Pseudodeterminism and $\mathsf{MA} \neq \mathsf{NP}^{\mathsf{BPP}}$ in Communication Complexity

Thomas Watson*

August 24, 2026

Abstract

We prove an exponential separation between zero-sided-error randomized and two-sided-error pseudodeterministic communication complexities of partial boolean functions. This qualitatively improves and simplifies the proof of the separation by Göös, Harms, Riazanov, Sofronova, Sokolov, and Yuan (STOC 2026), which had a two-sided-error randomized upper bound. Then, we generalize our technique to separate the communication complexity analogues of MA and $\mathsf{NP}^{\mathsf{BPP}}$.

1 Introduction

A randomized algorithm for a search problem (relation) is such that for every input, with high probability, the algorithm outputs a solution. A *pseudodeterministic* algorithm for a search problem is a randomized algorithm such that for every input, there exists a solution s such that with high probability, the algorithm outputs s. Thus "pseudodeterministic" is sandwiched between "deterministic" and "randomized." One benefit of pseudodeterministic algorithms is that the success probability can be amplified, whereas for randomized algorithms it generally can't be (unless there's an efficient algorithm to check whether a given s is indeed a solution). Pseudodeterminism has applications in cryptography, machine learning, and distributed computing, and has been studied in the settings of time complexity [GG11, GGR13, OS17, DPV18, OS18, Gol25, DPV21, LOS21, DPWV22, CLORS26], space complexity [GL19, GGMW20, BKKS23, GGS23], query complexity [GGR13, GIPS21, CDM25, Gav25], communication complexity [HN12, BHHLT26, GHRSSY26], parallel time complexity [GG17, GG21], interactive proofs [GGH18, GGH19], and quantum computing [AGL26].

Suppose $F\colon \{0,1\}^N \to \{0,1,\perp\}$ is a partial boolean function (promise decision problem), where $\perp$ means "input is invalid; don't care about the output." We view F as a search problem where $\perp$ means "both 0 and 1 are solutions." On an invalid input, a pseudodeterministic algorithm must accept with either high or low probability (it doesn't matter which), whereas a randomized algorithm may accept with any probability. Thus, in any model of computation, the pseudodeterministic complexity of F is the minimum randomized complexity of any total function $F'\colon \{0,1\}^N \to \{0,1\}$ that agrees with F.

We consider the model of two-party communication protocols. $\mathsf{P} \subseteq \mathsf{ZPP} \subseteq \mathsf{RP} \subseteq \mathsf{BPP}$ are the complexity classes of all (infinite families of) functions $F\colon \{0,1\}^N \times \{0,1\}^N \to \{0,1,\perp\}$ with $\mathrm{polylog}\, N$

*Department of Computer Science, University of Memphis. Supported by NSF grant CCF-1942742.

deterministic, zero-sided-error, one-sided-error, and two-sided-error randomized communication complexity, respectively. (In the literature, sometimes a ^{cc} superscript differentiates such classes from their time complexity counterparts.) Recall $\mathsf{ZPP} = \mathsf{RP} \cap \mathsf{coRP}$. Let psP be the analogous class for two-sided-error pseudodeterministic communication complexity. [GHRSSY26] proved $\mathsf{BPP} \not\subseteq \mathsf{psP}$ by showing that some two-party partial boolean function has two-sided-error randomized communication complexity $O(\log N)$ and two-sided-error pseudodeterministic communication complexity $\widetilde{\Omega}(\sqrt{N})$. Their argument does not yield an upper bound with one-sided error. We improve the upper bound all the way to zero-sided error. Our result qualitatively improves, quantitatively matches, and somewhat simplifies the proof of the main result in [GHRSSY26].

Theorem 1. $\mathsf{ZPP} \not\subseteq \mathsf{psP}$ *in communication complexity.*

It may appear unrelated, but this theorem is a stepping stone and warm-up for our next theorem.

Communication complexity analogues of other classical complexity classes have many applications, as surveyed in [GPW18b]. A grand challenge is to separate the communication complexity polynomial hierarchy. A notable subclass of the polynomial hierarchy is MA, corresponding to Merlin–Arthur communication: Merlin (who knows both Alice's and Bob's inputs) sends a message (witness) to Alice and Bob (jointly constituting Arthur), who then run a randomized communication protocol with each other. On a 1-input, some witness makes Alice and Bob accept with probability $\geq 2/3$. On a 0-input, every witness makes Alice and Bob accept with probability $\leq 1/3$. The classic problems Disjointness and Inner Product Mod 2 have Merlin–Arthur communication complexity $\widetilde{O}(\sqrt{N})$ [AW09, Che20] and $\Omega(\sqrt{N})$ [Kla03]. No $\omega(\sqrt{N})$ lower bound is known for the Merlin–Arthur communication complexity of any explicit function. Also, MA is contained in AM (Arthur–Merlin) and in $\mathsf{S_2P}$ (symmetric alternation), which are subclasses of the communication polynomial hierarchy for which no $\omega(\log N)$ lower bound is known for any explicit function. Thus MA is close to the frontier of communication complexity lower bounds. Also, Merlin–Arthur communication has applications to streaming [CCMT14, GR15, GS24], property testing [GR18], hardness of approximation [ARW17], and cryptography [BBGT25].

$\mathsf{NP}^{\mathsf{BPP}}$ is the class of all $F\colon \{0,1\}^N \times \{0,1\}^N \to \{0,1,\perp\}$ with NP-type protocols that can make adaptive oracle queries to some $G\colon \{0,1\}^M \times \{0,1\}^M \to \{0,1,\perp\}$ in BPP with $M \in \operatorname{poly} N$. For every valid input to F and every possible witness, the queries must be valid inputs to G. A randomized protocol could handle the whole sequence of queries, so there might as well be just one query, consisting of the input and the witness: $\mathsf{NP}^{\mathsf{BPP}}$ equals the class $\mathsf{N} \cdot \mathsf{BPP}$ (also denoted $\exists \cdot \mathsf{BPP}$) of all $F\colon \{0,1\}^N \times \{0,1\}^N \to \{0,1,\perp\}$ such that for some $G\colon \{0,1\}^{N+W} \times \{0,1\}^{N+W} \to \{0,1,\perp\}$ in BPP with $W \in \operatorname{polylog} N$, and for all valid inputs (x,y) to F,

$$F(x,y)=1 \;\Rightarrow\; \exists w\colon\; G(xw,yw)=1 \qquad F(x,y)=0 \;\Rightarrow\; \forall w\colon\; G(xw,yw)=0$$

and (xw,yw) is a valid input to G for all w. (For surveys of complexity class dot operators, see [ZP03] and [Koz06, lecture G].) The $\mathsf{NP}^{\mathsf{BPP}}$ requirement that queries are valid corresponds to the $\mathsf{N} \cdot \mathsf{BPP}$ requirement that (xw,yw) is valid. At a glance, $\mathsf{N} \cdot \mathsf{BPP}$ looks like MA where Merlin sends w and Alice and Bob run the randomized protocol for $G(xw,yw)$. When $F(x,y)=1$, some w makes Alice and Bob accept with probability $\geq 2/3$, but for each other w, their acceptance probability must be either $\geq 2/3$ or $\leq 1/3$ (it doesn't matter which) for $\mathsf{N} \cdot \mathsf{BPP}$ but may be anything for MA. This is the connection to pseudodeterminism. We have $\mathsf{NP}^{\mathsf{BPP}} = \mathsf{N} \cdot \mathsf{BPP} \subseteq \mathsf{MA}$. We answer one of the remaining open questions mentioned in [GPW18b]:

