BPP is the class of n-bit communication problems with randomized communication cost $\operatorname{poly}\log n$. This separation was improved in [3] to hold for XOR functions (see also [4, 18, 23]).

Recently, there has been significant effort to understand the most extreme examples of the power of randomness in communication, i. e.the problems with constant cost. The question of how well EQUALITY oracles can derandomize constant cost communication was posed in [10, 13], who showed that EQUALITY is not "complete" for the class of constant-cost problems, i. e.$\mathsf{BPP}_0 \not\subseteq \mathsf{P}_0^{\mathrm{Eq}}$, where $\mathsf{P}_0^{\mathrm{Eq}}$ is the class of problems F with $\mathsf{D}^{\mathrm{Eq}}(F) = O(1)$. But the best known lower bound on D^{Eq} for a constant-cost problem is from [10] (see also [12]), who proved a D^{Eq} lower bound matching Theorem 1.3:

$$\mathsf{R}(\mathrm{HD}_1) = O(1) \qquad \text{and} \qquad \mathsf{D}^{\mathrm{Eq}}(\mathrm{HD}_1) = \Theta(\log n).$$

This leads to the question, implicit in [4] and explicit in the survey [15], of whether constant-cost protocols can be replaced with $\operatorname{poly}\log n$ EQUALITY queries. We answer *no*, improving the separation $\mathsf{BPP} \not\subseteq \mathsf{P}^{\mathrm{Eq}}$ to $\mathsf{BPP}_0 \not\subseteq \mathsf{P}^{\mathrm{Eq}}$. Our example F is an XOR function, so we also improve on the separation of [3].

Separation of BPP_0 and k-HAMMING DISTANCE. Following the result that EQUALITY is not complete for BPP_0, [7] showed that the infinite hierarchy of k-HAMMING DISTANCE problems HD_k (decide if x, y differ on at most k bits) is also not complete: there exists F with $\mathsf{R}(F) = O(1)$ and yet $\mathsf{D}^{\mathrm{HD}_k}(F) = \omega(1)$ for every constant k, where $\mathsf{D}^{\mathrm{HD}_k}(F)$ is the minimum number of queries to an HD_k oracle required to compute F. We give a significantly simpler and quantitatively superior proof (for a different F), with a lower bound of $\tilde{\Omega}(\sqrt{n})$ instead of $\omega(1)$:

Corollary 1.5. *There exists an n-bit function F such that for any constant k,*

$$\mathsf{R}(F) = O(1) \qquad \textit{and} \qquad \mathsf{D}^{HD_k}(F) \geq \tilde{\Omega}(\sqrt{n}).$$

Two Proofs with Five Corollaries

We give two incomparable proofs of Theorem 1.4: one analytic, one combinatorial, each with different consequences beyond the ones above, which we elaborate in Section 5.

Analytic proof: γ_2-norm and decision trees. We show in Theorem 3.2 that the γ_2-*norm* of our problem F (equivalently, the spectral norm of f, see Section 5.2) is $2^{\Omega(\sqrt{n})}$. As a consequence:

- Our function F is an XOR function, meaning $F(x, y) = f(x \oplus y)$ for some function f. Since XOR functions $F(x, y) = f(x \oplus y)$ satisfy the property that the γ_2-norm of F is equal to the

Fourier spectral norm of f [10], we exhibit a function f with *approximate* spectral norm $O(1)$ yet *exact* spectral norm $2^{\Omega(\sqrt{n})}$ (Theorem 5.4).

- We answer [3, Question 8], asking whether there exists a function $f\colon \{0,1\}^n \to \{0,1\}$ with randomized parity decision tree size $O(1)$ but deterministic parity decision tree size $n^{\omega(1)}$. Our f has deterministic parity decision tree size $2^{\Omega(\sqrt{n})}$ (Theorem 5.5).
- We make progress on [4, Question 5], asking whether any n-bit function with $\mathsf{R}(F) = O(1)$ has γ_2-norm $2^{\Omega(n)}$. Our function does not achieve this maximal value but it improves exponentially on the best known value of $\Theta(\sqrt{n})$, for the HD_1 function [10].

Combinatorial proof: non-deterministic EQUALITY protocols. Using the *blocky cover number* of [18], we show that F has EQUALITY oracle cost $\Omega(\sqrt{n})$ even for a *non-deterministic* protocol. As a consequence of our proof:

- We improve the complexity class separation in Theorem 1.4, from $\mathsf{BPP}_0 \not\subseteq \mathsf{P}^{\mathrm{EQ}}$ to $\mathsf{BPP}_0 \not\subseteq \mathsf{NP}^{\mathrm{EQ}}$. This improves on a result of [18] who showed $\mathsf{BPP} \not\subseteq \mathsf{NP}^{\mathrm{EQ}}$.
- We tighten the theorem of [18] relating the *blocky cover number* and the non-deterministic EQUALITY oracle cost $\mathsf{ND}^{\mathrm{EQ}}(\cdot)$. This improves the lower bounds on $\mathsf{ND}^{\mathrm{EQ}}(\cdot)$ given in [18, 3] and answers the question posed after [3, Theorem 5], asking if $\mathsf{ND}^{\mathrm{EQ}}(\mathrm{IIP}_3^n) = \Omega(n)$, where IIP_3^n is the INTEGER INNER PRODUCT function defined in [2].

2 The Problem

The problem is a special case of those studied recently by Sherstov & Storozhenko [21]. Alice and Bob are given matrices $A, B \in \mathbb{F}_2^{n\times n}$ and their goal is to decide if the $\mathbb{F}_2$-rank of $A + B$ is at most 1; i. e.$\textsc{RankOne}_n\colon \{0,1\}^{n\times n} \times \{0,1\}^{n\times n} \to \{0,1\}$ is defined by

$$\textsc{RankOne}_n(A,B) \coloneqq \begin{cases} 1 & \text{if } A \oplus B \text{ has rank} \le 1 \\ 0 & \text{otherwise.} \end{cases}$$

Note that a matrix $C \in \{0,1\}^{n\times n}$ has rank ≤ 1 if and only if its 1-entries form a combinatorial rectangle, i. e.there are sets $X, Y \subseteq [n]$ such that $C(x,y) = 1$ iff $(x,y) \in X \times Y$. This problem is an XOR problem, i. e.$\textsc{RankOne}_n(A,B) = f(A \oplus B)$ for the boolean function $f\colon \{0,1\}^{n\times n} \to \{0,1\}$ defined as $f(M) = 1$ if and only if M has rank at most 1.

Sherstov & Storozhenko [21] prove tight bounds for the randomized communication complexity of computing rank r over any finite field. For the sake of completeness, we include a simple proof that $\mathsf{R}(\textsc{RankOne}_n) = O(1)$. More specifically, we prove that the randomized parity decision tree depth of f is $O(1)$ (which immediately implies the same for randomized communication).

A function $g\colon \{0,1\}^n \to \{0,1\}$ is computed by a depth-d parity decision tree if, for any $x \in \{0,1\}^n$, $g(x)$ can be computed with at most d adaptive queries of the form $\oplus_{i\in S} x_i$ for chosen

$S \subseteq [n]$. A function g is computed by a *randomized* parity decision tree if there exists a distribution μ over parity decision trees such that for every input $x \in \{0,1\}^n$, $\Pr_{T\sim\mu}[\boldsymbol{T}(x) = g(x)] \geq 2/3$.

