Communication Complexity of Collision

Mika Göös
EPFL, Lausanne, Switzerland

Siddhartha Jain
EPFL, Lausanne, Switzerland

Abstract
The Collision problem is to decide whether a given list of numbers \( (x_1, \ldots, x_n) \in [n]^n \) is 1-to-1 or 2-to-1 when promised one of them is the case. We show an \( n \Omega(1) \) randomised communication lower bound for the natural two-party version of Collision where Alice holds the first half of the bits of each \( x_i \) and Bob holds the second half. As an application, we also show a similar lower bound for a weak bit-pigeonhole search problem, which answers a question of Itsykson and Riazanov (CCC 2021).

2012 ACM Subject Classification Theory of computation → Communication complexity

Keywords and phrases Collision, Communication complexity, Lifting

Digital Object Identifier 10.4230/LIPIcs.APPROX/RANDOM.2022.19

Category RANDOM


Acknowledgements We thank anonymous RANDOM reviewers for their helpful comments.

1 Introduction

Collision problem

The Collision problem \( \text{Col}_N : [N]^N \to \{0, 1, *\} \) is the following partial (promise) function. The input is a list of numbers \( z = (z_1, \ldots, z_N) \in [N]^N \) where \( N \) is even. The goal is to distinguish between the following two cases, when promised that \( z \) satisfies one of them.

- \( \text{Col}_N(z) = 0 \) if \( z \) is 1-to-1, that is, every number in the list \( z \) appears in the list once.
- \( \text{Col}_N(z) = 1 \) if \( z \) is 2-to-1, that is, every number in the list \( z \) appears in the list twice.

The Collision problem has been studied exhaustively in quantum query complexity [10, 1, 5, 14, 20, 6, 2, 3, 12]. It was initially introduced to model the task of breaking collision resistant hash functions, a central problem in cryptanalysis. A robust variant of Collision is complete for NISZK [8], and consequently it has been featured in black-box oracle separations [21, 9]. The problem has also been used in reductions to show hardness of other problems such as set-equality [23] and various problems in property testing [11]. Upper bounds for Collision has been used to design quantum algorithms for triangle finding [22] and approximate counting [4].

In this paper, we consider a natural bipartite communication version of this problem, where we split the binary encoding of each number between two parties, Alice and Bob. Specifically, for \( N = 2^n \) where \( n \) is even, we will define a bipartite function

\[
\text{BiCol}_N : (\{0, 1\}^{n/2})^N \times (\{0, 1\}^{n/2})^N \to \{0, 1, *\}.
\]

Here Alice gets as input a list of half-numbers \( x = (x_1, \ldots, x_N) \in (\{0, 1\}^{n/2})^N \), Bob gets a list of half-numbers \( y = (y_1, \ldots, y_N) \in (\{0, 1\}^{n/2})^N \), and we view their concatenation \( z := x \cdot y \), defined by \( z_i := x_i y_i \), as an input to \( \text{Col}_N \). Their goal is to compute \( \text{BiCol}_N(x, y) := \text{Col}_N(x \cdot y) \).
Upper bounds

We first observe that $\text{BiCol}_N$ admits a deterministic protocol that communicates at most $O(\sqrt{N \log N})$ bits. Indeed, if $x \cdot y$ is 1–1, then since Alice’s half-numbers are $n/2$ bits long, there are $\sqrt{N}$ distinct half-numbers, each appearing $\sqrt{N}$ many times in $x$. We may assume this is true also if $x \cdot y$ is 2–1 (as otherwise it is easy to tell that we are in case 2–1). Consider the set of indices $I := \{i \in [N] : x_i = 0^{n/2}\}$, $|I| = \sqrt{N}$. Then $x \cdot y$ restricted to indices $I$ is 1–1 (resp. 2–1) if the original unrestricted input is 1–1 (resp. 2–1). Hence Alice can send the indices $I$ to Bob, who can determine the value of the function.

If we are allowed randomness, we can do slightly better: there is a randomised protocol of cost $O(N^{1/4} \log N)$. In this protocol, Alice samples a subset $I' \subseteq I$ of size $|I'| = \Theta(N^{1/4})$ uniformly at random and sends it to Bob, who checks for a collision in his part of the input. If the original input was 2–1, then by the birthday paradox, Bob will observe a collision with high probability.