Theorem 2. $\mathsf{MA} \not\subseteq \mathsf{NP}^{\mathsf{BPP}}$ *in communication complexity.*

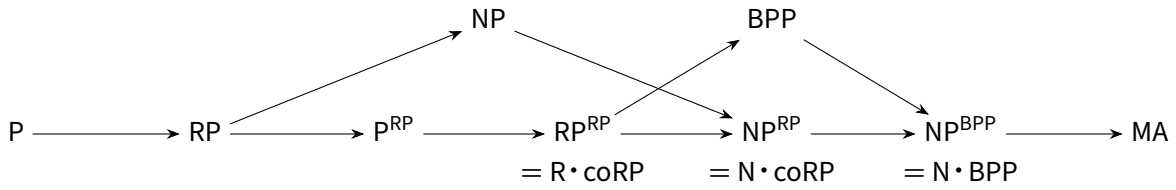

Figure 1: Inclusions among communication complexity classes, where $\mathcal{C}_1 \longrightarrow \mathcal{C}_2$ means $\mathcal{C}_1 \subseteq \mathcal{C}_2$

Consider time complexity classes for a moment: Under a standard derandomization assumption, MA collapses to NP and hence equals $\mathsf{NP}^{\mathsf{BPP}}$. But the distinction still matters since some results such as $\mathsf{EXP} \subseteq \mathsf{P/poly} \Rightarrow \mathsf{EXP} = \mathsf{MA}$ [BFL91] aren't known with $\mathsf{NP}^{\mathsf{BPP}}$ in place of MA. [FFKL03] proved the relativized separation $\mathsf{MA} \not\subseteq \mathsf{NP}^{\mathsf{BPP}}$. In general, relativized separations of time complexity classes are implied by separations of analogous query complexity classes, but the converse doesn't necessarily hold. In this case, the proof in [FFKL03] doesn't yield $\mathsf{MA} \not\subseteq \mathsf{NP}^{\mathsf{BPP}}$ in query complexity, but the latter separation was shown by Mika Göös and reported in [Wat20a].

The upshot of Theorem 2 is that we contribute to the goal of better understanding the communication polynomial hierarchy, by picking apart its subclasses.

Figure 1 provides some context regarding the theme of randomized oracles in communication complexity. We'd like to highlight the open problem of proving $\mathsf{BPP} \not\subseteq \mathsf{NP}^{\mathsf{RP}}$. The weaker separation $\mathsf{BPP} \not\subseteq \mathsf{NP}^{\textsc{Equality}}$ is known [PSS23], but neither of the two weaker separations $\mathsf{BPP} \not\subseteq \mathsf{RP}^{\mathsf{RP}}$ and $\mathsf{NP}^{\mathsf{BPP}} \not\subseteq \mathsf{NP}^{\mathsf{RP}}$ is known. Analogous to $\mathsf{NP}^{\mathsf{NP}} = \mathsf{N} \cdot \mathsf{coNP} = \Sigma_2\mathsf{P}$, we have the folklore facts $\mathsf{RP}^{\mathsf{RP}} = \mathsf{R} \cdot \mathsf{coRP}$ and $\mathsf{NP}^{\mathsf{RP}} = \mathsf{N} \cdot \mathsf{coRP}$.

$\mathsf{BPP} \subseteq \mathsf{R} \cdot \mathsf{coRP}$ would hold by essentially the proof of $\mathsf{BPP} \subseteq \Sigma_2\mathsf{P}$ in [Lau83] if we removed the implicit one-sided-error pseudodeterminism in the definition of $\mathsf{R} \cdot \mathsf{coRP}$. [MV96, BF99] proved the relativized separation of the time complexity classes $\mathsf{BPP} \not\subseteq \mathsf{RP}^{\mathsf{RP}}$, but the proof doesn't yield $\mathsf{BPP} \not\subseteq \mathsf{RP}^{\mathsf{RP}}$ in query complexity. Proving the latter separation would be a first step toward proving $\mathsf{BPP} \not\subseteq \mathsf{RP}^{\mathsf{RP}}$ in communication complexity.

Similarly, $\mathsf{N} \cdot \mathsf{BPP} \subseteq \mathsf{N} \cdot \mathsf{coRP}$ would hold if we removed the pseudodeterminism. This is just the observation that for MA, two-sided error can be made one-sided (perfect completeness). By the way, $\mathsf{N} \cdot \mathsf{coRP}$ is also interesting since it contains the complement of List Non-Equality, which is a classic total function exhibiting a quadratic separation between zero-sided-error randomized and deterministic communication complexities [KN97, §4.1].

The class P^{RP} is also notable. It contains Greater Than. We have $\mathsf{BPP} \not\subseteq \mathsf{P}^{\mathsf{RP}}$ since $\mathsf{BPP} \not\subseteq \mathsf{P}^{\mathsf{NP}}$ [PSS14]. Restricting P^{RP} to constant numbers of queries yields the randomized boolean hierarchy, which is known to be strict [PSW21].

1.1 Definitions

For basic background on communication complexity, see the textbooks [KN97, Juk12, RY20, Wat26]. We define communication models for computing two-party partial functions $F : \{0,1\}^N \times \{0,1\}^N \to \{0,1,\bot\}$ where $\bot$ means "don't care," and if $F(x,y) \neq \bot$ we say (x,y) is a valid input. For each model, the corresponding complexity measure of F is the minimum cost of any protocol computing F in the model, and the corresponding complexity class is the set of all infinite families of Fs with complexity $\operatorname{polylog} N$. For example, P is the class of all families with deterministic communication complexity $\operatorname{polylog} N$. If D is a distribution over deterministic protocols P (that output 1 or 0), we define the notation $D(x,y) = \mathbf{Pr}_{P \sim D}\big[P(x,y) = 1\big]$.

An RP-type (one-sided-error randomized) protocol of cost d for F is a distribution D over deterministic protocols of depth d such that for all valid (x, y):

$$F(x,y) = 1 \;\Rightarrow\; D(x,y) \geq 2/3 \qquad F(x,y) = 0 \;\Rightarrow\; D(x,y) = 0$$

A BPP-type (two-sided-error randomized) protocol of cost d for F is a distribution D over deterministic protocols of depth d such that for all valid (x, y):

$$F(x,y) = 1 \;\Rightarrow\; D(x,y) \geq 2/3 \qquad F(x,y) = 0 \;\Rightarrow\; D(x,y) \leq 1/3$$

A psP-type (two-sided-error pseudodeterministic) protocol of cost d for F is a distribution D over deterministic protocols of depth d such that for all valid or invalid (x, y), we have $D(x,y) \in [0, 1/3] \cup [2/3, 1]$, and:

$$F(x,y) = 1 \;\Rightarrow\; D(x,y) \geq 2/3 \qquad F(x,y) = 0 \;\Rightarrow\; D(x,y) \leq 1/3$$

