Electronic Colloquium on Computational Complexity, Report No. 22 (2014)

# Fooling Pairs in Randomized Communication Complexity

Shay Moran* Makrand Sinha† Amir Yehudayoff‡

**Abstract**

Fooling pairs are one of the standard methods for proving lower bounds for deterministic two-player communication complexity. We study fooling pairs in the context of randomized communication complexity. We show that every fooling pair induces far away distributions on transcripts of private-coin protocols. We then conclude that the private-coin randomized $\varepsilon$-error communication complexity of a function $f$ with a fooling set $\mathcal{S}$ is at least order $\log \frac{\log |\mathcal{S}|}{\varepsilon}$. This is tight, for example, for the equality and greater-than functions.

## 1 Introduction

Communication complexity provides a mathematical framework for studying communication between two or more parties. It was introduced by Yao [Yao79] and has found numerous applications since. We focus on the two-player case, and provide a brief introduction to it. For more details see the textbook by Kushilevitz and Nisan [KN97].

In this model, there are two players called Alice and Bob. The players wish to compute a function $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$, where Alice knows $x \in \mathcal{X}$ and Bob knows $y \in \mathcal{Y}$. To achieve this goal, they need to communicate. The *communication complexity* of $f$ measures the minimum number of bits the players must exchange in order to compute $f$. The communication is done according to a pre-determined protocol. Protocol may be deterministic or use private/public randomness. See Section 1.1 for definitions.

*Max Planck Institute for Informatics, Saarbrücken, Germany, and Technion-IIT, Israel. smoran@mpi-inf.mpg.de.

†Department of Computer Science and Engineering, University of Washington, Seattle. makrand@cs.washington.edu. Partially supported by BSF.

‡Department of Mathematics, Technion-IIT, Israel. amir.yehudayoff@gmail.com. Horev fellow – supported by the Taub foundation. Supported by ISF and BSF.



ISSN 1433-8092

A fundamental problem in this context is proving lower bounds on the communication complexity of a given function $f$. Lower bounds methods for deterministic communication complexity are based on the fact that any protocol for $f$ defines a partition of $\mathcal{X} \times \mathcal{Y}$ to $f$-monochromatic rectangles. Thus, a lower bound on the size of a minimal partition of this kind readily translates to a lower bound on the communication complexity of $f$. Three basic bounds of this type are based on rectangle size, fooling sets, and matrix rank (see [KN97]). Both matrix rank and rectangle size lower bounds have natural and well-known analogues in the randomized setting: The approximate rank lower bound [LS09, Kra96] and the discrepancy lower bound [KN97]. In this note we show that fooling sets also have natural counterparts in the randomized setting. A weaker variant of the structure we present is implicit in [BYJKS02], where it is used as part of a lower bound proof for the randomized communication complexity of the disjointness function.

## 1.1 Communication complexity

A *private-coin communication protocol* for computing a function $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ is a binary tree with the following generic structure. Each node in the protocol is owned either by Alice or by Bob. For every $x \in \mathcal{X}$, each internal node $v$ owned by Alice is associated with a distribution $P_{v,x}$ on the children of $v$. Similarly, for every $y \in \mathcal{Y}$, each internal node $v$ owned by Bob is associated with a distribution $P_{v,y}$ on the children of $v$. The leaves of the protocol are labeled by $\mathcal{Z}$.

On input $x, y$, a protocol $\pi$ is executed as follows.

1. Set $v$ to be the root node of the protocol-tree defined above.

2. If $v$ is a leaf, then the protocol outputs the label of the leaf. Otherwise, if Alice owns the node $v$, she samples a child according to the distribution $P_{v,x}$ and sends a bit to Bob indicating which child was sampled. The case when Bob owns the node is analogous.

3. Set $v$ to be the sampled node and return to the previous step.

A protocol is *deterministic* if for every internal node $v$, the distribution $P_{v,x}$ or $P_{v,y}$ has support of size one. A *public-coin* protocol is a distribution over private-coin protocols defined as follows: Alice and Bob first sample a shared random $r$ to choose a protocol $\pi_r$, and they execute a private protocol $\pi_r$ as above.