Lower bound

As our main result, we prove a small polynomial lower bound for $\text{BiCol}_N$, which shows that the above randomised protocol cannot be improved too dramatically.

> Theorem 1. $\text{BiCol}_N$ has randomised (and even quantum) communication complexity $\Omega(N^{1/12})$.

We conjecture that the $O(N^{1/4} \log N)$-bit protocol for $\text{BiCol}_N$ is essentially optimal (up to logarithmic factors) for randomised protocols. It is an interesting open problem to close this gap.

1.1 Application

Bit-pigeonhole principle

We also show a lower bound for a search problem associated with the pigeonhole principle. We define $\text{PHP}_N^M$ where $M > N$ as the following search problem: On input $z = (z_1, \ldots, z_M) \in [N]^M$ the goal is to output a collision, that is, a pair of distinct indices $i, j \in [M]$ such that $z_i = z_j$. We note that $\text{PHP}_N^M$ is a total search problem (not a promise problem); it always has a solution since we require $M > N$. As before, we can turn $\text{PHP}_N^M$ naturally into a bipartite communication search problem $\text{BiPHP}_N^M$ where $N = 2^n$ so that

- Alice holds $x = (x_1, \ldots, x_M) \in (\{0, 1\}^{n/2})^M$;
- Bob holds $y = (y_1, \ldots, y_M) \in (\{0, 1\}^{n/2})^M$; and
- the goal is find a collision, that is, distinct $i, j \in [M]$ such that $x_i y_i = x_j y_j$.

Lower bounds

Itsykson and Riazanov [17] proved that $\text{BiPHP}_N^{N+1}$ requires $\Omega(\sqrt{N})$ bits of randomised communication. Their proof was via a randomised reduction from set-disjoiyness. A corollary of their result is that any proof system that can be efficiently simulated by randomised protocols (most notably, tree-like Res$^\oplus$ [18]) requires exponential size to refute bit-pigeonhole formulas featuring $N + 1$ pigeons and $N$ holes. They asked whether a similar communication lower bound could be proved for the weak pigeonhole principle with $M = 2N$ pigeons and $N$ holes. We answer their question in the affirmative in the following theorem.
Theorem 2. BiPHP$_N^{2N}$ has randomised (and even quantum) communication complexity \(\Omega(N^{1/12})\).

Previously, Hrubeš and Pudlák [15] showed a small polynomial lower bound for BiPHP$_M^N$ for every \(M > N\) against deterministic (and even dag-like) protocols. By contrast, Theorem 2 is the first randomised lower bound in the \(M = 2N\) regime.

1.2 Techniques

Our proof of Theorem 1 proceeds as follows. A popular method to prove communication lower bounds is to start with a partial boolean function \(f : \{0,1\}^n \to \{0,1,\ast\}\) that is hard to compute for decision trees and then apply a lifting theorem and then apply a lifting theorem (we use one due to Sherstov [26]) to conclude that the function \(f \circ g\) obtained by composing \(f\) with a small gadget \(g : \Sigma \times \Sigma \to \{0,1\}\) is hard for communication protocols. Here \(f \circ g : \Sigma^n \times \Sigma^n \to \{0,1,\ast\}\) is the communication problem where Alice holds \(x \in \Sigma^n\), Bob holds \(y \in \Sigma^n\), and their goal is to output

\[(f \circ g)(x, y) \coloneqq f(g(x_1, y_1), \ldots, g(x_n, y_n)).\]

A straightforward application of lifting often produces communication problems that are “artificial” since they are of the composed form. In particular, at first blush, it seems that the BiCol$_N$ problem cannot be written in the form \(f \circ g\) for any \(f\) and any \(g\) for which a lifting theorem holds. To address this issue, our main technical innovation is to show how the composed function Col$_N \circ g$, where \(g\) is a sufficiently “regular” gadget, can indeed be reduced to the natural problem BiCol$_{N'}$. In this reduction, the input length will blow up polynomially, \(N' = N^{\Theta(1)}\), which is the main reason why we only get a small polynomial lower bound. Our new reduction generalises a previous reduction from [17, §6], which was tailored for the 2-bit Xor gadget.