An NP-type (nondeterministic) protocol of cost d for F is a set $\mathcal{P}$ of $\leq 2^d$ deterministic protocols of depth d such that for all valid (x, y):

$$F(x,y) = 1 \;\Rightarrow\; \exists P \in \mathcal{P} :\; P(x,y) = 1 \qquad F(x,y) = 0 \;\Rightarrow\; \forall P \in \mathcal{P} :\; P(x,y) = 0$$

An MA-type (Merlin–Arthur) protocol of cost d for F is a set $\mathcal{D}$ of $\leq 2^d$ distributions over deterministic protocols of depth d such that for all valid (x, y):

$$F(x,y) = 1 \;\Rightarrow\; \exists D \in \mathcal{D} :\; D(x,y) \geq 2/3 \qquad F(x,y) = 0 \;\Rightarrow\; \forall D \in \mathcal{D} :\; D(x,y) \leq 1/3$$

An N·BPP-type protocol of cost d for F is a set $\mathcal{D}$ of $\leq 2^d$ distributions over deterministic protocols of depth d such that for all valid (x, y), we have $D(x,y) \in [0, 1/3] \cup [2/3, 1]$ for all $D \in \mathcal{D}$, and:

$$F(x,y) = 1 \;\Rightarrow\; \exists D \in \mathcal{D} :\; D(x,y) \geq 2/3 \qquad F(x,y) = 0 \;\Rightarrow\; \forall D \in \mathcal{D} :\; D(x,y) \leq 1/3$$

An N·coRP-type protocol of cost d for F is a set $\mathcal{D}$ of $\leq 2^d$ distributions over deterministic protocols of depth d such that for all valid (x, y), we have $D(x,y) \in [0, 1/3] \cup \{1\}$ for all $D \in \mathcal{D}$, and:

$$F(x,y) = 1 \;\Rightarrow\; \exists D \in \mathcal{D} :\; D(x,y) = 1 \qquad F(x,y) = 0 \;\Rightarrow\; \forall D \in \mathcal{D} :\; D(x,y) \leq 1/3$$

An R·coRP-type protocol of cost d for F is a distribution D_1 over distributions D_2 over deterministic protocols of depth d such that for all valid (x, y), we have $D_2(x,y) \in [0, 1/3] \cup \{1\}$ for all D_2 in D_1's support, and:

$$F(x,y) = 1 \;\Rightarrow\; \mathbf{Pr}_{D_2 \sim D_1}\big[D_2(x,y) = 1\big] \geq 2/3 \qquad F(x,y) = 0 \;\Rightarrow\; \mathbf{Pr}_{D_2 \sim D_1}\big[D_2(x,y) \leq 1/3\big] = 1$$

The error probabilities in these models can be amplified as usual. In particular, amplifying from $1/3$ to any constant > 0 only affects the cost by a constant factor.

2 Approach

2.1 Intuition

Query-to-communication lifting is a general approach to deducing communication complexity lower bounds from query complexity (decision tree depth) lower bounds. The idea is to compose an outer

function $f\colon \{0,1\}^n \to \{0,1,\bot\}$ with a two-party gadget function $g\colon \{0,1\}^h \times \{0,1\}^h \to \{0,1\}$ to define the two-party function $F\colon (\{0,1\}^h)^n \times (\{0,1\}^h)^n \to \{0,1,\bot\}$ by $F(x,y) = f\big(g(x_1,y_1)\cdots g(x_n,y_n)\big)$. A lifting theorem says F's communication complexity is at least f's query complexity if g is complicated enough to effectively preclude communication protocols from doing anything more clever than just running a decision tree for f and straightforwardly evaluating $g(x_i,y_i)$ when the decision tree queries its ith input bit. The query lower bound for f is the "spherical cow in a vacuum" version of the communication lower bound for F. The lifting theorem handles all the messiness of arbitrary communication protocols.

We have lifting theorems for many models of query/communication complexity, such as deterministic (P), nondeterministic (NP), randomized (BPP), and so on [RM99, GLMWZ16, Göö15, GPW18a, GKPW19, GPW20, GGKS20, Wat20b, CFKMP21, PSW21, LMMPZ22]. In these settings, any old query lower bound proof is fine, and the lifting theorem is used as a black box. For other models, we don't know a general lifting theorem, but we may still be able to apply lifting techniques in a white-box manner to imitate a particular query lower bound proof for a particular f. Examples of white-box query-to-communication lifting include [Wat16, YZ24, HMWYZ25, GHRSSY26].

We don't have lifting theorems for psP or $\mathsf{NP}^{\mathsf{BPP}}$. If we did, our theorems would automatically follow from the corresponding query complexity separations, which are simple to prove. So we use the white-box approach, like [GHRSSY26]. But the simplest proofs of $\mathsf{ZPP} \not\subseteq \mathsf{psP}$ and $\mathsf{MA} \not\subseteq \mathsf{NP}^{\mathsf{BPP}}$ in query complexity aren't "liftable." For example: The proof of $\mathsf{MA} \not\subseteq \mathsf{NP}^{\mathsf{BPP}}$ in query complexity in [Wat20a] reaches a contradiction of some randomized decision tree accepting some input z with probability $\approx 1/2$ when it should be $\geq 2/3$ or $\leq 1/3$. In the composed function F, z corresponds to a *slice* of inputs $\big\{(x,y) : g(x_1,y_1)\cdots g(x_n,y_n) = z\big\}$. The acceptance probabilities might be $\geq 2/3$ for half of the slice's inputs and $\leq 1/3$ for the other half, leading to average acceptance probability $\approx 1/2$ over the slice, without yielding a contradiction. So we first adapt the query complexity lower bound proofs to make them amenable to lifting.

Definitions: A randomized decision tree of cost d is a distribution D over deterministic decision trees T of depth d. For an input $z \in \{0,1\}^n$, define the notation $D(z) = \mathbf{Pr}_{T\sim D}\big[T(z) = 1\big]$. Let $|z|$ be z's weight (number of 1s), and let $z_{\leftarrow} = z_1 \cdots z_{n/2}$ and $z_{\rightarrow} = z_{n/2+1} \cdots z_n$ be z's left and right halves.

Intuition for $\mathsf{ZPP} \not\subseteq \mathsf{psP}$: To prove the query complexity version, define $f\colon \{0,1\}^n \to \{0,1,\bot\}$ by:

$$f(z) = \begin{cases} 1 & \text{if } |z_{\rightarrow}| \geq n/3 \text{ and } |z_{\leftarrow}| = 0 \\ 0 & \text{if } |z_{\leftarrow}| \geq n/3 \text{ and } |z_{\rightarrow}| = 0 \end{cases}$$

$f \in \mathsf{ZPP}$: We have $f \in \mathsf{RP}$ by the randomized decision tree that picks a uniformly random $i \in \{n/2+1,\ldots,n\}$ and queries and outputs z_i. We have $\overline{f} \in \mathsf{RP}$ by the randomized decision tree that picks a uniformly random $i \in \{1,\ldots,n/2\}$ and queries and outputs z_i.