Theorem 2.1. *Let $f : \{0,1\}^{n\times n} \to \{0,1\}$ be as above: $f(M) = 1$ iff $\mathrm{rk}_{\mathbb{F}_2}(M) \leq 1$. Then it is computed by a randomized parity decision tree of constant depth (i. e.independent of n).*

Proof. Given input M, the tree chooses sets $\boldsymbol{A}_1, \boldsymbol{A}_2, \boldsymbol{B}_1, \boldsymbol{B}_2 \subseteq [n]$ uniformly at random. For each $\alpha, \beta \in [2]$, the tree queries $\boldsymbol{C}_{\alpha,\beta} \coloneqq \bigoplus_{(i,j)\in \boldsymbol{A}_\alpha \times \boldsymbol{B}_\beta} M_{ij}$, to form the 2×2 matrix $\boldsymbol{C}$. The tree outputs 1 iff $\mathrm{rk}(\boldsymbol{C}) \leq 1$.

The transformation from M to $\boldsymbol{C}$ can be seen as a two-step process: first, we generate a $n \times 2$ matrix $\boldsymbol{C}'$ where column $i \in [2]$ is the sum of columns $j \in \boldsymbol{B}_i$ of M. Then we generate the 2×2 matrix $\boldsymbol{C}$ where row j is the sum of rows $i \in \boldsymbol{A}_j$ of $\boldsymbol{C}'$. Neither step may increase the rank of the matrix, so if $\mathrm{rk}(M) \leq 1$, then $\Pr[\mathrm{rk}(\boldsymbol{C}) \leq 1] = 1$.

Now suppose $\mathrm{rk}(M) \geq 2$. Each column of $\boldsymbol{C}'$ is chosen uniformly from the column space of M. The size of the column space is at least 4, so the probability that both columns of $\boldsymbol{C}'$ are nonzero and distinct is at least $\frac{3}{4} \cdot \frac{1}{2} = \frac{3}{8}$. Conditional on this event, by the same argument, the probability that both rows of $\boldsymbol{C}$ are nonzero and distinct is at least $\frac{3}{8}$. Therefore, the tree will output 0 with probability at least 9/64. We can boost this to 2/3 by repetition. ∎

To clarify notation, observe that the inputs to this function are naturally expressed with n^2 variables, whereas Theorem 1.4 is stated for a function on n variables. So to prove Theorem 1.4 we must show

$$\mathsf{D}^{\mathrm{EQ}}(\textsc{RankOne}_n) = \Theta(n). \tag{2.1}$$

The upper bound is simple:

Proposition 2.2. $\mathsf{D}^{EQ}(\textit{RankOne}_n) = O(n)$.

Proof. Suppose Alice receives a matrix A with rows $a_1, \ldots, a_n \in \{0,1\}^n$, and Bob receives a matrix B with rows $b_1, \ldots, b_n \in \{0,1\}^n$. Then $\mathrm{rk}(A \oplus B) \leq 1$ if and only if each pair $i, j \in [n]$ with $a_i \neq b_i$ and $a_j \neq b_j$ satisfy $a_i \oplus b_i = a_j \oplus b_j$. Using n queries $\mathrm{EQ}(a_1, b_1), \mathrm{EQ}(a_2, b_2), \ldots, \mathrm{EQ}(a_n, b_n)$, Alice and Bob can find i such that $a_i \neq b_i$ if such an i exists (otherwise $\mathrm{rk}(A \oplus B) = 0$). Then for every $j \in [n]$ such that $a_j \neq b_j$ they check that $a_j \oplus b_j = a_i \oplus b_i$ by making the query $\mathrm{EQ}(a_j \oplus a_i, b_j \oplus b_i)$. If any EQUALITY-query comes out negative, Alice and Bob output 0, otherwise they output 1. ∎

3 Analytic Proof

We analyze the γ_2-norm of $\textsc{RankOne}_n$. The γ_2-norm of a matrix $M \in \mathbb{R}^{N\times N}$ is defined as

$$\gamma_2(M) \coloneqq \min_{M=UV} \|U\|_{\mathrm{row}} \|V\|_{\mathrm{col}},$$

where the minimum is over matrices $U, V \in \mathbb{R}^d$ (in any dimension d) satisfying $M = UV$, $\|U\|_{\mathrm{row}}$ is the maximum ℓ_2-norm of any row of U, and $\|V\|_{\mathrm{col}}$ is the maximum ℓ_2-norm of any

column of V. The γ_2-norm is related to the EQUALITY oracle cost by

$$\forall M \in \{0,1\}^{N\times N} : \qquad \frac{1}{2}\log \gamma_2(M) \le \mathsf{D}^{\mathrm{EQ}}(M) \qquad ([10]). \tag{3.1}$$

To give a lower bound on γ_2, we use the Hölder's inequality framework introduced in [3]. Write $\|M\|_F := (\sum_{i,j\in[N]} M_{i,j}^2)^{1/2}$ for the Frobenius norm of a matrix $M \in \mathbb{R}^{N\times N}$. Then:

Lemma 3.1 (Corollary of Hölder's inequality, [3])**.** *For any matrix $M \in \mathbb{R}^{N\times N}$,*

$$\gamma_2(M) \ge \frac{1}{N}\cdot\frac{\|M\|_F^3}{\sqrt{\mathrm{tr}((M^TM)^2)}}.$$

In the next theorem, note that the number of bits in the input of $\textsc{RankOne}_n$ is n^2, not n; by renaming the number of bits and applying Equation (3.1), we get the bound in Theorem 1.4.

Theorem 3.2. *$\gamma_2(\textsc{RankOne}_n) = 2^{\Theta(n)}$. As a consequence, $\mathsf{D}^{EQ}(\textsc{RankOne}_n) = \Omega(n)$.*

Proof. The upper bound follows from Theorem 2.2 and Equation (3.1). For the lower bound, we shall apply Theorem 3.1 to the matrix $\textsc{RankOne}_n \in \{0,1\}^{N\times N}$ where $N = 2^{n^2}$. For convenience we write $M := \textsc{RankOne}_n$. Since this matrix is boolean, the Frobenius norm is $\|M\|_F = (\sum_{i,j\in[N]} M_{i,j}^2)^{1/2} = (\sum_{i,j\in[N]} M_{i,j})^{1/2}$, so it suffices to count the number of 1-valued entries. Rows of M are identified with matrices $A \in \{0,1\}^{n\times n}$. There are $(2^n-1)^2 \ge 2^{2n-2}$ rectangles $R \subseteq [n]\times[n]$ and they are in 1-to-1 correspondence with rank-1 matrices $Z \in \{0,1\}^{n\times n}$; here and in what follows, let us abuse language and consider the all-0 matrix (corresponding to the empty rectangle) to also be "rank-1". For fixed row A, each rank-1 matrix Z has a unique $B \in \{0,1\}^{n\times n}$ such that $A \oplus B = Z$. Therefore the number of 1-valued entries in each row A is 2^{2n}. So

$$\|M\|_F = \sqrt{N\cdot 2^{2n-2}} = 2^{n-1}\cdot\sqrt{N}. \tag{3.2}$$

Now we bound the denominator in Theorem 3.1,

$$\mathrm{tr}((M^TM)^2) = \sum_{x,y,z,w\in[N]} M_{x,z}M_{x,w}M_{y,z}M_{y,w}.$$

Rows and columns $x,y,z,w \in [N]$ are identified with matrices $X,Y,Z,W \in \{0,1\}^{n\times n}$. The product $M_{x,z}M_{x,w}M_{y,z}M_{y,w}$ equals 1 iff $R_1 := X\oplus Z$, $R_2 := X\oplus W$, $R_3 := Y\oplus Z$, and $R_4 := Y\oplus W$ are all rank-1 matrices in $\{0,1\}^{n\times n}$. Then the quadruple (X,Y,Z,W) is uniquely determined by $(X,R_1,\ldots,R_4)$ which in turn is determined by (X,R_1,R_2,R_3) since $R_4 = R_1\oplus R_2\oplus R_3$. So:

$$\sum_{x,y,z,w} M_{x,z}M_{x,w}M_{y,z}M_{y,w} = N\cdot\Big|\{(R_1,R_2,R_3)\in(\{0,1\}^{n\times n})^3 \mid \mathrm{rk}(R_i)\le 1;\ \mathrm{rk}(R_1\oplus R_2\oplus R_3)\le 1\}\Big|.$$

Now it remains to bound the number of triples (R_1,R_2,R_3) of rank-1 matrices that sum to a rank-1 matrix. Recall that rank-1 matrices over $\mathbb{F}_2$ are precisely the matrices whose 1-entries form a combinatorial rectangle, let $A_i\times B_i \subseteq [n]^2$ be this rectangle for R_i for $i\in[3]$.