For an input $(x, y)$, we denote by $\pi(x, y)$ the sequence of messages exchanged between the parties. We call $\pi(x, y)$ the *transcript* of the protocol $\pi$ on input $(x, y)$. Another way to think of $\pi(x, y)$ is as a leaf in the protocol-tree. We denote by $L(\pi(x, y))$ the label of the leaf $\pi(x,y)$ in the tree. The *communication complexity* of a protocol $\pi$, denoted by $\mathsf{CC}(\pi)$ is the depth of the protocol-tree of $\pi$. For a private-coin protocol $\pi$, we denote by $\Pi(x,y)$ the distribution of the transcript of $\pi(x,y)$.

For a function $f$, the *deterministic* communication complexity of $f$, denoted by $D(f)$, is the minimum of $\mathsf{CC}(\pi)$ over all deterministic protocols $\pi$ such that $L(\pi(x,y)) = f(x,y)$ for every $x, y$. For $\varepsilon > 0$, we denote by $R_\varepsilon(f)$ the minimum of $\mathsf{CC}(\pi)$ over all public-coin protocols $\pi$ such that for every $(x,y)$, it holds that $\mathbb{P}[L(\pi(x,y)) \neq f(x,y)] \leq \varepsilon$ where the probability is taken over all coin flips in the protocol $\pi$. We call $R_\varepsilon(f)$ the *$\varepsilon$-error public-coin randomized* communication complexity of $f$. Analogously we define $R_\varepsilon^{\mathsf{pri}}(f)$ as the *$\varepsilon$-error private-coin* randomized communication complexity.

Although public-coin protocols are more general than private-coin ones, Newman [New91] proved that for boolean functions every public-coin protocol can be efficiently simulated by a private-coin protocol: If $f : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$ then for every $0 < \varepsilon < 1/2$,

$$R_{2\varepsilon}(f) \leq R_{2\varepsilon}^{\mathsf{pri}}(f) = O\left(R_\varepsilon(f) + \log \frac{\log(|\mathcal{X}||\mathcal{Y}|)}{\varepsilon}\right).$$

The additive logarithmic factor on the right-hand-side is often too small to matter, but it does make a difference in the bounds we prove below.

## 1.2 Fooling pairs and sets

Fooling sets are a well-known tool for proving lower bounds for $D(f)$. A pair $(x,y), (x',y') \in \mathcal{X} \times \mathcal{Y}$ is called *a fooling pair* for $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ if

- $f(x,y) = f(x',y')$, and
- either $f(x',y) \neq f(x,y)$ or $f(x,y') \neq f(x,y)$.

Observe that if $(x,y)$ and $(x',y')$ are a fooling pair then $x \neq x'$ and $y \neq y'$.

It is easy to see that if $(x,y)$ and $(x',y')$ form a fooling pair then there is no $f$-monochromatic rectangle that contains both of them. An immediate conclusion is the following:

**Lemma 1.1** ([KN97]). *Let $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ be a function, let $(x,y)$ and $(x',y')$ be a fooling pair for $f$ and let $\pi$ be a deterministic protocol for $f$. Then*

$$\pi(x,y) \neq \pi(x',y').$$

A subset $\mathcal{S} \subseteq \mathcal{X} \times \mathcal{Y}$ is a *fooling set* if every $p \neq p'$ in $\mathcal{S}$ form a fooling pair. Lemma 1.1 implies the following basic lower bound for deterministic communication complexity.

**Theorem 1.2** ([KN97]). *Let $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ be a function and let $\mathcal{S}$ be a fooling set for $f$. Then*

$$D(f) \geq \log_2(|\mathcal{S}|).$$

The same properties do not hold for randomized protocol, but the following variants are true. Let $\pi$ be an $\varepsilon$-error private-coin protocol for $f$, and let $(x, y), (x', y')$ be a fooling pair for $f$.

Here we prove that the probabilistic analogue of $\pi(x, y) \neq \pi(x', y')$ holds: we have that $|\Pi(x, y) - \Pi(x', y')|$ is large, where $|\Pi(x, y) - \Pi(x', y')|$ is the statistical distance between the two distributions on transcripts.