$f \notin \mathsf{psP}$: Suppose for contradiction that some total function $f'\colon \{0,1\}^n \to \{0,1\}$ that agrees with f has a $1/3$-error randomized decision tree D of cost $n/20$. Initially let $z = 0^n$, and assume $f'(z) = 1$ so $D(z) \geq 2/3$. A symmetric argument handles the case $f'(z) = 0$. If we obtain z' from z by flipping a uniformly random 0 to 1 in $z_{\leftarrow}$, then $\mathbf{Pr}_{z',T\sim D}\big[T(z') \text{ queries the flipped bit}\big] \leq (n/20)/(n/2) < 1/3$, so $\mathbf{E}_{z'}\big[D(z')\big] = \mathbf{Pr}_{z',T\sim D}\big[T(z') = 1\big] \geq \mathbf{Pr}_{z',T\sim D}\big[T(z) = 1 \text{ and } T(z') \text{ doesn't query the flipped bit}\big] > D(z) - 1/3 \geq 1/3$. Hence there exists an outcome z' such that $D(z') > 1/3$, so $f'(z') = 1$ and thus $D(z') \geq 2/3$. Update z to z'. Repeat this process, maintaining the invariant $f'(z) = 1$, until $n/3$ many 0s have been flipped to 1s in $z_{\leftarrow}$. Then $f(z) = 0$ and thus $f'(z) = 0$, which is a contradiction.

This iterative argument alternates between "sneak another 1 into $z_{\leftarrow}$ without decreasing $D(z)$ much" and "boost $D(z)$ back up to $\geq 2/3$." The latter happens automatically as long as $D(z) > 1/3$.

But it's not automatic when we imitate this argument in communication complexity: We maintain the invariant that $F'(x,y)=1$ for a large fraction of all (x,y) in z's slice. We can sneak another 1 into $z_{\leftarrow}$ without decreasing this fraction much, but the decreases would accumulate, so we need to interleave boosting steps. A key idea from [GHRSSY26] and its progenitor [Gav25] exploits the hypothesized pseudodeterministic protocol to boost the fraction of 1-inputs of F' in z's slice by restricting to some subrectangle. This restriction fixes (hardwires) some of z's bits, so we can't subsequently flip any fixed 0s to 1s. This threatens our goal of getting $|z_{\leftarrow}| \geq n/3$. The next idea from [Gav25, GHRSSY26] is to instead randomly sneak $\sqrt{n}$ many 1s at a time into $z_{\leftarrow}$ to offset the fixed 0s, so $z_{\leftarrow}$ still ends up with many more 1s than 0s. If the pseudodeterministic protocol has cost $0.01\sqrt{n}$ (a weaker but good enough lower bound), then typically only $\approx 0.01\sqrt{n}$ bits of z get fixed per iteration, in which case the protocol "hardly notices" the $\sqrt{n}$ many bits being flipped (à la birthday paradox). Some iterations may fix many more than $0.01\sqrt{n}$ bits, but that can't happen too often since it causes a corresponding decrease in a certain potential function.

Our proof is similar in outline to [GHRSSY26] but simpler in the technical details. We iteratively whittle down a set of inputs to the outer function f like in [GHRSSY26], but a fundamental difference is that we also focus on an individual input z in this set, iteratively changing which input we're focusing on. To accomplish this, we employ the query-to-communication lifting tool from [GLMWZ16] rather than the one in [GHRSSY26].

Intuition for $\mathsf{MA} \not\subseteq \mathsf{NP}^{\mathsf{BPP}}$: To prove the query complexity version (in a less straightforward but more "liftable" way than in [Wat20a]): Viewing the input z as a square binary matrix, first define f by $f(z)=1$ if some row is all-1s, and $f(z)=0$ if every row is at most a third 1s. This f is canonically in MA, where rows correspond to Merlin's witnesses and columns correspond to Arthur's randomness. One row will play a distinguished role, and each other row will be all-1s or all-0s and thus might as well be a single bit. So redefine $f\colon \{0,1\}^n \to \{0,1,\bot\}$ by letting $z_{\leftarrow}$ be the distinguished row and $z_{\rightarrow}$ be all the "single bit rows":

$$f(z) \;=\; \begin{cases} 1 & \text{if } |z_{\leftarrow}| = n/2 \quad \text{or} \quad |z_{\rightarrow}| > 0 \\ 0 & \text{if } |z_{\leftarrow}| \leq n/6 \text{ and } |z_{\rightarrow}| = 0 \end{cases}$$

$f \notin \mathsf{NP}^{\mathsf{BPP}} = \mathsf{N}\cdot\mathsf{BPP}$: Suppose for contradiction f has an $\mathsf{N}\cdot\mathsf{BPP}$-type decision tree of cost δn where the BPP part has been amplified to have error probability ε instead of $1/3$, where $\delta=\varepsilon=1/20$. Initially let $z = 1^{n/2}0^{n/2}$, so $f(z)=1$. Fixing the pertinent witness for input z yields a randomized decision tree D of cost δn that has acceptance probability $\geq 1-\varepsilon$ for input z, and $\leq \varepsilon$ for each 0-input of f, and $\geq 1-\varepsilon$ or $\leq \varepsilon$ for each other 1-input of f. Similar to $\mathsf{ZPP} \not\subseteq \mathsf{psP}$, we iteratively modify the initial 1-input z to reach some 0-input by sneaking a total of $n/3$ many 0s into $z_{\leftarrow}$ (and leaving $z_{\rightarrow}$ alone), maintaining the invariant that $D(z) \geq 2/3$. At the end, $f(z)=0$ and thus $D(z) \leq \varepsilon$, contradicting the invariant. In each iteration, randomly sneaking another 0 into $z_{\leftarrow}$ only decreases $D(z)$ by $\leq \delta n/(n/6) = 6\delta$, so $D(z) \geq 2/3 - 6\delta > 1/3$ after this. We claim that $D(z)$ is automatically boosted back to $\geq 2/3$, but this is trickier to see because this intermediate z is an invalid input to f and thus $D(z)$ is unconstrained.

Proof of the claim: Consider the set Z of all "nearby" 1-inputs z' obtained from the current z (after flipping a 1 to 0 in $z_{\leftarrow}$) by flipping a 0 to 1 in $z_{\rightarrow}$. We have $\mathbf{Pr}_{z'\in Z,\, T\sim D}\big[T(z) \neq T(z')\big] \leq \mathbf{Pr}_{z'\in Z,\, T\sim D}\big[T(z') \text{ queries the flipped bit}\big] \leq \delta n/|Z| = 2\delta$ and thus $D(z) \in \mathbf{E}_{z'\in Z}\big[D(z')\big] \pm 2\delta$. Since D behaves pseudodeterministically on Z, it's an ε-error randomized decision tree for some $f'\colon Z \to \{0,1\}$. We have $\mathbf{E}_{z'\in Z}\big[D(z')\big] \in \mathbf{E}_{z'\in Z}\big[f'(z')\big] \pm \varepsilon$. There exists a deterministic decision tree T in the support of D such that $\mathbf{Pr}_{z'\in Z}\big[f'(z') \neq T(z')\big] \leq \varepsilon$ and thus $\mathbf{E}_{z'\in Z}\big[f'(z')\big] \in \mathbf{E}_{z'\in Z}\big[T(z')\big] \pm \varepsilon$. We have

$\mathbf{Pr}_{z'\in Z}\big[T(z')\neq T(z)\big]\le \mathbf{Pr}_{z'\in Z}\big[T(z')$ queries the flipped bit$\big]\le \delta n/|Z| = 2\delta$ and thus $\mathbf{E}_{z'\in Z}\big[T(z')\big]\in T(z)\pm 2\delta$. Stringing everything together, $D(z)\in T(z)\pm(4\delta+2\varepsilon)\subseteq T(z)\pm 1/3$. If $T(z)=0$ then $D(z)\le 1/3$ contradicting $D(z)>1/3$, so we must have $T(z)=1$ and thus $D(z)\ge 2/3$. In summary, $D(z)>1/3$ is automatically boosted to $D(z)\ge 2/3$, and we continue to the next iteration.