We say that two sets A, B are in *general position* if they are not disjoint and neither set is a subset of another. In other words $A \setminus B$, $A \cap B$, and $B \setminus A$ are all non-empty. We first show that there are at most $6 \cdot 3^n \cdot 2^{4n}$ triples (R_1, R_2, R_3) where the sides of R_1, R_2 are *not* in general position. Then we show that, if the sides of the first two rectangles R_1, R_2 *are* in general position, there is only a constant number of choices for R_3, meaning that there are at most $9 \cdot 2^{4n}$ of these triples. Therefore

$$\operatorname{tr}((M^T M)^2) = \sum_{x,y,z,w} M_{x,z} M_{x,t} M_{y,z} M_{y,w} \leq N \left(6 \cdot 3^n \cdot 2^{4n} + 9 \cdot 2^{4n}\right) \leq 15 \cdot N \cdot 3^n \cdot 2^{4n}.$$

Then Theorem 3.1 implies

$$\gamma_2(\textsc{RankOne}_n) \geq \frac{1}{N} \cdot \frac{N^{3/2} 2^{3n-3}}{\sqrt{15} \cdot \sqrt{N} \cdot (3 \cdot 2^4)^{n/2}} = \frac{1}{8\sqrt{15}} \cdot \left(\frac{8}{\sqrt{3} \cdot 4}\right)^n = 2^{\Omega(n)},$$

which concludes the proof, once we establish the claimed bounds on the number of triples.

Structured pairs. We count the number of triples (R_1, R_2, R_3) where $R_1 = A_1 \times B_1$ and $R_2 = A_2 \times B_2$ have either A_1, A_2 or B_1, B_2 not in general position. First we count the number of choices for A_1, A_2 where $A_1 \subseteq A_2$. This is at most 3^n because each $i \in [n]$ can be included in $A_2 \setminus A_1$, A_1, or neither. Therefore the number of triples (R_1, R_2, R_3) where $A_1 \subseteq A_2$ is at most $3^n \cdot (2^n)^4$, accounting for the choices of A_3, B_1, B_2, B_3. Similar arguments hold for the other cases of non-general position of A_1, A_2 or B_1, B_2. There are 6 cases in total, so the number of triples (R_1, R_2, R_3) is at most $6 \cdot 3^n \cdot 2^{4n}$.

General position. We count the number of triples (R_1, R_2, R_3) which sum to a rank-1 matrix, and where A_1, A_2 and B_1, B_2 are both in general position. We claim that there is only a constant number options for $R_3 = A_3 \times B_3$ such that $\operatorname{rk}(R_1 \oplus R_2 \oplus R_3) = 1$. Let us first rule out the case where $A_3 \supseteq A_1 \cup A_2$ or $B_3 \supseteq B_1 \cup B_2$. Let us take representatives i, j, k from $A_1 \setminus A_2$, $A_1 \cap A_2$, $A_2 \setminus A_1$ respectively, and i', j', k' from $B_1 \setminus B_2$, $B_1 \cap B_2$, $B_2 \setminus B_1$ respectively. The submatrix of $R_1 \oplus R_2$ on rows $\{i, j, k\}$ and columns $\{i', j', k'\}$ is

$$P \coloneqq (R_1 \oplus R_2)|_{\{i,j,k\} \times \{i',j',k'\}} = J_3 \oplus I_3,$$

where J_3 is 3×3 all-1 matrix and I_3 is the 3×3 identity matrix. Then if $A_3 \supseteq \{i, j, k\}$ then $P \oplus R_3|_{\{i,j,k\} \times \{i',j',k'\}}$ has either two distinct columns from $J_3 \oplus I_3$ or two distinct columns from I_3, in both cases $\operatorname{rk}(R_1 \oplus R_2 \oplus R_3) \geq 2$. The same argument shows that $B_3 \not\supseteq \{i', j', k'\}$.

Then there are a row and a column that are nonzero in $R_1 \oplus R_2$ and zero in R_3. Suppose that their values in $R_1 \oplus R_2$ are $a \in \{0,1\}^n$ and $b \in \{0,1\}^n$, respectively. Since $\operatorname{rk}(R_1 \oplus R_2 \oplus R_3) = 1$, any two nonzero rows of $R_1 \oplus R_2 \oplus R_3$ must be equal, and any two nonzero columns must also be equal. Since a, b are nonzero, this requires $R_1 \oplus R_2 \oplus R_3 = a \cdot b^T$. For fixed R_1, R_2, there are only three possible values of a and b, so there are at most 9 options for the value of R_3. Therefore there are at most $9 \cdot (4^n)^2$ triples (R_1, R_2, R_3) in this case. ∎

4 Combinatorial Proof

We prove a lower bound on the non-deterministic EQUALITY oracle cost of $\textsc{RankOne}_n$. The non-deterministic EQUALITY oracle cost of any matrix $M \in \{0,1\}^{N\times N}$ is denoted $\mathsf{ND}^{\mathrm{EQ}}(M)$. It is defined as the minimum value t such that there are numbers m, d with $m + d = t$, where there exist matrices $M_1, \dots, M_{2^m} \in \{0,1\}^{N\times N}$ satisfying:

1. $\mathsf{D}^{\mathrm{EQ}}(M_i) \le d$ for all $i \in [2^m]$;
2. If $M(x,y) = 1$ then $\exists i \in [2^m]$, $M_i(x,y) = 1$; and
3. If $M(x,y) = 0$ then $\forall i \in [2^m]$, $M_i(x,y) = 0$.

By definition, $\mathsf{ND}^{\mathrm{EQ}}(M) \le \mathsf{D}^{\mathrm{EQ}}(M)$. To prove a lower bound on $\mathsf{ND}^{\mathrm{EQ}}$, we require the *blocky cover number* defined in [18].

Definition 4.1 (Blocky Cover)**.** A matrix $B \in \{0,1\}^{N\times N}$ is called *blocky* if it is obtained from an identity matrix $I_{m,m}$ with $m \le N$ by duplicating rows or columns, permuting rows or columns, or adding all-0 rows or columns. Let $M \in \{0,1\}^{N\times N}$ be a boolean matrix. The *blocky cover number* $\mathrm{bc}(M)$ is the minimum number r such that there exist r blocky matrices $B_1, \dots, B_r \in \{0,1\}^{N\times N}$ with $M = \bigvee_{i=1}^{r} B_i$, where $\bigvee$ denotes entrywise OR.