To prove Theorem 2 we give a randomised decision-to-search reduction from BiCol$_N$ to BiPHP$_N^{2N}$. That is, we show that if there is an efficient randomised protocol for solving the total search problem BiPHP$_N^{2N}$, then there is an efficient randomised protocol for solving the promise problem BiCol$_N$. Given this reduction, Theorem 2 then follows from Theorem 1. Similar style of randomised reductions have been considered in prior works [25, 16, 13, 17], although they have always reduced from set-disjointness.

2 Redductions and regular functions

We assume some familiarity with communication complexity; see, e.g., the textbooks [19, 24]. In particular, it is often useful to view a bipartite function \(f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}\) as a \(2^n\)-by-\(2^n\) boolean matrix. We now give several definitions for the purposes of the proof of our main result.

Definition 3 (Rectangular reduction). For bipartite functions \(f, g\) with domains \(\{0,1\}^n \times \{0,1\}^n\) and \(\{0,1\}^m \times \{0,1\}^m\), we write \(f \leq g\) if there is a rectangular reduction from \(f\) to \(g\), that is, there exist \(a : \{0,1\}^n \to \{0,1\}^m\) and \(b : \{0,1\}^n \to \{0,1\}^m\) such that \(f(x, y) = g(a(x), b(y))\) for all \(x, y\).

Next, using basic language from group theory, we define a new class of highly symmetric boolean functions that we call regular. (We borrow the term regular from group theory where group actions satisfying the property in Definition 4 below are called regular.)
Let $\Pi_n$ denote the symmetric group on $[n]$, that is, the set of all permutations $[n] \rightarrow [n]$. Let $S \subseteq \Pi_n \times \Pi_n$ be any group. We let $S$ act on the set $[n] \times [n]$ by permuting the rows and columns, that is, an element $s = (s^A, s^B) \in S$ acts on $(x, y) \in [n] \times [n]$ by $s \cdot (x, y) := (s^A(x), s^B(y))$. For $(x, y) \in [n] \times [n]$, we define its orbit by $S \cdot (x, y) := \{ s \cdot (x, y) : s \in S \}$.

\textbf{Definition 4 (Regular function).} A bipartite function $f : \{0, 1\}^k \times \{0, 1\}^k \rightarrow \{0, 1\}$ is regular if there is a group $S \subseteq \Pi_{2k} \times \Pi_{2k}$ acting on the domain of $f$ such that the orbit of any $(x, y) \in f^{-1}(b)$, where $b \in \{0, 1\}$, equals $f^{-1}(b)$, and, moreover, for every pair of inputs $(x_1, y_1), (x_2, y_2) \in f^{-1}(b)$ there is a unique $s \in S$ such that $s \cdot (x_1, y_1) = s \cdot (x_2, y_2)$.

It follows from the definition that $|S| = |f^{-1}(b)| = 2^{2k-1}$ for both $b \in \{0, 1\}$. A simple example of a regular function is the 2-bit XOR function together with the 2-element group consisting of the identity map and the map $(x, y) \mapsto (-x, -y)$. However, the XOR function does not satisfy a fully general lifting theorem. This is why we consider the following more complicated gadget, called a \textit{versatile} gadget, which has been shown to satisfy various lifting theorems [26, 13, 7].

\textbf{Definition 5.} $\text{Ver} : \mathbb{Z}_4 \times \mathbb{Z}_4 \rightarrow \{0, 1\}$ is defined by $\text{Ver}(x, y) := 1$ if $x + y \pmod{4} \in \{2, 3\}$.

\textbf{Lemma 6.} $\text{Ver}$ is regular.

\textbf{Proof.} Consider the group $S \subseteq \Pi_4 \times \Pi_4$ generated by the elements $(x, y) \mapsto (x + 1, y - 1)$ and $(x, y) \mapsto (1 - x, -y)$ where we use modulo 4 arithmetic. By explicit computations, we see that (here we list each element as a function of $(x, y)$)

$$S = \{(x, y), (x + 1, y - 1), (x + 2, y - 2), (x + 3, y - 3), (1 - x, -y), (2 - x, 3 - y), (3 - x, 2 - y), (-x, -y)\}.$$ 

It is straightforward to check that $S$ gives rise to orbits $\text{Ver}^{-1}(0)$ and $\text{Ver}^{-1}(1)$; see Figure 1. Moreover, since $|S| = 8 = |\text{Ver}^{-1}(b)|$ for $b \in \{0, 1\}$, the uniqueness property holds, too. \hfill $\blacksquare$

Previously, [13] showed that $\text{Ver}$ is random self-reducible, that is, it admits a randomised reduction that maps any fixed input $(x, y) \in \text{Ver}^{-1}(b)$ into a uniform random input in $\text{Ver}^{-1}(b)$. It is easy to see that if a function is regular, then it is also random self-reducible (the random self-reduction is to apply a random symmetry from $S$). The converse, however, is unclear to us: If $f$ is random self-reducible and balanced (meaning $|f^{-1}(0)| = |f^{-1}(1)|$), is it necessarily regular?