**Lemma 1.3** (Analogue of Lemma 1.1). *Let $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ be a function, let $(x, y)$ and $(x', y')$ be a fooling pair for $f$, and let $\pi$ be an $\varepsilon$-error private-coin protocol for $f$. Then*

$$|\Pi(x, y) - \Pi(x', y')| \geq 1 - 2\sqrt{\varepsilon}.$$

Lemma 1.3 is not only an analogue of Lemma 1.1 but is actually a generalization of it. Indeed, plugging $\varepsilon = 0$ in Lemma 1.3 implies Lemma 1.1. Moreover, it implies that the bound from Theorem 1.2 holds also in the 0-error private-coin randomized case.

An analogue of Theorem 1.2 holds as well:

**Theorem 1.4** (Analogue of Theorem 1.2). *Let $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ be a function and let $\mathcal{S}$ be a fooling set for $f$. Let $1/|\mathcal{S}| \leq \varepsilon < 1/3$. Then,*

$$R_\varepsilon^{\mathsf{pri}}(f) = \Omega\left(\log \frac{\log |\mathcal{S}|}{\varepsilon}\right).$$

The lower bound provided by the theorem above seems exponentially weaker than the one in Theorem 1.2, but it is tight. The equality function $\mathsf{EQ}$ over $n$-bit strings has a large fooling set of size $2^n$, but it is well-known (see [KN97]) that

$$R_\varepsilon^{\mathsf{pri}}(\mathsf{EQ}) = O\left(\log \frac{n}{\varepsilon}\right).$$

Theorem 1.4 therefore provide a tight lower bound on $R_\varepsilon^{\mathsf{pri}}(\mathsf{EQ})$ in terms of both $n$ and $\varepsilon$. It also provides a tight lower bound for the greater-than function. Moreover, Theorem 1.4 is a generalization of Theorem 1.2 and basically implies it by choosing $\varepsilon = 1/|\mathcal{S}|$.

The proof of the lower bound uses a general lower bound on the rank of perturbed identity matrices by Alon [Alo09]. Interestingly, although not every fooling set comes from an identity matrix (e.g. in the greater-than function), there is always some perturbed identity matrix in the background (the one used in the proof of Theorem 1.4).

We remark that for any constant $0 < \varepsilon < 1/3$, a version of Theorem 1.4 has been known for a long time. In particular, Håstad and Wigderson [HW07] give a proof of the following result[1] which appears in [Yao79] without proof: for every function $f$ with a fooling set $\mathcal{S}$ and for every $0 < \varepsilon < 1/3$,

$$R_\varepsilon^{\mathsf{pri}}(f) = \Omega\left(\log\log|\mathcal{S}|\right). \tag{1.1}$$

The right-hand side above does not depend on $\varepsilon$. The same lower bound as in (1.1) also directly follows from Theorem 1.2 and from the following general result [KN97]: for every function $f$ and for every $0 \le \varepsilon < 1/2$,

$$R_\varepsilon^{\mathsf{pri}}(f) = \Omega(\log D(f)).$$

## 1.3 Two types of fooling pairs

Let $(x,y),(x',y')$ be a fooling pair for a boolean function $f$. For simplicity, consider the case $(x,y) = (0,0)$ and $(x',y') = (1,1)$. There are essentially two types of fooling pairs:

- The $\mathsf{AND}$ type for which $f(1,0) \neq f(0,1)$.
- The $\mathsf{XOR}$ type for which $f(1,0) = f(0,1)$.

A partial proof of Lemma 1.3 is implicit in [BYJKS02]. The case considered in [BYJKS02] corresponds to a fooling pair of the $\mathsf{AND}$ type. Let $\pi$ be a private-coin $\varepsilon$-error protocol for $f$ that is the $\mathsf{AND}$ of two bits. In this case, by definition it must hold that $\Pi(0,0)$ is far away from $\Pi(1,1)$. The cut-and-paste property (see Corollary 2.2) implies that the same holds for $\Pi(0,1)$ and $\Pi(1,0)$.