We imitate this proof in communication complexity using query-to-communication lifting techniques, like with $\mathsf{ZPP}\not\subseteq\mathsf{psP}$. We sneak $\sqrt{n}$ many 0s into $z_{\leftarrow}$ per iteration, to offset the fixed 1s, of which there are typically only $\approx 0.01\sqrt{n}$ per iteration, assuming the protocol has cost $0.01\sqrt{n}$. The most subtle aspect of the proof is in the analogue to the boosting step: This requires restricting to a subrectangle that fixes some bits of the input to f. Doing this naively might result in a fixed 1 in the right half of the input (preventing us from reaching a 0-input at the end of the proof) since the boosting focuses on the inputs $z'\in Z$, which each have a 1 in their right half. Intuitively, the restriction must focus on z itself to maintain $z_{\rightarrow}=0^{n/2}$, but must accomplish boosting on Z. This involves a nuanced back-and-forth between z and Z, like how the query complexity proof considers $T(z)$ even though T was chosen to work on Z.

2.2 The lifting lemma

We use the technical centerpiece of [GLMWZ16]. To state it, we need some definitions. Assume $h=100\log n$ and $m\le n$. Let $S=\{0,1\}^h\times\{0,1\}^h$ and $S^m=(\{0,1\}^h)^m\times(\{0,1\}^h)^m$. Define $g:S\to\{0,1\}$ by $g(x,y)=(x\cdot y) \bmod 2$, and define $g^m:S^m\to\{0,1\}^m$ by $g^m(x,y)=\big(g(x_1,y_1),\dots,g(x_m,y_m)\big)$. For any rectangle $R\subseteq S^m$ and $z\in\{0,1\}^m$, define $R_z=\big\{(x,y)\in R\,:\,g^m(x,y)=z\big\}$. A rectangle $R\subseteq S^m$ is *balanced* iff for each z, $|R_z|$ is within a factor 1.01 of $|R|/2^m$. A basic fact is that S^m itself is balanced, since $|S_1|=(1-2^{-h})|S|/2$ and so for every z, $|S^m_z|=|S_{z_1}|\cdots|S_{z_m}|$ and $|S^m|/2^m=(|S|/2)^m$ are within a factor $1/(1-2^{-h})^m\le 1/(1-m2^{-h})\le 1/(1-n2^{-100\log n})=1/(1-n^{-99})\le 1.01$.

A *structure* of *width* w is a triple of partial assignments $(a,b,c)\in(\{0,1,*\}^h)^m\times(\{0,1,*\}^h)^m\times\{0,1,*\}^m$ (where $*$ means unassigned) such that for w many $i\in[m]$, (a_i,b_i,c_i) is totally assigned and $g(a_i,b_i)=c_i$, and for all other $i\in[m]$, (a_i,b_i,c_i) is totally unassigned. Let $S^{a,b}\subseteq S^m$ be the rectangle of all (x,y) that agree with (a,b), and note that $g^m(S^{a,b})\subseteq\{0,1\}^m$ is the set of all z that agree with c. A rectangle $R\subseteq S^m$ is (a,b,c)-*balanced* iff $R\subseteq S^{a,b}$ and for each z that agrees with c, $|R_z|$ is within a factor 1.01 of $|R|/2^{m-w}$.

Lemma 3 ([GLMWZ16]). *For every rectangle $R\subseteq S^m$ and $z\in\{0,1\}^m$ with $|R_z|\ge 2^{-k}|S^m_z|$, there exists a set $\mathcal{Q}$ of pairwise disjoint subrectangles of R such that $\sum_{Q\in\mathcal{Q}}|Q_z|\ge 0.99|R_z|$ and for each $Q\in\mathcal{Q}$ there exists a structure (a,b,c) of width $w\le k+8$ such that z agrees with c, Q is (a,b,c)-balanced, and $|Q_z|\ge 2^{-(k+8-w)}|S^{a,b}_z|$.*

(Note to readers familiar with the "packing algorithm" in [GLMWZ16]: A tiny tweak is needed to get Lemma 3 as stated. The proof in [GLMWZ16] yields $|Q_z|\ge 2^{-(k-10w\log n)}|S^{a,b}_z|$ if $w>0$ (and we drop the insignificant factor $10\log n$ for the sake of tidiness) and $|Q_z|\ge 2^{-(k+8+\log n)}|S^m_z|$ if $w=0$, which can only happen for one Q, namely the remaining rectangle at the end of the top level of the packing algorithm. To get rid of the $+\log n$ for that pesky Q, we just halt the top level partitioning and discard the remaining Q when $|Q_z|<2^{-8}|R_z|$. This only contributes $2^{-8}<0.005$ to the algorithm's error parameter, which we set as $\varepsilon=0.01$.)

More notation: For any $z\in\{0,1\}^m$ and set of indices $I\subseteq[m]$, let z^I be z but with the bits indexed by I flipped. For any rectangle $R\subseteq S^m$ and set $\mathcal{I}$ of sets of indices, let $R_{z^{\mathcal{I}}}=\bigcup_{I\in\mathcal{I}}R_{z^I}$. See Figure 2.

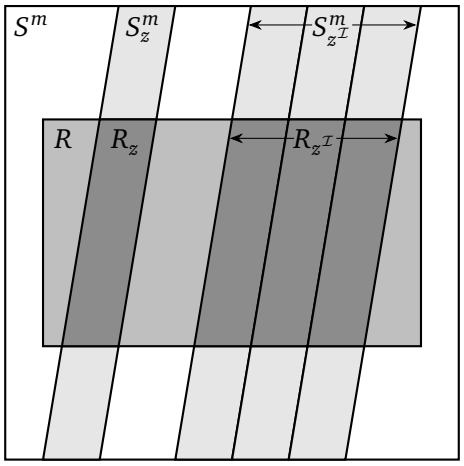

Figure 2: Illustration of R_z and $R_{z^{\mathcal{I}}}$

3 ZPP $\not\subseteq$ psP

We prove Theorem 1. For $z \in \{0,1\}^n$, let $|z|$ be z's weight (number of 1s), and let $z_{\leftarrow} = z_1 \cdots z_{n/2}$ and $z_{\rightarrow} = z_{n/2+1} \cdots z_n$ be z's left and right halves. Define $f : \{0,1\}^n \to \{0,1,\perp\}$ by:

$$f(z) = \begin{cases} 1 & \text{if } |z_{\rightarrow}| \geq n/3 \text{ and } |z_{\leftarrow}| = 0 \\ 0 & \text{if } |z_{\leftarrow}| \geq n/3 \text{ and } |z_{\rightarrow}| = 0 \end{cases}$$

With the setup from §2.2, define $F : S^n \to \{0,1,\perp\}$ by $F(x,y) = f(g^n(x,y))$.