\section{Lower bound for bipartite collision}

In this section we prove Theorem 1. We start with a standard application of a lifting theorem to establish a lower bound for the (somewhat artificial) composed function $\text{Col}_N \circ \text{Ver}$. Here we think of $\text{Col}_N$ as a boolean function $\{0, 1\}^N \rightarrow \{0, 1\}$ where $N = 2^n$.

\textbf{Lemma 7.} $\text{Col}_N \circ \text{Ver}$ has randomised (and even quantum) communication complexity $\Omega(N^{1/3})$.

\textbf{Proof.} Aaronson and Shi [5] (building on [1]) showed that $\deg_{1/3}(\text{Col}_N) \geq \Omega(N^{1/3})$ where $\deg_{1/3}(f)$ for a partial boolean function $f$ is the least degree of a multivariate polynomial $p(x)$ such that $p(x) = f(x) \pm 1/3$ for all $x$ such that $f(x) \in \{0, 1\}$ and $|p(x)| \leq 4/3$ for all $x$ with $f(x) = \ast$. Sherstov [26, §12] proved that for any partial boolean function $f$, we have that the randomised (and even quantum) communication complexity of $f \circ \text{Ver}$ is at least $\Omega(\deg_{1/3}(f))$. Combining these two results proves the lemma. \hfill $\blacksquare$
These bipartite inputs encode, via the gadgets, the input $a$ where the ordering and multiplicity of elements.

Let $S$ be the symmetry group relative to which $\text{Ver}$ is a regular gadget and $N'$ is polynomially larger than $N$. Choosing $g := \text{Ver}$ in the following theorem and combining it with Lemma 7 completes the proof of Theorem 1. Note that the input length becomes $N' := N^4$ so that we obtain the lower bound $\Omega(N^{1/3}) = \Omega(N^{n/12})$, as claimed.

**Theorem 8.** Let $g : \{0, 1\}^k \times \{0, 1\}^k \to \{0, 1\}$ be a regular gadget. For every $N = 2^n$, 

$$\text{Col}_N \circ g \leq \text{BiCol}_{N^2}.$$

**Proof.** Consider the bipartite function $\text{Col}_N \circ g$. Alice’s input is an $N$-tuple $(a^{(1)}, \ldots, a^{(N)})$ where $a^{(j)} \in \{0, 1\}^k$ for each $j \in [N]$. Bob’s input $(b^{(1)}, \ldots, b^{(N)})$ has a similar form. These bipartite inputs encode, via the gadgets, the input $(z^{(1)}, \ldots, z^{(N)})$ to $\text{Col}_N$ such that 

$$z^{(j)} := g^n(a^{(j)}, b^{(j)}) := (g(a_1^{(j)}, b_1^{(j)}), \ldots, g(a_n^{(j)}, b_n^{(j)})) \in \{0, 1\}^n$$

where $a_i^{(j)}, b_i^{(j)} \in \{0, 1\}^k$.

Let $S \subseteq \Pi_{2k} \times \Pi_{2k}$ be the symmetry group relative to which $g$ is regular. Recall that $|S| = 2^{2k-1}$ and each $s \in S$ has the form $s = (s^A, s^B)$ with $s^A, s^B \in \Pi_{2k}$. We fix an arbitrary ordering of the elements of $S$ and write $S(i)$ for the $i$-th element in this ordering. Thus $S = \{S(1), \ldots, S(2^{2k-1})\}$.

We first describe how the reduction expands each individual input $(a, b) := (a^{(j)}, b^{(j)})$ to $g^n$ into an ordered list of inputs to $g^n$. In more detail, the reduction

- takes an input $(a, b) = (a_1, \ldots, a_n, b_1, \ldots, b_n) \in \{0, 1\}^k 2^n$ to $g^n$, and
- returns $\text{Unfold}(a, b) \in \{0, 1\}^{2kn}$, an ordered list of $2^{2k-1}$ many inputs to $g^n$.