The case of a fooling pair of the $\mathsf{XOR}$ type was not analyzed before. If $\pi$ is a private-coin $\varepsilon$-error protocol for $\mathsf{XOR}$ of two bits, then it does not immediately follow that $\Pi(0,0)$ is far away from $\Pi(1,1)$, nor that $\Pi(0,1)$ is far away from $\Pi(1,0)$. Lemma 1.3 implies that in fact both are true, but the argument can not use the cut-and-paste property. Our argument actually gives a better quantitative result for the $\mathsf{XOR}$ function as compared to the $\mathsf{AND}$ function.

The importance of the special case of Lemma 1.3 from [BYJKS02] is related to proving a lower bound on the randomized communication complexity of the disjointness

[1] In fact, the theorem in [Yao79, HW07] is more general than the one stated here. We state the theorem in this form since it fits well the focus of this text.

function $\mathsf{DISJ}$ defined over $\{0,1\}^n \times \{0,1\}^n$: $\mathsf{DISJ}(x,y) = 1$ if for all $i \in [n]$ it holds that $x_i \wedge y_i = 0$. They reproved that $R_{1/3}(\mathsf{DISJ}) \geq \Omega(n)$. This lower bound is extremely important and useful in many contexts and was first proved in [KS92].

On a high level, the proof of [BYJKS02] can be summarised in today's language as follows: Let $\pi$ be a private-coin protocol with (1/3)-error for $\mathsf{DISJ}$. We want to show that $\mathsf{CC}(\pi) = \Omega(n)$. The argument has two different parts: The first part of the argument essentially relates the *internal information cost* (as was later defined in [BBCR13]) of computing one copy of the $\mathsf{AND}$ function with the communication of the protocol $\pi$ for $\mathsf{DISJ}$. This is a direct-sum-esque result. More concretely, if $\mu$ is a distribution on $\{0,1\}^2$ such that $\mu(1,1) = 0$ then

$$\mathsf{IC}_\mu(\mathsf{AND}) \leq \frac{\mathsf{CC}(\pi)}{n},$$

where $\mathsf{IC}_\mu(\mathsf{AND})$ is the infimum over all (1/3)-error private-coin protocols $\tau$ for $\mathsf{AND}$ of the internal information cost of $\tau$. The second part of the argument shows that if $\mu$ is uniform on the set $\{(0,0),(0,1),(1,0)\}$ then $\mathsf{IC}_\mu(\mathsf{AND}) > 0$. The challenge in proving the second part stems from the fact that $\mu$ is supported on the zeros of $\mathsf{AND}$, so it is trivial to compute $\mathsf{AND}$ on inputs from $\mu$. However, the protocols $\tau$ in the definition of $\mathsf{IC}_\mu(\mathsf{AND})$ are guaranteed to succeed for every $x, y$ and not only on the support of $\mu$. The authors of [BYJKS02] use the cut-and-paste property (see Corollary 2.2 below) to argue that indeed $\mathsf{IC}_\mu(\mathsf{AND}) > 0$.

The argument as described above is very specific to the $\mathsf{AND}$ function. Here we show that it follows from a more general fooling-set based method.

We conclude this discussion with another observation concerning the difference between the two types of fooling pairs. Let $\mathsf{EQ}_k : [k] \times [k] \to \{0,1\}$ be the equality function on $k$ elements. Consider the following two seemingly similar functions on a pair of $n$-tuples of elements of $[k]$ for $k \in \{2,3\}$:

$$f_2(x,y) = \bigvee_{i=1}^{n} \mathsf{EQ}_2(x_i,y_i) \quad \text{and} \quad f_3(x,y) = \bigvee_{i=1}^{n} \mathsf{EQ}_3(x_i,y_i).$$

Since all the fooling pairs of $\mathsf{EQ}_2$ are of the $\mathsf{XOR}$ type, the private-coin communication complexity and internal information cost of $f_2$ are constants ($f_2$ is basically equality on $n$-bit strings). On the other hand, since $\mathsf{EQ}_3$ contains a fooling pair of the $\mathsf{AND}$ type, the private-coin complexity and internal information cost of $f_3$ are $\Omega(n)$.

# 2 Fooling pairs and sets

## 2.1 Preliminaries

**Communication.** In the case of deterministic protocols, the set of inputs reaching a particular leaf forms a rectangle (a product set inside $\mathcal{X} \times \mathcal{Y}$). In the case of private-coin randomized protocols, the following holds (see for example Lemma 6.7 in [BYJKS02]).