Blocky covers are related to non-deterministic EQUALITY oracle cost by the following inequality from [18]. For all $A \in \{0,1\}^{N\times N}$,

$$\mathsf{ND}^{\mathrm{EQ}}(A) \le \log \mathrm{bc}(A) \le O(\mathsf{ND}^{\mathrm{EQ}}(A) \cdot \log\log N). \tag{4.1}$$

In Section 6, we improve the upper bound in this inequality:

Lemma 4.2. *For any $A \in \{0,1\}^{N\times N}$,*

$$\mathsf{ND}^{EQ}(A) \le \log \mathrm{bc}(A) \le \mathsf{ND}^{EQ}(A) + O(\log\log N).$$

We may now improve Theorem 1.4 to $\mathsf{ND}^{\mathrm{EQ}}(\textsc{RankOne}_n) = \Omega(n)$ with the following bound on blocky cover number.

Theorem 4.3. $\mathrm{bc}(\textsc{RankOne}_n) = 2^{\Omega(n)}$. *As a consequence,* $\mathsf{ND}^{EQ}(\textsc{RankOne}_n) = \Omega(n)$.

Proof. In this proof, write $M^{-1}(1)$ for the set of 1-valued entries in a boolean matrix M, and write $|M| = |M^{-1}(1)|$ for the number of 1-valued entries. We use standard notation $\mathrm{H}(\boldsymbol{Z})$ for the binary entropy of a random variable $\boldsymbol{Z}$, so $\mathrm{H}(\boldsymbol{Z}) := -\sum_{z\in\mathcal{Z}} \Pr[\boldsymbol{Z} = z] \log \Pr[\boldsymbol{Z} = z]$.

Recall from Equation (3.2) that $|\textsc{RankOne}_n| = 2^{n^2} \cdot 2^{2n}$. A rectangle $R = U \times V$ is *1-chromatic* if, for all $(u,v) \in U \times V$, $\textsc{RankOne}_n(u,v) = 1$. Let $\mathrm{bc}(\textsc{RankOne}_n) = K$, so $\textsc{RankOne}_n = \bigvee_{i\in[K]} B_i$, where the B_i are blocky matrices, which can be written as a disjoint union of 1-chromatic rectangles $B_i = \bigvee_{j\in[b_j]} R_{i,j}$ where $R_{i,j} = U_{i,j} \times V_{i,j}$ is a 1-chromatic rectangle in B_i.

Claim 4.4. *There exists a 1-chromatic rectangle $R = U \times V$ with $|U|, |V| \ge 2^{2n}/(2K)$.*

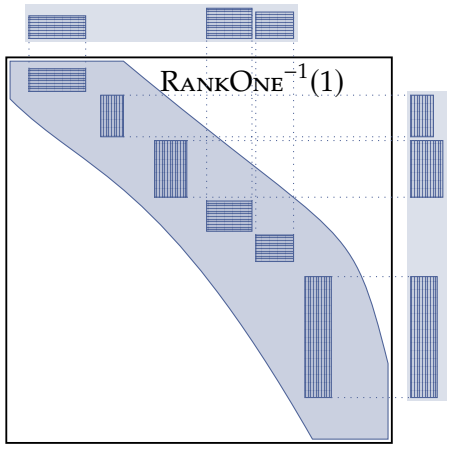


Figure 1: Illustration of Theorem 4.4. The rectangles represent the 1-entries of a blocky matrix B with $B^{-1}(1) \subseteq \textsc{RankOne}^{-1}(1)$. Short rectangles are filled with horizontal lines and narrow ones are filled with the vertical lines. We then can conclude that the total area of each type of the rectangles is small.

Proof of claim. For the sake of contradiction, assume each 1-chromatic rectangle $R = U \times V$ has $|U| < 2^{2n}/(2K)$, in which case we call the rectangle *short*, or $|V| < 2^{2n}/(2K)$, in which case we call it *narrow*. Then by definition of K, we obtain a contradiction as follows:

$$\begin{aligned}
2^{n^2} \cdot 2^{2n} = |\textsc{RankOne}_n| &\le \sum_{i=1}^{K} |B_i| = \sum_{i=1}^{K} \sum_{j=1}^{b_i} |U_{i,j}| \cdot |V_{i,j}| \\
&< \sum_{i=1}^{K} \left(\sum_{j \in [b_i], R_{i,j} \text{ short}} |V_{i,j}| \cdot 2^{2n}/(2K) + \sum_{j \in [b_i], R_{i,j} \text{ narrow}} |U_{i,j}| \cdot 2^{2n}/(2K) \right) \\
&\le \tfrac{1}{2} 2^{2n} \max_{i \in [K]} \left(\sum_{j \in [b_i]} |V_{i,j}| + \sum_{j \in [b_i]} |U_{i,j}| \right) \\
&\le \tfrac{1}{2} 2^{2n} \max_{i \in [K]} \left(2^{n^2} + 2^{n^2} \right) = 2^{2n} \cdot 2^{n^2}.
\end{aligned}$$

■

Suppose that $K < 2^{n/1000}$. Then Theorem 4.4 implies that there exists a 1-chromatic rectangle $R = U \times V$ with $|U|, |V| \ge 2^{n(2-1/100)}$. This contradicts the next claim:

Claim 4.5. *Let $R = U \times V$ be a 1-chromatic rectangle. Then* $\min(|U|, |V|) < 2^{\alpha n}$ *for* $\alpha = 2 - 10^{-2}$.

Proof of claim. Suppose for the sake of contradiction that $|U|, |V| \ge 2^{\alpha n}$. Let $u \in U$ and $v \in V$ be arbitrary, and let $\boldsymbol{A} \sim U$, $\boldsymbol{B} \sim V$ be uniformly random, so that $\boldsymbol{A}, \boldsymbol{B} \in \{0,1\}^{n \times n}$. Since R is 1-chromatic, $\boldsymbol{A} \oplus v$ and $\boldsymbol{B} \oplus u$ are always rank-1 matrices, so we may write $\boldsymbol{A} \oplus v$ as an outer product $\boldsymbol{\ell}^A \cdot (\boldsymbol{r}^A)^T$ where $\boldsymbol{\ell}^A, \boldsymbol{r}^A \in \{0,1\}^n$, and similarly $\boldsymbol{B} \oplus u := \boldsymbol{\ell}^B (\boldsymbol{r}^B)^T$. Then $\mathrm{H}(\boldsymbol{\ell}^A, \boldsymbol{r}^A), \mathrm{H}(\boldsymbol{\ell}^B, \boldsymbol{r}^B) \ge \alpha n$.

By the chain rule for entropy, $\sum_{i \text{ odd}} \mathrm{H}(\boldsymbol{\ell}_i^A, \boldsymbol{r}_i^A, \boldsymbol{\ell}_{i+1}^A, \boldsymbol{r}_{i+1}^A) \geq n(2 - 10^{-2})$, therefore for at least 2/3-fraction of odd $i \in [n]$, $\mathrm{H}(\boldsymbol{\ell}_i^A, \boldsymbol{r}_i^A, \boldsymbol{\ell}_{i+1}^A, \boldsymbol{r}_{i+1}^A) \geq 2 - 3 \cdot 10^{-2}$. Similarly, for at least 2/3-fraction of odd $i \in [n]$, $\mathrm{H}(\boldsymbol{\ell}_i^B, \boldsymbol{r}_i^B, \boldsymbol{\ell}_{i+1}^B, \boldsymbol{r}_{i+1}^B) \geq 2 - 3 \cdot 10^{-2}$. Then for 1/3-fraction of odd coordinates i, both inequalities are satisfied. Suppose without loss of generality that this is the case for $i = 1$.