For any $n$-tuple of indices $I = (i_1, \ldots, i_n) \in [|S|]^n$, we define the $I$-th pair in $\text{Unfold}(a, b)$ by

$$\text{Unfold}(a, b)_I := (s^A_i(a_1) s^A_i(a_2) \ldots s^A_i(a_n), \quad s^B_i(b_1) s^B_i(b_2) \ldots s^B_i(b_n))$$

where $s_j := S(i_j)$. Alice’s half

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**Figure 1** (a) The bipartite function $\text{Ver} : \mathbb{Z}_4 \times \mathbb{Z}_4 \to \{0, 1\}$. (b) The group relative to which $\text{Ver}$ is regular is generated by two elements whose actions on $\text{Ver}^{-1}(1)$ are illustrated here. The first generator is $(x, y) \mapsto (x + 1, y - 1)$ (black arrows) and the second is $(x, y) \mapsto (1 - x, -y)$ (orange arrows).

Besides each pair in the list $\text{Unfold}(a, b)$ being an input to $g^n$, we will also soon interpret them as pairs of half-numbers that are part of the input to $\text{BiCol}_{N^2}$. Below, we write $\text{SetUnfold}(a, b) \subseteq \{0, 1\}^{2kn}$ for the set of elements in the list $\text{Unfold}(a, b)$, that is, ignoring the ordering and multiplicity of elements.
Claim 9. We have the following properties.
(i) \( \text{UNFOLD}(a, b) = (g^n)^{-1}(z) = g^{-1}(z_1) \times \cdots \times g^{-1}(z_n) \) where \( z_i := g(a_i, b_i) \).
(ii) All pairs in UNFOLD(a, b) are distinct.
(iii) Suppose \( g^n(a, b) \neq g^n(a', b') \). Then \( \text{UNFOLD}(a, b) \cap \text{UNFOLD}(a', b') = \emptyset \).
(iv) Suppose \( g^n(a, b) = g^n(a', b') \). Then \( \text{UNFOLD}(a, b) = \text{UNFOLD}(a', b') \).

Proof. Item (i): Up to reordering of bits, the set equals \( (S \cdot (a_1, b_1)) \times (S \cdot (a_2, b_2)) \times \cdots \times (S \cdot (a_n, b_n)) \). By regularity, the orbit \( S \cdot (a_i, b_i) \) is equal to \( g^{-1}(z_i) \) for any \( i \). Item (ii): The uniqueness property of the regular group action ensures that we do not get any repeated elements. Item (iii): If \( z := g^n(a, b) \neq g^n(a', b') =: z' \) then there is some \( i \) such that \( z_i \neq z'_i \). The \( i \)-th component of every pair in UNFOLD(a, b) lies in \( g^{-1}(z_i) \) while the \( i \)-th component of every pair in UNFOLD(a, b) lies in \( g^{-1}(z'_i) \). The claim follows since these preimage sets are disjoint. Item (iv): If \( g^n(a, b) = g^n(a', b') \), then i shows UNFOLD produces the same set for both \((a, b)\) and \((a', b')\).

Our final reduction from \( \text{COL}_N \circ g \) maps Alice’s \((a^{(1)}, \ldots, a^{(N)})\) and Bob’s \((b^{(1)}, \ldots, b^{(N)})\) (which together encode the input \( z = (z^{(1)}, \ldots, z^{(N)}) \) to \( \text{COL}_N \)) to an input to \( \text{BiCOL}_{2N} \), given by

\[
\text{UNFOLD}(a^{(1)}, b^{(1)}), \ldots, \text{UNFOLD}(a^{(N)}, b^{(N)}).
\]

Note that the reduction is rectangular: Alice can compute her part of the input, and Bob has.