$F \in$ ZPP: We have $F \in$ RP by the randomized protocol that picks a uniformly random $i \in \{n/2+1,\ldots,n\}$ and computes and outputs $g(x_i, y_i)$. We have $\overline{F} \in$ RP by the randomized protocol that picks a uniformly random $i \in \{1,\ldots,n/2\}$ and computes and outputs $g(x_i, y_i)$.

$F \notin$ psP: Suppose for contradiction that some total function $F' : S^n \to \{0,1\}$ that agrees with F has a randomized protocol D of cost $d = 0.01\sqrt{n}$ that's been amplified to have two-sided error probability 0.01 instead of 1/3. Let $F_1 = F^{-1}(1)$ and $F_0 = F^{-1}(0)$ and $F'_1 = F'^{-1}(1)$ and $F'_0 = F'^{-1}(0)$. Let $z = 0^n$ and assume $|F'_1 \cap S^n_z| \geq 0.5|S^n_z|$. A symmetric argument handles the case $|F'_0 \cap S^n_z| \geq 0.5|S^n_z|$.

We describe a process that iteratively updates $z \in \{0,1\}^n$, a structure (a,b,c) of width w, a rectangle $R \subseteq S^n$, and $k \geq 0$, maintaining these invariants:

$$|z_{\rightarrow}| = 0 \qquad z \text{ agrees with } c \qquad R \text{ is } (a,b,c)\text{-balanced} \qquad |R_z| \geq 2^{-k}|S^{a,b}_z| \qquad |F'_1 \cap R_z| \geq 0.5|R_z|$$

Initially, $z = 0^n$, (a,b,c) is all $*$s, $w = 0$, $R = S^n$, and $k = 0$. Each iteration extends (a,b,c) and shrinks R to a subrectangle. Each iteration is either *safe*, in which case $\sqrt{n}$ many 0s flip to 1s in $z_{\leftarrow}$ and k increases by $\leq d + 13$, or *unsafe*, in which case z doesn't change and k decreases by $\geq$ (increase in w)$/2 > 0$. This continues until $|z_{\leftarrow}| \geq n/3$, in other words, $(n/3)/\sqrt{n} = \sqrt{n}/3$ safe iterations. Thus at the end, we have $f(z) = 0$ and therefore $R_z \subseteq F_0 \subseteq F'_0$, contradicting the invariant $|F'_1 \cap R_z| \geq 0.5|R_z| > 0$. Since the safe iterations increase k by $\leq (d+13)\sqrt{n}/3$ in total, and the unsafe iterations decrease k by $\geq w/2$ in total, and since $k \geq 0$, we always have $w/2 \leq (d+13)\sqrt{n}/3$, which implies $w \leq 0.02n$ since $d = 0.01\sqrt{n}$.

We now describe an iteration. Since $c_i \neq *$ for $\leq w \leq 0.02n$ many $i \leq n/2$, and $z_i = 1$ for $\leq n/3 + \sqrt{n}$ many $i \leq n/2$, we have $c_i = *$ and $z_i = 0$ for $\geq n/2 - 0.02n - (n/3 + \sqrt{n}) \geq 0.1n$ many $i \leq n/2$. Let $\mathcal{I}$ be the set of all sets $I \subseteq \{i \leq n/2 : c_i = * \text{ and } z_i = 0\}$ with $|I| = \sqrt{n}$.

Since D is a 0.01-error randomized protocol for F', there exists a deterministic protocol P in the support of D such that $P(x,y) \neq F'(x,y)$ with probability ≤ 0.01 over (x,y) sampled from the uniform mixture of the uniform distribution over R_z and the uniform distribution over $R_{z^{\mathcal{I}}}$. Hence $P(x,y) \neq F'(x,y)$ for $\leq 0.02|R_z|$ many $(x,y) \in R_z$ and for $\leq 0.02|R_{z^{\mathcal{I}}}|$ many $(x,y) \in R_{z^{\mathcal{I}}}$. Let $P_1 = P^{-1}(1)$ and $P_0 = P^{-1}(0)$. Since P has depth d, $P_1 \cap R$ is partitioned into at most 2^d rectangles $R^1, R^2, R^3, \ldots$. Say ℓ is *major* if $|R^\ell_z| \geq 2^{-(d+4)}|R_z|$ and *minor* otherwise. For each major ℓ, we have $|R^\ell_z| \geq 2^{-(k+d+4)}|S^{a,b}_z|$, so by Lemma 3 (applied to the projections of R^ℓ and z to the $*$ coordinates, with $m = n-w$), there exists a set $\mathcal{Q}^\ell$ of pairwise disjoint subrectangles of R^ℓ such that $\sum_{Q\in\mathcal{Q}^\ell} |Q_z| \geq 0.99|R^\ell_z|$ and for each $Q \in \mathcal{Q}^\ell$ there exists a structure (a',b',c') of width w' extending (a,b,c) such that z agrees with c', Q is (a',b',c')-balanced, and $|Q_z| \geq 2^{-((k+d+4)+8-(w'-w))}|S^{a',b'}_z|$. We have

$$\begin{aligned} |F'_1 \cap P_0 \cap R_z| &\leq 0.02|R_z| \\ \textstyle\sum_{\text{minor } \ell} |R^\ell_z| &\leq 2^d \cdot 2^{-(d+4)}|R_z| \leq 0.07|R_z| \\ \textstyle\sum_{\text{major } \ell} \big(|R^\ell_z| - \sum_{Q\in\mathcal{Q}^\ell} |Q_z|\big) &\leq \textstyle\sum_{\text{major } \ell} 0.01|R^\ell_z| \leq 0.01|R_z| \end{aligned}$$

and thus, letting $\mathcal{Q} = \bigcup_{\text{major } \ell} \mathcal{Q}^\ell$:

$$\begin{aligned} \textstyle\sum_{Q\in\mathcal{Q}} |Q_z| &= |(F'_1 \cup P_1) \cap R_z| - |F'_1 \cap P_0 \cap R_z| - \textstyle\sum_{\text{minor } \ell} |R^\ell_z| - \sum_{\text{major } \ell} \big(|R^\ell_z| - \sum_{Q\in\mathcal{Q}^\ell} |Q_z|\big) \\ &\geq 0.5|R_z| - 0.02|R_z| - 0.07|R_z| - 0.01|R_z| \\ &= 0.4|R_z| \end{aligned}$$

Say $Q \in \mathcal{Q}$ is *good* if $w' - w \leq 3d$ (for the w' associated with Q) and *bad* otherwise. This iteration is *safe* if $\sum_{\text{good } Q\in\mathcal{Q}} |Q_z| \geq 0.2|R_z|$ and *unsafe* otherwise, in which case $\sum_{\text{bad } Q\in\mathcal{Q}} |Q_z| \geq 0.2|R_z|$.