Then $\mathrm{H}(\boldsymbol{\ell}_1^A, \boldsymbol{r}_1^A, \boldsymbol{\ell}_2^A, \boldsymbol{r}_2^A) \geq 2(2-10^{-2}) > \log 15$, hence $|\operatorname{supp}(\boldsymbol{\ell}_1^A, \boldsymbol{r}_1^A, \boldsymbol{\ell}_2^A, \boldsymbol{r}_2^A)| = 16$, and similarly $|\operatorname{supp}(\boldsymbol{\ell}_1^B, \boldsymbol{r}_1^B, \boldsymbol{\ell}_2^B, \boldsymbol{r}_2^B)| = 16$. Thus $(\boldsymbol{A} \oplus v)|_{[2]\times[2]}$ and $(u \oplus \boldsymbol{B})|_{[2]\times[2]}$ can be arbitrary rank-1 matrices, so in particular there exists $(a, b) \in \operatorname{supp}(\boldsymbol{A}) \times \operatorname{supp}(\boldsymbol{B})$ such that $(a \oplus b)|_{[2]\times[2]}$ is the identity matrix: take a and b such that $(a \oplus v)|_{[2]\times[2]}$ and $(u \oplus b)|_{[2]\times[2]}$ form the decomposition of $(v \oplus u)|_{[2]\times[2]} \oplus I_2$ as a sum of rank-1 matrices. Hence $\mathrm{rk}(a \oplus b) \geq 2$, a contradiction. ■

This concludes the proof of the theorem. ■

5 Consequences

We conclude the paper with some corollaries of our proofs, as mentioned in the introduction.

5.1 Constant-Cost Communication vs. k-Hamming Distance

We will prove Theorem 1.5, which shows that constant-cost randomized communication does not reduce to k-Hamming Distance.

Remark 5.1. We must clarify a subtlety in the definition of $\mathsf{D}^{Q}(P)$, the cost of a deterministic communication protocol with access to an oracle for problem Q. For the purpose of studying the class BPP_0, the natural definition of D^{Q} is as follows (see e. g.[13, 8, 7]). Q is a family of boolean matrices, i. e.a communication problem, containing matrices $Q \in \{0,1\}^{N\times N}$ for a variety of input sizes N. $\mathsf{D}^{Q}(P)$ is the minimum cost of a deterministic protocol computing $P \in \{0,1\}^{N\times N}$, where on input x, y, the two parties Alice and Bob in each round may construct inputs $a(x)$ and $b(y)$ of *arbitrary size*, and query the oracle on $Q(a(x), b(y))$, where $Q \in Q$ is any instance of problem Q. The difference between this definition and the standard definition of oracle protocols is that the query inputs $a(x), b(y)$ do not have bounded size. This is natural because for $Q \in \mathsf{BPP}_0$, the randomized communication cost is independent of input size.

Recent work [8] showed that there is no complete problem for BPP_0: there is no problem $Q \in \mathsf{BPP}_0$ such that $\mathsf{D}^{Q}(P) = O(1)$ for all problems $P \in \mathsf{BPP}_0$. The reason is that, for every $Q \in \mathsf{BPP}_0$, there exists a constant k such that $\mathsf{D}^{Q}(\mathrm{HD}_k^n) = \omega(1)$. This raised the question of whether the infinite hierarchy of k-Hamming Distance problems $\mathrm{HD}_1, \mathrm{HD}_2, \cdots$ is complete, meaning that for every problem $\mathcal{P} \in \mathsf{BPP}_0$ there exists a constant k such that $\mathsf{D}^{\mathrm{HD}_k}(P_N) = O(1)$. The question was answered in [7], whose main result was:

Theorem 5.2 ([7])**.** *There exists a communication problem $F_n \colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ such that $\mathsf{R}(F_n) = O(1)$, yet for every constant k, $\mathsf{D}^{HD_k}(F_n) = \omega(1)$.*

The $\omega(1)$ function is not given explicitly and is the result of a lengthy Ramsey-theoretic proof. We give a simpler proof (using a different function F) with a quantitative bound.

Proof of Theorem 1.5. We prove that, for every constant k, $\mathsf{D}^{\mathrm{HD}_k}(\textsc{RankOne}_n) = \Omega(n/\log n)$. Given a deterministic protocol computing $\textsc{RankOne}_n$ using HD_k queries, we may replace each query Q with a protocol computing Q using $\textsc{Equality}$ queries. Then

$$\mathsf{D}^{\mathrm{EQ}}(\textsc{RankOne}_n) \le \mathsf{D}^{\mathrm{HD}_k}(\textsc{RankOne}_n) \cdot \max_Q \mathsf{D}^{\mathrm{EQ}}(Q),$$

where the maximum is over all $2^{n^2} \times 2^{n^2}$ matrices Q which represent oracle queries to HD_k; formally, these matrices Q are the ones which are obtained by taking any submatrix of $\mathrm{HD}_k^{n'}$ for arbitrarily large n' (due to Theorem 5.1), and then duplicating rows or columns to ensure the matrix is the same size as $\textsc{RankOne}_n$. We now require a bound on $\mathsf{D}^{\mathrm{EQ}}(Q)$ for arbitrary $2^{n^2} \times 2^{n^2}$ submatrices of $\mathrm{HD}_k^{n'}$ where n' can be arbitrarily large. This was proved in [8]:

Theorem 5.3 ([8, Proposition 4.1])**.** *For any k and any $n, N \in \mathbb{N}$ satisfying $N \le 2^n$, let M be an $N \times N$ submatrix of $HD_k^n \in \{0,1\}^{2^n \times 2^n}$. Then $\mathsf{D}^{EQ}(M) \le O(k \log\log N)$.*

So, by Theorem 5.3,

$$\mathsf{D}^{\mathrm{EQ}}(\textsc{RankOne}_n) \le O\left(\mathsf{D}^{\mathrm{HD}_k}(\textsc{RankOne}_n) \cdot k \log\log(2^{n^2})\right).$$

By Theorem 1.4, we conclude that $\mathsf{D}^{\mathrm{HD}_k}(\textsc{RankOne}_n) = \Omega\left(\frac{n}{k \log n}\right)$. ∎

5.2 Parity Decision Trees and Exact vs. Approximate Spectral Norm

We state some consequences for parity decision trees and exact vs. approximate spectral norms. The Fourier coefficients of a function $f\colon \{0,1\}^n \to \mathbb{R}$ are defined on subsets $S \subseteq [n]$ by

$$\hat{f}(S) \coloneqq \mathbb{E}_{\boldsymbol{x} \sim \{0,1\}^n}[f(\boldsymbol{x})(-1)^{\sum_{i \in S} \boldsymbol{x}_i}].$$

The Fourier norm is $\|\hat{f}\|_1 \coloneqq \sum_{S \subseteq [n]} |\hat{f}(S)|$. For an XOR problem $F(x, y) = f(x \oplus y)$, it is equivalent to the γ_2-norm:

$$\gamma_2(F) = \|\hat{f}\|_1 \qquad \text{([10, Corollary 3.9])}$$

For $\epsilon \in (0,1)$, the approximate spectral norm is defined as

$$\|\widehat{f}\|_{1,\epsilon} \coloneqq \inf_g \|\widehat{g}\|_1$$

where the infimum is over functions $g\colon \{0,1\}^n \to \mathbb{R}$ which satisfy $\|f - g\|_\infty < \epsilon$.

We can now state the corollaries. The first is an exponential improvement over the separation given by [5, Lemma 3].

Corollary 5.4. *There exists a function $f\colon \{0,1\}^{n\times n} \to \{0,1\}$ with approximate spectral norm $\|\widehat{f}\|_{1,1/3} = O(1)$ but exact spectral norm $\|\widehat{f}\|_1 = 2^{\Omega(n)}$.*

We remark that for some constants ϵ and ℓ the bound $\|\widehat{f}\|_{1,\epsilon} \le \ell$ [20, Theorem 2.5] (known as quantitative Cohen idempotence theorem) implies that $\|\widehat{f}\|_1 = O(1)$, so this corollary (as well as [5, Lemma 3]) gives a barrier for improving the dependency between ℓ and ϵ in this result.