**Lemma 2.1** (Rectangle property for private-coin protocols)**.** *Let $\pi$ be a private-coin protocol over inputs from $\mathcal{X} \times \mathcal{Y}$, and let $\mathcal{L}$ denote the set of leaves of $\pi$. There exist functions $\alpha : \mathcal{L} \times \mathcal{X} \to [0,1]$, $\beta : \mathcal{L} \times \mathcal{Y} \to [0,1]$ such that for every $(x,y) \in \mathcal{X} \times \mathcal{Y}$ and every $\ell \in \mathcal{L}$,*

$$\mathbb{P}[\pi(x,y) \text{ reaches } \ell] = \alpha(\ell,x) \cdot \beta(\ell,y).$$

Here too the lemma is in fact a generalization of what happens in the deterministic case where $\alpha, \beta$ take values in $\{0,1\}$ rather than in $[0,1]$.

The above implies the following property of private-coin protocols that is more commonly known as the cut-and-paste property [PS86, CK91]. The *Hellinger* distance between two distributions $p, q$ over a finite set $\mathcal{U}$ is defined as

$$h(p,q) = \sqrt{1 - \sum_{u \in \mathcal{U}} \sqrt{p(u)q(u)}}.$$

**Corollary 2.2** (Cut-and-paste property)**.** *Let $(x,y)$ and $(x',y')$ be inputs to a randomized private-coin protocol $\pi$. Then*

$$h(\Pi(x,y), \Pi(x',y')) = h(\Pi(x',y), \Pi(x,y')).$$

The following immediately following from definitions.

**Proposition 2.3.** *Let $(x,y)$ and $(x',y')$ be such that $f(x,y) \neq f(x',y')$. Then, for any $\varepsilon$-error private-coin protocol $\pi$ for $f$,*

$$|\Pi(x,y) - \Pi(x',y')| \geq 1 - 2\varepsilon.$$

**Distances.** We use the following relationship between Statistical and Hellinger Distances.

**Lemma 2.4** (Statistical and Hellinger Distances)**.** *Let $p$ and $q$ be distributions such that the statistical distance $|p - q| \geq 1 - \varepsilon$ for $0 \leq \varepsilon \leq 1$. Then, $h^2(p,q) \geq 1 - \sqrt{2\varepsilon}$.*

*Proof.* In general, $h^2(p,q) \le |p-q| \le \sqrt{h^2(p,q)(2-h^2(p,q))}$. $\square$

**A geometric claim.** We use the following technical claim that has a geometric flavor. For two vectors $\mathbf{a}, \mathbf{b} \in \mathbb{R}^m$, we denote by $\langle \mathbf{a}, \mathbf{b} \rangle$ the standard inner product between $\mathbf{a}, \mathbf{b}$. Denote by $\mathbb{R}_+$ the set of non-negative real numbers.

**Claim 2.5.** *Let $\varepsilon_1, \varepsilon_2, \delta_1, \delta_2 > 0$ and let $\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d} \in \mathbb{R}_+^m$ be vectors such that*

$$\langle \mathbf{a}, \mathbf{b} \rangle \ge 1 - \varepsilon_1, \qquad \langle \mathbf{c}, \mathbf{d} \rangle \ge 1 - \varepsilon_2,$$
$$\langle \mathbf{a}, \mathbf{c} \rangle \le \delta_1, \qquad \langle \mathbf{b}, \mathbf{d} \rangle \le \delta_2.$$

*Then,*

$$\sum_{i\in[m]} |\mathbf{a}(i)\mathbf{b}(i) - \mathbf{c}(i)\mathbf{d}(i)| \ge 2 - (\varepsilon_1 + \varepsilon_2 + \delta_1 + \delta_2).$$