It remains to check that the reduction treats 1–1 and 2–1 inputs correctly. If the input \( z \to \text{COL}_N \) is 1–1, then the reduction produces a 1–1 input by ii and iii. If the input \( z \to \text{COL}_N \) is 2–1 then for every index \( i \) there is exactly one more index \( j \) such that \( z^{(i)} := g^n(a^{(i)}, b^{(i)}) = g^n(a^{(j)}, b^{(j)}) =: z^{(j)} \). Hence, by iv the lists \( \text{UNFOLD}(a^{(i)}, b^{(i)}) \) and \( \text{UNFOLD}(a^{(j)}, b^{(j)}) \) have every element colliding with each other. This produces a 2–1 input.

4 Lower bound for bipartite pigeonhole

In this section we prove Theorem 2. We do it by describing a reduction from the decision problem \( \text{BiCOL}_N \) to the search problem \( \text{BiPHP}^N_N \).

Theorem 10. If there is a randomised protocol for \( \text{BiPHP}^N_N \) of communication cost \( d \), then there is a randomised protocol for \( \text{BiCOL}_N \) of cost \( O(d) \).

Proof. The proof idea is to start with an input to \( \text{BiCOL}_N \) and then append it with more numbers to construct an input to \( \text{BiPHP}^N_N \). Adding more numbers will create some new collisions in the input list, but our reduction will remember which collisions where “planted” during the reduction. We then randomly shuffle the input list so as to make the planted collisions indistinguishable from collisions (if any) coming from the original input to \( \text{BiCOL}_N \). We now explain this in more detail.

Let \( (x, y) \) be an input to \( \text{BiCOL}_N \). That is, Alice holds \( x = (x_1, \ldots, x_N) \in (\{0, 1\}^{n/2})^N \) and Bob holds \( y = (y_1, \ldots, y_N) \in (\{0, 1\}^{n/2})^N \). In the reduction, we first append Alice’s input by the planted half-numbers \( (a_1, \ldots, a_N) \in (\{0, 1\}^{n/2})^N \) and Bob’s input by the planted half-numbers \( (b_1, \ldots, b_N) \in (\{0, 1\}^{n/2})^N \) where the concatenated strings \( a_ib_i \), \( i \in [N] \), range lexicographically over all binary numbers in \( \{0, 1\}^n \).

Next, Alice and Bob use public randomness to sample a permutation \( \pi \colon [2N] \to [2N] \) uniformly at random, which they then use to permute their lists of length 2N. While doing so, they remember which positions in the permuted list occupy planted numbers (namely,
those in positions $\pi(\{N + 1, \ldots, 2N\})$. Call the resulting list $(x', y')$. We now let Alice and Bob run the hypothesised protocol $\mathcal{P}$ for BiPHP$_N^N$ on input $(x', y')$ to find some collision $x'_i y'_i = x'_j y'_j$ where $i \neq j$. (We assume for simplicity that $\mathcal{P}$ finds a collision with probability 1. The following analysis can be adapted even when $\mathcal{P}$ errs with bounded probability.)

We have two cases depending on whether $(x, y)$ was 1–1 or 2–1 (see Figure 2):

- If $(x, y)$ was 1–1 then $(x', y')$ is 2–1. Moreover, each collision in $(x', y')$ involves a planted number. In particular, the collision $\{i, j\}$ found by the protocol always features at least one planted number.

- If $(x, y)$ was 2–1 then $(x', y')$ is an input where $N/2$ many numbers appear thrice, and $N/2$ numbers appear once. We claim that the collision $\{i, j\}$ found by $\mathcal{P}$ will not feature a planted number with probability at least $1/3$ (over the random choice of $\pi$). Indeed, let $k \notin \{i, j\}$ be the third position such that $x'_i y'_i = x'_j y'_j = x'_k y'_k$. Then conditioned on $\pi$ having produced the input $(x', y')$, each position in $\{i, j, k\}$ is equally likely to occupy a planted number. Thus, with probability 1/3, the planted number lies in position $k$ and not in $\{i, j\}$.

Our protocol for BiCol$_N$ guesses that $(x, y)$ is 2–1 if the collision $\{i, j\}$ returned by $\mathcal{P}$ does not involve a planted number. We can further reduce the error probability down to $(2/3)^t$ by repeating the randomised reduction and $\mathcal{P}$ some $t = O(1)$ times and seeing if any one of these runs finds a collision without a planted number. \hfill $\blacksquare$
19:8 Communication Complexity of Collision

References


3 Scott Aaronson. The collision lower bound after 12 years, 2013. QStart talk. URL: https://scottaaronson.blog/?p=1458.