The second corollary answers [3, Question 8].

Corollary 5.5. *There exists a function $f\colon \{0,1\}^{n\times n} \to \{0,1\}$ with randomized parity decision tree size $O(1)$ and deterministic parity decision tree size $2^{\Omega(n)}$.*

The separating function $f\colon \{0,1\}^{n\times n} \to \{0,1\}$ in both cases is defined by $f(A) = 1$ iff $A \in \{0,1\}^{n\times n}$ has $\mathrm{rk}(A) \le 1$, so $\textsc{RankOne}_n(x,y) = f(x \oplus y)$.

Proof of Theorem 5.4. By [10, Proposition 4.3] we get that $\|\widehat{f}\|_{1,1/3} = O(1)$ since 1/3-error randomized communication cost of RankOne is $O(1)$ by Theorem 2.1. On the other hand, by [10, Corollary 3.9] combined with Theorem 3.2 we get $\|\widehat{f}\|_1 = 2^{\Omega(n)}$ as required. ∎

Proof of Theorem 5.5. The upper bound on randomized parity decision tree size of f was proved in Theorem 2.1. If f has a parity decision tree (PDT) of size s, then $f(x) = \sum_{i\in[s]} A_i(x)$ where A_i are characteristic functions of the affine spaces corresponding to 1-labeled leaves of the PDT. It is well known that $\|\widehat{A_i}\|_1 \le 1$. Then $\|\hat{f}\|_1 \le \sum_{i\in[s]} \|\widehat{A_i}\|_1 \le s$. By Theorem 3.2,

$$2^{\Omega(n)} \le \gamma_2(\textsc{RankOne}_n) = \|\hat{f}\|_1 \le s.$$ ∎

5.3 Non-Deterministic Lower Bounds

The paper [2] showed that $\mathsf{BPP} \not\subseteq \mathsf{P}^{\mathrm{EQ}}$ using the Integer Inner Product function, defined as $\mathrm{IIP}_3^n\colon [-2^n, 2^n]^3 \times [-2^n, 2^n]^3 \to \{0,1\}$, where $\mathrm{IIP}_3^n(x,y) = 1$ iff $\sum_{i\in[3]} x_i y_i = 0$. Later, [18, 3] improved this separation to $\mathsf{BPP} \not\subseteq \mathsf{NP}^{\mathrm{EQ}}$ using IIP_3 in the latter work (and the higher-dimensional IIP_6 in the prior work). [3] prove a lower bound of $\mathsf{ND}^{\mathrm{EQ}}(\mathrm{IIP}_3^n) = \Omega(n/\log n)$ using Equation (6.1) and asking whether the $\log n$ factor could be removed. With our improved Theorem 4.2 we can remove this log factor.

We need the notion of maxrect(·) from [18]. For a matrix $A \in \{0,1\}^{N\times N}$ let $\alpha(A)$ be the number of 1-entries in A and let $\beta(A)$ be the area of the largest 1-chromatic rectangle in A. Then

$$\mathrm{maxrect}(A) := \frac{\alpha(A)}{N\sqrt{\beta(A)}}.$$

The following two theorems, together with the fact that bc(·) does not increase when taking submatrices, imply $\mathrm{bc}(\mathrm{IIP}_3^n) = 2^{\Omega(n)}$:

Theorem 5.6 (Theorem 5 in [3])**.** *IIP_3^n has a submatrix A such that* $\mathrm{maxrect}(A) = 2^{\Omega(n)}$.

Theorem 5.7 (Theorem 29 in [18]). *For every $A \in \{0,1\}^{N\times N}$ we have* $\mathrm{bc}(A) \geq \Omega(\mathrm{maxrect}(A))$.

Then, by Theorem 4.2 (and the trivial bound $\mathsf{D}^{\mathrm{EQ}}(\mathrm{IIP}_3^n) = O(n)$):

Corollary 5.8. $\mathsf{ND}^{EQ}(IIP_3^n) = \Theta(n)$.

6 Proof of Theorem 4.2

Let us now prove Theorem 4.2. Let $A \in \{0,1\}^{N\times N}$. Our goal is to show that

$$\log \mathrm{bc}(A) \leq \mathsf{ND}^{\mathrm{EQ}}(A) + O(\log\log N).$$

To prove this, we will use the fractional blocky cover instead of the blocky cover:

Definition 6.1 (Fractional Blocky Cover). For any $A \in \{0,1\}^{N\times N}$, a *fractional blocky cover* of A is a choice of values $m \in \mathbb{N}$, $\lambda_1, \ldots, \lambda_m \geq 0$, and blocky matrices $B_1, \ldots, B_m$ such that

$$A(x,y) = 0 \implies \sum_{i=1}^{m} \lambda_i B_i(x,y) = 0 \qquad A(x,y) = 1 \implies \sum_{i=1}^{m} \lambda_i B_i(x,y) \geq 1.$$

We write $\mathrm{fbc}(A)$ for the minimum value of $\sum_i \lambda_i$ over all fractional blocky covers of A.

We require the following properties of the fractional blocky cover:

Proposition 6.2 (Properties of FBC). *Let $P, Q \in \{0,1\}^{N\times N}$ be any boolean matrices and let J be the all-1s matrix. Then*

1. *For any blocky matrix B, $\mathrm{fbc}(J - B) \leq 4$.*
2. $\mathrm{fbc}(P \wedge Q) \leq \mathrm{fbc}(P) \cdot \mathrm{fbc}(Q)$.
3. $\mathrm{fbc}(P \vee Q) \leq \mathrm{fbc}(P) + \mathrm{fbc}(Q)$.
4. $\mathrm{bc}(P) \leq O(\mathrm{fbc}(P) \cdot \log N)$.

We prove these properties below. First let us complete the proof of Theorem 4.2.

Proof of Theorem 4.2. Let $A \in \{0,1\}^{N\times N}$. Due to property (4) of Theorem 6.2, it suffices to show $\log \mathrm{fbc}(A) = O(\mathsf{ND}^{\mathrm{EQ}}(A))$. Let $d, m \in \mathbb{N}$ be such that $d + m = \mathsf{ND}^{\mathrm{EQ}}(A)$ and there exist 2^m deterministic EQUALITY-oracle protocols T_i of depth at most d such that

$$\forall x, y \in [N] : \qquad A(x,y) = \bigvee_{i=1}^{2^m} T_i(x,y).$$

By property (3) of Theorem 6.2, $\mathrm{fbc}(A) \leq \sum_{i=1}^{2^m} \mathrm{fbc}(M_i)$ where $M_i \in \{0,1\}^{N\times N}$ is the matrix computed by protocol T_i. It now suffices to show that $\mathrm{fbc}(M_i) \leq 5^d$ for every i, so that $\log \mathrm{fbc}(A) \leq \log(2^m 5^d) < 3 \cdot \mathsf{ND}^{\mathrm{EQ}}(A)$.