*Proof.*

$$\begin{aligned}
&\sum_{i\in[m]} |\mathbf{a}(i)\mathbf{b}(i) - \mathbf{c}(i)\mathbf{d}(i)| \\
&\quad \ge \sum_{i\in[m]} \left(\sqrt{\mathbf{a}(i)\mathbf{b}(i)} - \sqrt{\mathbf{c}(i)\mathbf{d}(i)}\right)^2 && (\forall t, s \ge 0 \ \ |t-s| \ge \left(\sqrt{t} - \sqrt{s}\right)^2) \\
&\quad = \langle \mathbf{a}, \mathbf{b} \rangle + \langle \mathbf{c}, \mathbf{d} \rangle - \sum_{i\in[m]} 2\sqrt{\mathbf{a}(i)\mathbf{b}(i)\mathbf{c}(i)\mathbf{d}(i)} \\
&\quad = \langle \mathbf{a}, \mathbf{b} \rangle + \langle \mathbf{c}, \mathbf{d} \rangle - \sum_{i\in[m]} 2\sqrt{\mathbf{a}(i)\mathbf{c}(i) \cdot \mathbf{b}(i)\mathbf{d}(i)} \\
&\quad \ge \langle \mathbf{a}, \mathbf{b} \rangle + \langle \mathbf{c}, \mathbf{d} \rangle - \sum_{i\in[m]} (\mathbf{a}(i)\mathbf{c}(i) + \mathbf{b}(i)\mathbf{d}(i)) && \text{(AM-GM inequality)} \\
&\quad = \langle \mathbf{a}, \mathbf{b} \rangle + \langle \mathbf{c}, \mathbf{d} \rangle - (\langle \mathbf{a}, \mathbf{c} \rangle + \langle \mathbf{b}, \mathbf{d} \rangle) \\
&\quad \ge 2 - (\varepsilon_1 + \varepsilon_2 + \delta_1 + \delta_2).
\end{aligned}$$

$\square$

## 2.2 Fooling pairs induce far away distributions

*Proof of Lemma 1.3.* Let the fooling pair be $(x,y)$ and $(x',y')$ and assume without loss of generality that $f(x,y) = f(x',y') = 1$. We distinguish between the following two cases.

(a) $f(x,y') \ne f(x,y')$.

(b) $f(x',y) = f(x,y') = 0$.

In the first case, Proposition 2.3 implies that $|\Pi(x',y)-\Pi(x,y')| \geq 1-2\varepsilon$. Proposition 2.2 implies that $h(\Pi(x,y),\Pi(x',y')) = h(\Pi(x',y),\Pi(x,y'))$. Lemma 2.4 thus implies that $|\Pi(x,y)-\Pi(x',y')| \geq 1-2\sqrt{\varepsilon}$.

Let us now consider the second case. Let $\mathcal{L}$ be the set of all leaves of $\pi$ and let $\mathcal{L}_1$ denote those leaves which are labeled by 1. For $x \in \mathcal{X}$, $y \in \mathcal{Y}$, define the vectors $\mathbf{a}_x \in \mathbb{R}_+^{\mathcal{L}_1}$ as $\mathbf{a}_x(\ell) = \alpha(\ell,x)$, and the vectors $\mathbf{b}_y \in \mathbb{R}_+^{\mathcal{L}_1}$ as $\mathbf{b}_y(\ell) = \beta(\ell,y)$ where $\alpha$ and $\beta$ are the functions from Lemma 2.1. Since $f(x,y)=1$ and $\pi$ is an $\varepsilon$-error protocol for $f$,

$$\langle \mathbf{a}_x, \mathbf{b}_y \rangle = \sum_{\ell \in \mathcal{L}_1} \alpha(\ell,x)\cdot\beta(\ell,y) = \mathbb{P}[L(\pi(x,y))=1] \geq 1-\epsilon.$$

Similarly, we have $\langle \mathbf{a}_{x'}, \mathbf{b}_{y'} \rangle \geq 1-\varepsilon$, $\langle \mathbf{a}_x, \mathbf{b}_{y'} \rangle \leq \varepsilon$ and $\langle \mathbf{a}_{x'}, \mathbf{b}_y \rangle \leq \varepsilon$. Observe

$$2|\Pi(x,y)-\Pi(x',y')| \geq \sum_{\ell \in \mathcal{L}_1} |\mathbf{a}_x(\ell)\mathbf{b}_y(\ell) - \mathbf{a}_{x'}(\ell)\mathbf{b}_{y'}(\ell)|.$$

Applying Proposition 2.5 with the vectors $\mathbf{a}_x, \mathbf{b}_y, \mathbf{a}_{x'}, \mathbf{b}_{y'}$ yields that $|\Pi(x,y)-\Pi(x',y')| \geq 1-2\varepsilon$. □

## 2.3 A lower bound based on fooling sets

The following result of Alon [Alo09] on the rank of perturbed identity matrices is a key ingredient.