Unsafe iteration: We have

$$\textstyle\sum_{\text{bad } Q\in\mathcal{Q}} |F'_0 \cap Q_z| \leq |F'_0 \cap P_1 \cap R_z| \leq 0.02|R_z| \leq 0.1 \sum_{\text{bad } Q\in\mathcal{Q}} |Q_z|$$

so there exists a bad $Q \in \mathcal{Q}$ with associated (a',b',c') and w' such that $|F'_0 \cap Q_z| \leq 0.1|Q_z| \leq 0.5|Q_z|$, so $|F'_1 \cap Q_z| \geq 0.5|Q_z|$. We conclude the iteration by updating $(a,b,c) \leftarrow (a',b',c')$ and $w \leftarrow w'$ and $R \leftarrow Q$ and $k \leftarrow k + d + 12 - (w' - w)$. The invariants are maintained. As we wanted for an unsafe iteration, z doesn't change and k decreases by (increase in w) $- d - 12 \geq$ (increase in w)$/2$ since (increase in w) $> 3d$ since Q is bad.

Safe iteration: For each good $Q \in \mathcal{Q}$ with associated (a',b',c') and w', if we sample a uniformly random $I \in \mathcal{I}$ and a uniformly random permutation of I's elements, then

$$\begin{aligned} \mathbf{Pr}[z^I \text{ doesn't agree with } c'] &= \mathbf{Pr}\big[(\exists i \in I) : c'_i = 0\big] \\ &= \mathbf{Pr}\big[(\exists i : c_i = * \text{ and } c'_i = 0)\ (\exists e \in [\sqrt{n}]) : I\text{'s } e\text{th element is } i\big] \\ &\leq \textstyle\sum_{i : c_i = * \text{ and } c'_i = 0} \sum_{e\in[\sqrt{n}]} \mathbf{Pr}[I\text{'s } e\text{th element is } i] \\ &\leq (w' - w) \cdot \sqrt{n} \cdot 1/0.1n \\ &\leq 3d \cdot 10/\sqrt{n} \\ &= 0.3 \end{aligned}$$

since I's eth element is uniformly distributed over a set of $\geq 0.1n$ many i, and since $w' - w \leq 3d$ since Q is good. If z^I agrees with c', then $|Q_{z^I}| \geq 0.99|Q|/2^{n-w'} \geq 0.98|Q_z|$ since z agrees with c' and Q is (a',b',c')-balanced. Thus:

$$|Q_{z^{\mathcal{I}}}| = \textstyle\sum_{I\in\mathcal{I}} |Q_{z^I}| \geq \sum_{I\in\mathcal{I} : z^I \text{ agrees with } c'} |Q_{z^I}| \geq 0.7|\mathcal{I}| \cdot 0.98|Q_z| \geq 0.6|\mathcal{I}| \cdot |Q_z|$$

It follows that:

$$\sum_{\text{good } Q\in\mathcal{Q}} |Q_{z^{\mathcal{I}}}| \;\geq\; 0.6|\mathcal{I}| \sum_{\text{good } Q\in\mathcal{Q}} |Q_z| \;\geq\; 0.6|\mathcal{I}| \cdot 0.2|R_z| \;=\; 0.12|\mathcal{I}| \cdot |R_z|$$

We have $|R_z| \geq 0.99|R|/2^{n-w} \geq 0.98|R_{z^I}|$ for each $I \in \mathcal{I}$ since z and z^I agree with c and R is (a,b,c)-balanced, so:

$$|R_z| \;\geq\; 0.98 \sum_{I\in\mathcal{I}} |R_{z^I}|/|\mathcal{I}| \;=\; 0.98|R_{z^{\mathcal{I}}}|/|\mathcal{I}|$$

It follows that:

$$\sum_{\text{good } Q\in\mathcal{Q}} |Q_{z^{\mathcal{I}}}| \;\geq\; 0.12|\mathcal{I}| \cdot |R_z| \;\geq\; 0.12 \cdot 0.98|R_{z^{\mathcal{I}}}| \;\geq\; 0.1|R_{z^{\mathcal{I}}}|$$

We have

$$\sum_{\text{good } Q\in\mathcal{Q}} |F_0' \cap Q_{z^{\mathcal{I}}}| \;\leq\; |F_0' \cap P_1 \cap R_{z^{\mathcal{I}}}| \;\leq\; 0.02|R_{z^{\mathcal{I}}}| \;\leq\; 0.2 \sum_{\text{good } Q\in\mathcal{Q}} |Q_{z^{\mathcal{I}}}|$$

so there exists a good $Q \in \mathcal{Q}$ with associated (a',b',c') and w' such that $|F_0' \cap Q_{z^{\mathcal{I}}}| \leq 0.2|Q_{z^{\mathcal{I}}}| \leq 0.5|Q_{z^{\mathcal{I}}}|$, so $|F_1' \cap Q_{z^{\mathcal{I}}}| \geq 0.5|Q_{z^{\mathcal{I}}}|$. Hence there exists an $I \in \mathcal{I}$ such that $|F_1' \cap Q_{z^I}| \geq 0.5|Q_{z^I}|$ and z^I agrees with c' (since $Q_{z^I} = \emptyset$ if z^I doesn't agree with c'). Also:

$$|Q_{z^I}| \;\geq\; 0.98|Q_z| \;\geq\; 0.98 \cdot 2^{-(k+d+12)}|S_z^{a',b'}| \;\geq\; 0.98 \cdot 2^{-(k+d+12)} \cdot 0.98|S_{z^I}^{a',b'}| \;\geq\; 2^{-(k+d+13)}|S_{z^I}^{a',b'}|$$

We conclude the iteration by updating $z \leftarrow z^I$ and $(a,b,c) \leftarrow (a',b',c')$ and $w \leftarrow w'$ and $R \leftarrow Q$ and $k \leftarrow k+d+13$. The invariants are maintained. As we wanted for a safe iteration, $\sqrt{n}$ many 0s flip to 1s in $z_{\leftarrow}$ and k increases by $\leq d+13$.

4 $\mathsf{MA} \not\subseteq \mathsf{NP}^{\mathsf{BPP}}$

We prove Theorem 2. For $z \in \{0,1\}^n$, let $|z|$ be z's weight (number of 1s), and let $z_{\leftarrow} = z_1 \cdots z_{n/2}$ and $z_{\rightarrow} = z_{n/2+1} \cdots z_n$ be z's left and right halves. Define $f\colon \{0,1\}^n \to \{0,1,\perp\}$ by:

$$f(z) \;=\; \begin{cases} 1 & \text{if } |z_{\leftarrow}| = n/2 \quad \text{or} \quad |z_{\rightarrow}| > 0 \\ 0 & \text{if } |z_{\leftarrow}| \leq n/6 \text{ and } |z_{\rightarrow}| = 0 \end{cases}$$

With the setup from §2.2, define $F\colon S^n \to \{0,1,\perp\}$ by $F(x,y) = f(g^n(x,y))$.

$F \in \mathsf{MA}$: Consider the randomized protocol that picks a uniformly random $i \in \{1,\ldots,n/2\}$ and computes and outputs $g(x_i,y_i)$, and for each $i \in \{n/2+1,\ldots,n\}$ consider the deterministic protocol that computes and outputs $g(x_i,y_i)$. This set of $n/2+1$ protocols is an MA-type protocol of cost $O(\log n)$ for F: If $F(x,y)=1$ then at least one of these protocols outputs 1 with probability $1 \geq 2/3$, and if $F(x,y)=0$ then each of these protocols outputs 1 with probability $\leq 1/3$.