Fix any $T = T_i$, which is a decision tree with each inner node v associated with a blocky matrix B_v. Without loss of generality we may assume the depth is exactly d and that the tree is full. For each node v, let $M_v \in \{0,1\}^{N\times N}$ be the matrix computed by the subtree rooted at v, and write $\mathrm{depth}(v)$ for the depth of this subtree. We prove by induction that $\mathrm{fbc}(M_v) \le 5^{\mathrm{depth}(v)}$. If $\mathrm{depth}(v) = 1$, then M_v is either a blocky matrix B or its complement $J - B$, so by property (1) of Theorem 6.2, $\mathrm{fbc}(M_v) \le 4$. For depth $d' > 1$, let ℓ, r be the left and right child of v. Then

$$M_v = (B_v \wedge M_\ell) \vee ((J - B_v) \wedge M_r),$$

so by properties (1), (2), and (3) of Theorem 6.2,

$$\begin{aligned}\mathrm{fbc}(M_v) &\le \mathrm{fbc}(B_v)\mathrm{fbc}(M_\ell) + \mathrm{fbc}(J - B_v)\mathrm{fbc}(M_r) \le \mathrm{fbc}(M_\ell) + 4\mathrm{fbc}(M_r)\\ &\le 5^{d'-1} + 4 \cdot 5^{d'-1} = 5^{d'},\end{aligned}$$

with the last inequality by induction. This completes the proof of the lemma. ∎

Finally, we establish the properties of fractional blocky covers that we have used above.

Proof of Theorem 6.2.

Claim 6.3. *Let J be the all-1s matrix and let B be any blocky matrix. Then* $\mathrm{fbc}(J - B) \le 4$.

Proof. It suffices to prove the claim for the identity matrix $B = I_{N\times N}$, since duplicating rows and columns does not change the value of fbc. The claim follows from the fact that the EQUALITY communication problem has a constant-cost one-sided error randomized protocol. That is, define the following probability distribution over rectangles $R \subseteq [N] \times [N]$. We choose $\boldsymbol{R}$ by including each $x \in [N]$ in a set $\boldsymbol{X} \subseteq [N]$ independently with probability $1/2$, and then take $\boldsymbol{R} = \boldsymbol{X} \times ([N] \setminus \boldsymbol{X})$. If $x = y$, then $\Pr[(x,y) \in \boldsymbol{R}] = 0$. If $x \neq y$ then $\Pr[(x,y) \in \boldsymbol{R}] = 1/4$. For each rectangle R, set $\lambda_R := 4 \cdot \Pr[\boldsymbol{R} = R]$. It follows that

$$\mathrm{fbc}(J - I_{N\times N}) \le \sum_R \lambda_R = 4.$$ ∎

Claim 6.4. *Let $P, Q \in \{0,1\}^{N\times N}$. Then* $\mathrm{fbc}(P \wedge Q) \le \mathrm{fbc}(P) \cdot \mathrm{fbc}(Q)$.

Proof of claim. Let $\alpha_1, \dots, \alpha_p$ and $B_1, \dots, B_p$ be a fractional blocky cover of P, and let $\beta_1, \dots, \beta_q$ and $B'_1, \dots, B'_q$ be a fractional blocky cover of Q. For any $x, y \in [N]$, consider

$$\sum_{i,j} \alpha_i \beta_j (B_i \wedge B'_j)(x,y) = \left(\sum_i \alpha_i B_i(x,y)\right) \cdot \left(\sum_j \beta_j B'_j(x,y)\right) \tag{6.1}$$

Note that $B_i \wedge B'_j$ is itself a blocky matrix. If $P \wedge Q(x,y) = 0$ then $P(x,y) = 0$ or $Q(x,y) = 0$ so Equation (6.1) is 0. If $P \wedge Q(x,y) = 1$ then $P(x,y) = Q(x,y) = 1$ so Equation (6.1) is at least 1. So

$$\mathrm{fbc}(P \wedge Q) \le \sum_{i,j} \alpha_i \beta_j = \mathrm{fbc}(P) \cdot \mathrm{fbc}(Q).$$ ∎

Claim 6.5. *Let* $P, Q \in \{0,1\}^{N\times N}$. *Then* $\mathrm{fbc}(P \vee Q) \le \mathrm{fbc}(P) + \mathrm{fbc}(Q)$.

Proof of claim. Let $\alpha_1, \dots, \alpha_p$ and $B_1, \dots, B_p$ be a fractional blocky cover of P, and let $\beta_1, \dots, \beta_q$ and $B'_1, \dots, B'_q$ be a fractional blocky cover of Q. It is straightforward to check that the union of these fractional blocky covers is itself a fractional blocky cover for $P \vee Q$, so that $\mathrm{fbc}(P \vee Q) \le \sum_i \alpha_i + \sum_j \beta_j$. ∎

Claim 6.6. *Let* $P \in \{0,1\}^{N\times N}$. *Then* $\mathrm{bc}(P) \le O(\mathrm{fbc}(P) \cdot \log N)$.

Proof of claim. This is by standard randomized rounding. Let $\lambda_1, \dots, \lambda_m \ge 0$ and $B_1, \dots, B_m$ be a fractional blocky cover of P with $\sum_\ell \lambda_\ell = \mathrm{fbc}(P)$. Let $\boldsymbol{M}_1, \dots, \boldsymbol{M}_t$ be random blocky matrices chosen independently from the distribution $\Pr[\boldsymbol{M}_i = B_j] = \frac{\lambda_j}{\mathrm{fbc}(P)}$. Fix any $x, y \in [N]$ and note that

$$P(x,y) = 0 \implies \Pr[\exists i \,:\, \boldsymbol{M}_i(x,y) = 1] = 0$$

since $B_\ell(x,y) = 0$ for all $\ell \in [m]$. Now suppose $P(x,y) = 1$. Then $\sum_\ell \lambda_\ell B_\ell(x,y) \ge 1$, so, by independence of each $\boldsymbol{M}_i$,

$$\Pr[\forall i \,:\, \boldsymbol{M}_i(x,y) = 0] = \Pr[\boldsymbol{M}_1(x,y) = 0]^t = \left(1 - \frac{1}{\mathrm{fbc}(P)}\right)^t \le e^{-\frac{t}{\mathrm{fbc}(P)}}.$$

Setting $t = O(\mathrm{fbc}(P)\log N)$ and using the union bound over at most N^2 pairs $x, y \in [N]$ with $P(x,y) = 1$, we conclude that there exists a choice of $t = O(\mathrm{fbc}(P)\log N)$ blocky matrices which cover the 1-valued entries of P. ∎

This completes the proof of all of the properties from Theorem 6.2. ∎

Acknowledgments

Thanks to Kaave Hosseini for suggesting Theorem 5.4 and to Tsun-Ming Cheung for comments on the presentation of this article. Thanks to an anonymous reviewer for pointing out a simpler proof of Theorem 4.4.

The project is supported by Swiss State Secretariat for Education, Research, and Innovation (SERI) under contract number MB22.00026.