**Lemma 2.6.** *Let $\frac{1}{2\sqrt{m}} \leq \varepsilon < \frac{1}{4}$. Let $M$ be an $m \times m$ matrix such that $|M(i,j)| \leq \varepsilon$ for all $i \neq j$ in $[m]$ and $|M(i,i)| \geq \frac{1}{2}$ for all $i \in [m]$. Then,*

$$\mathsf{rank}(M) \geq \Omega\left(\frac{\log m}{\varepsilon^2}\right).$$

*Proof of Theorem 1.4.* Let $\mathcal{L}$ denote the set of leaves of $\pi$. Let $A \in \mathbb{R}^{\mathcal{S}\times\mathcal{L}}$ be the matrix defined by

$$A_{(x,y),\ell} = \sqrt{\mathbb{P}[\pi(x,y)=\ell]}.$$

Let

$$M = AA^T$$

where $A^T$ is $A$ transposed. First,

$$M_{(x,y),(x,y)} = 1.$$

Second, if $(x,y) \neq (x',y')$ in $\mathcal{S}$ then by Lemma 1.3 we know $|\Pi(x,y)-\Pi(x',y')| \geq 1-2\sqrt{\varepsilon}$

so by Lemma 2.4

$$h^2(\Pi(x,y),\Pi(x',y')) \geq 1 - 2\varepsilon^{1/4}$$

which implies

$$M_{(x,y),(x',y')} = 1 - h^2(\Pi(x,y),\Pi(x',y')) \leq 2\varepsilon^{1/4}.$$

Lemma 2.6 implies that[2] the rank of $M$ is at least $\Omega\left(\frac{\log|\mathcal{S}|}{\sqrt{\varepsilon}}\right)$. On the other hand,

$$2^{CC(\pi)} \geq |\mathcal{L}| \geq \mathsf{rank}(M).$$

□

# References


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

[BBCR13] Boaz Barak, Mark Braverman, Xi Chen, and Anup Rao. How to compress interactive communication. *SIAM J. Comput.*, 42(3):1327–1363, 2013.

[BYJKS02] Ziv Bar-Yossef, T. S. Jayram, Ravi Kumar, and D. Sivakumar. An Information Statistics Approach to Data Stream and Communication Complexity. In *FOCS*, pages 209–218, 2002.

[CK91] Benny Chor and Eyal Kushilevitz. A zero-one law for boolean privacy. *SIAM J. Discrete Math.*, 4(1):36–47, 1991.

[HW07] J. Hastad and A. Wigderson. The randomized communication complexity of set disjointness. *Theory of Computing*, 3(1):211–219, 2007.

[KN97] Eyal Kushilevitz and Noam Nisan. *Communication complexity*. Cambridge University Press, New York, NY, USA, 1997.

[Kra96] Matthias Krause. Geometric Arguments Yield Better Bounds for Threshold Circuits and Distributed Computing. *Theor. Comput. Sci.*, 156(1&2):99–117, 1996.


[2] We may assume that say $\varepsilon < 2^{-12}$ by repeating the given randomized protocol a constant number of times.

[KS92] Bala Kalyanasundaram and Georg Schnitger. The probabilistic communication complexity of set intersection. *SIAM J. Discrete Math.*, 5(4):545–557, 1992.

[LS09] Troy Lee and Adi Shraibman. Lower bounds in communication complexity. *Foundations and Trends in Theoretical Computer Science*, 3(4):263–398, 2009.

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

[PS86] Ramamohan Paturi and Janos Simon. Probabilistic communication complexity. *J. Comput. Syst. Sci.*, 33(1):106–123, 1986.

[Yao79] Andrew Chi-Chih Yao. Some complexity questions related to distributive computing (preliminary report). In *STOC*, pages 209–213, 1979.



ECCC ISSN 1433-8092

http://eccc.hpi-web.de