References

[1] MARK BRAVERMAN AND OMRI WEINSTEIN: A discrepancy lower bound for information complexity. *Algorithmica*, 76(3):846–864, 2016. [doi:10.1007/s00453-015-0093-8] 2

[2] ARKADEV CHATTOPADHYAY, SHACHAR LOVETT, AND MARC VINYALS: Equality alone does not simulate randomness. In *Proc. 34th Comput. Complexity Conf. (CCC'19)*, pp. 14:1–11. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2019. [doi:10.4230/LIPIcs.CCC.2019.14] 2, 3, 4, 12

[3] TSUN-MING CHEUNG, HAMED HATAMI, KAAVE HOSSEINI, ALEKSANDAR NIKOLOV, TONIANN PITASSI, AND MORGAN SHIRLEY: A lower bound on the trace norm of Boolean matrices and its applications. In *Proc. 16th Innovations in Theoret. Comp. Sci. Conf. (ITCS'25)*, pp. 37:1–15. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2025. [doi:10.4230/LIPIcs.ITCS.2025.37] 2, 3, 4, 6, 12

[4] TSUN-MING CHEUNG, HAMED HATAMI, KAAVE HOSSEINI, AND MORGAN SHIRLEY: Separation of the factorization norm and randomized communication complexity. *Comput. Complexity*, 34(2):17, 2025. Preliminary version in CCC'23. [doi:10.1007/S00037-025-00278-3] 2, 3, 4

[5] TSUN MING CHEUNG, HAMED HATAMI, ROSIE ZHAO, AND ITAI ZILBERSTEIN: Boolean functions with small approximate spectral norm. *Discrete Analysis*, 6:1–22, 2024. [doi:10.19086/da.122971, arXiv:2409.10634] 2, 11, 12

[6] LOUIS ESPERET, NATHANIEL HARMS, AND ANDREY KUPAVSKII: Sketching distances in monotone graph classes. In *Proc. 26th Internat. Conf. on Randomization and Computation (RANDOM'22)*, pp. 18:1–23. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2022. [doi:10.4230/LIPIcs.APPROX/RANDOM.2022.18] 2

[7] YUTING FANG, MIKA GÖÖS, NATHANIEL HARMS, AND POOYA HATAMI: Constant-cost communication is not reducible to k-Hamming distance. In *Proc. 57th STOC*, pp. 565–571. ACM Press, 2025. [doi:10.1145/3717823.3718129] 2, 3, 10

[8] YUTING FANG, LIANNA HAMBARDZUMYAN, NATHANIEL HARMS, AND POOYA HATAMI: No complete problem for constant-cost randomized communication. In *Proc. 56th STOC*, pp. 1287–1298. ACM Press, 2024. [doi:10.1145/3618260.3649716] 2, 10, 11

[9] MIKA GÖÖS, NATHANIEL HARMS, AND ARTUR RIAZANOV: Equality is far weaker than constant-cost communication. In *Proc. 29th Internat. Conf. on Randomization and Computation (RANDOM'25)*, pp. 58:1–14. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2025. [doi:10.4230/LIPIcs.APPROX/RANDOM.2025.58] 1

[10] LIANNA HAMBARDZUMYAN, HAMED HATAMI, AND POOYA HATAMI: Dimension-free bounds and structural results in communication complexity. *Israel J. Math.*, 253(2):555–616, 2023. [doi:10.1007/s11856-022-2365-8] 2, 3, 4, 6, 11, 12

[11] NATHANIEL HARMS: Universal communication, universal graphs, and graph labeling. In *Proc. 11th Innovations in Theoret. Comp. Sci. Conf. (ITCS'20)*, pp. 33:1–27. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2020. [doi:10.4230/LIPIcs.ITCS.2020.33] 2

[12] NATHANIEL HARMS AND ARTUR RIAZANOV: Better boosting of communication oracles, or not. In *Proc. 44th Found. Softw. Techn. Theoret. Comp. Sci. Conf. (FSTTCS'24)*, pp. 25:1–24. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2024. [doi:10.4230/LIPIcs.FSTTCS.2024.25] 2, 3

[13] NATHANIEL HARMS, SEBASTIAN WILD, AND VIKTOR ZAMARAEV: Randomized communication and implicit graph representations. *TheoretiCS*, 4(20):1–81, 2025. Preliminary version in STOC'22. [doi:10.46298/THEORETICS.25.20] 2, 3, 10

[14] NATHANIEL HARMS AND VIKTOR ZAMARAEV: Randomized communication and implicit representations for matrices and graphs of small sign-rank. In *Proc. 35th Ann. ACM–SIAM Symp. on Discrete Algorithms (SODA'24)*, pp. 1810–1833. SIAM, 2024. [doi:10.1137/1.9781611977912.72] 2

[15] HAMED HATAMI AND POOYA HATAMI: Guest column: Structure in communication complexity and constant-cost complexity classes. *SIGACT News*, 55(1):67–93, 2024. [doi:10.1145/3654780.3654788] 3

[16] EYAL KUSHILEVITZ AND NOAM NISAN: *Communication complexity*. Cambridge Univ. Press, 1996. [doi:10.1017/CBO9780511574948] 2

[17] NOAM NISAN: The communication complexity of threshold gates. In DEZSŐ MIKLÓS, VERA T. SÓS, AND TAMÁS SZŐNYI, editors, *Combinatorics, Paul Erdős is Eighty, Vol. I*, volume 1 of *Bolyai Society Mathematical Studies*, pp. 301–315. J. Bolyai Math. Society, 1993. Facsimile of the entire volume is accessible at Rényi Institute. A preliminary version of this paper is available at the author's website. 2

[18] TONIANN PITASSI, MORGAN SHIRLEY, AND ADI SHRAIBMAN: The strength of equality oracles in communication. In *Proc. 14th Innovations in Theoret. Comp. Sci. Conf. (ITCS'23)*, pp. 89:1–19. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2023. [doi:10.4230/LIPIcs.ITCS.2023.89] 2, 3, 4, 8, 12, 13

[19] ANUP RAO AND AMIR YEHUDAYOFF: *Communication Complexity and Applications*. Cambridge Univ. Press, 2020. [doi:10.1017/9781108671644] 2

[20] TOM SANDERS: Boolean functions with small spectral norm, revisited. *Math. Proc. Cambridge Phil. Soc.*, 167(2):335–344, 2019. [doi:10.1017/S030500411800035X] 12

[21] ALEXANDER SHERSTOV AND ANDREY STOROZHENKO: The communication complexity of approximating matrix rank. In *Proc. 65th FOCS*, pp. 433–462. IEEE Comp. Soc., 2024. [doi:10.1109/FOCS61266.2024.00035] 4

[22] SRIKANTH SRINIVASAN AND AMIR YEHUDAYOFF: The discrepancy of greater-than, 2023. [arXiv:2309.08703] 2

[23] ISTVÁN TOMON: Factorization norms and Zarankiewicz problems, 2025. [arXiv:2502.18429] 3

[24] EMANUELE VIOLA: The communication complexity of addition. *Combinatorica*, 35(6):703–747, 2015. [doi:10.1007/s00493-014-3078-3] 2

AUTHORS

Mika Göös
Professor
EPFL
Lausanne, Switzerland
mika.goos@epfl.ch

Nathaniel Harms
Faculty member
EPFL & University of British Columbia
Lausanne, Switzerland & Vancouver, Canada
nharms@cs.ubc.ca

Artur Riazanov
PhD student
EPFL
Lausanne, Switzerland
tunyash@gmail.com

ABOUT THE AUTHORS

MIKA GÖÖS is an assistant professor at EPFL in the Theory Group. Previously, he was a postdoc at Stanford Theory, the Institute for Advanced Study, and the ToC group at Harvard. He completed his Ph. D. at the University of Toronto under the watchful eye of Toniann Pitassi. He obtained his B. S. from Aalto University, and his M. S. from the University of Oxford. In his spare time, Mika enjoys rock climbing and maintains a viral YouTube climbing channel. However, he is forsaking his dream of climbing an 7C-grade outdoor boulder one day due to now having small children at home.

NATHANIEL HARMS is an assistant professor at UBC. Previously, he was a postdoc under the mighty shadow of Mika Göös at EPFL, and he was indoctrinated by Eric Blais at the University of Waterloo. Before that, he was a baby. He spends his spare time wishing he was as cool as Artur Riazanov.

ARTUR RIAZANOV is a PhD student at EPFL in the Theory Group under the supervision of Mika Göös. Before coming to EPFL he was a researcher at Technion under the supervision of Yuval Filmus. He completed his M. S.at St. Petersburg Academic University under the supervision of Dmitry Itsykson. In his spare time, Artur is watching old movies, climbing, or is dancing to techno.