$F \notin \mathsf{NP}^{\mathsf{BPP}} = \mathsf{N}\cdot\mathsf{BPP}$: Suppose for contradiction F has an $\mathsf{N}\cdot\mathsf{BPP}$-type protocol $\mathcal{D}$ of cost $d = 0.01\sqrt{n}$ where the BPP part has been amplified to have error probability 0.01 instead of 1/3. The proof has a *preprocessing phase* and an *iterative phase*. For $z_{\leftarrow}$, we use the notation i, I, $\mathcal{I}$ for indices, sets of indices, and sets of sets of indices. For $z_{\rightarrow}$, we use the notation j, J, $\mathcal{J}$ for indices, sets of indices, and sets of sets of indices.

Preprocessing phase: For $z = 1^{n/2}0^{n/2}$ we have $f(z) = 1$, so $F(x,y) = 1$ for all $(x,y) \in S^n_z$. Since $|\mathcal{D}| \le 2^d$, there exists a $D \in \mathcal{D}$ such that $D(x,y) \ge 0.99$ for $\ge 2^{-d}|S^n_z|$ many $(x,y) \in S^n_z$. Define F' to have the same valid inputs as F, and such that D is a 0.01-error randomized protocol for F'. Let $F_1 = F^{-1}(1)$ and $F_0 = F^{-1}(0)$ and $F'_1 = F'^{-1}(1)$ and $F'_0 = F'^{-1}(0)$. Thus $|F'_1 \cap S^n_z| \ge 2^{-d}|S^n_z|$ and $F_1 \subseteq F'_1 \cup F'_0$ and $F_0 \subseteq F'_0$.

Let D' be the further amplified version of D that outputs the majority vote of $2d$ independent runs of D, so D' is a $0.01 \cdot 2^{-d}$-error randomized protocol for F' of cost $2d^2$. There exists a deterministic protocol P in the support of D' such that $P(x,y) \ne F'(x,y)$ with probability $\le 0.01 \cdot 2^{-d}$ over (x,y) sampled from the uniform mixture of the uniform distribution over S^n_z and the uniform distribution over $S^n_{z^{\mathcal{J}}}$ where $\mathcal{J} = \big\{\{n/2+1\}, \ldots, \{n\}\big\}$, noting that $S^n_z \cup S^n_{z^{\mathcal{J}}} \subseteq F_1 \subseteq F'_1 \cup F'_0$. Hence $P(x,y) \ne F'(x,y)$ for $\le 0.02 \cdot 2^{-d}|S^n_z|$ many $(x,y) \in S^n_z$ and for $\le 0.02 \cdot 2^{-d}|S^n_{z^{\mathcal{J}}}|$ many $(x,y) \in S^n_{z^{\mathcal{J}}}$. Let $P_1 = P^{-1}(1)$ and $P_0 = P^{-1}(0)$. Since P has depth $2d^2$, P_1 is partitioned into at most 2^{2d^2} rectangles $R^1, R^2, R^3, \ldots$. Say ℓ is *major* if $|R^\ell_z| \ge 2^{-(d+2d^2+4)}|S^n_z|$ and *minor* otherwise. For each major ℓ, by Lemma 3 (with $m = n$), there exists a set $\mathcal{Q}^\ell$ of pairwise disjoint subrectangles of R^ℓ such that $\sum_{Q \in \mathcal{Q}^\ell} |Q_z| \ge 0.99|R^\ell_z|$ and for each $Q \in \mathcal{Q}^\ell$ there exists a structure (a,b,c) of width $w \le d + 2d^2 + 12 \le 0.01n$ such that z agrees with c, Q is (a,b,c)-balanced, and $|Q_z| \ge 2^{-(d+2d^2+12-w)}|S^{a,b}_z|$. We have

$$\begin{aligned}
|F'_1 \cap P_0 \cap S^n_z| &\le 0.02 \cdot 2^{-d}|S^n_z| \le 0.02|F'_1 \cap S^n_z| \\
\textstyle\sum_{\text{minor } \ell} |R^\ell_z| &\le 2^{2d^2} \cdot 2^{-(d+2d^2+4)}|S^n_z| \le 0.07 \cdot 2^{-d}|S^n_z| \le 0.07|F'_1 \cap S^n_z| \\
\textstyle\sum_{\text{major } \ell}\big(|R^\ell_z| - \sum_{Q \in \mathcal{Q}^\ell} |Q_z|\big) &\le \textstyle\sum_{\text{major } \ell} 0.01|R^\ell_z| \le 0.01|P_1 \cap S^n_z|
\end{aligned}$$

and thus, letting $\mathcal{Q} = \bigcup_{\text{major } \ell} \mathcal{Q}^\ell$:

$$\begin{aligned}
\textstyle\sum_{Q \in \mathcal{Q}} |Q_z| &= |(F'_1 \cup P_1) \cap S^n_z| - |F'_1 \cap P_0 \cap S^n_z| - \textstyle\sum_{\text{minor } \ell} |R^\ell_z| - \sum_{\text{major } \ell}\big(|R^\ell_z| - \sum_{Q \in \mathcal{Q}^\ell} |Q_z|\big) \\
&\ge |(F'_1 \cup P_1) \cap S^n_z|(1 - 0.02 - 0.07 - 0.01) \\
&\ge 0.9|F'_1 \cap S^n_z| \\
&\ge 0.9 \cdot 2^{-d}|S^n_z|
\end{aligned}$$

For each $Q \in \mathcal{Q}$ with associated (a,b,c) and w, and for $J = \{j\} \in \mathcal{J}$, z^J agrees with c iff $c_j = *$, which holds for $\ge n/2 - w \ge 0.98|\mathcal{J}|$ many $J \in \mathcal{J}$. If z^J agrees with c, then $|Q_{z^J}| \ge 0.99|Q|/2^{n-w} \ge 0.98|Q_z|$ since z agrees with c and Q is (a,b,c)-balanced. Thus:

$$|Q_{z^{\mathcal{J}}}| = \textstyle\sum_{J \in \mathcal{J}} |Q_{z^J}| \ge \sum_{J \in \mathcal{J} : z^J \text{ agrees with } c} |Q_{z^J}| \ge 0.98|\mathcal{J}| \cdot 0.98|Q_z| \ge 0.9|\mathcal{J}| \cdot |Q_z|$$

It follows that:

$$\textstyle\sum_{Q \in \mathcal{Q}} |Q_{z^{\mathcal{J}}}| \ge 0.9|\mathcal{J}| \sum_{Q \in \mathcal{Q}} |Q_z| \ge 0.9|\mathcal{J}| \cdot 0.9 \cdot 2^{-d}|S^n_z| \ge 0.8|\mathcal{J}| \cdot 2^{-d}|S^n_z|$$

We have $|S^n_z| \ge 0.99|S^n|/2^n \ge 0.98|S^n_{z^J}|$ for each $J \in \mathcal{J}$ since S^n is balanced, so:

$$|S^n_z| \ge 0.98 \textstyle\sum_{J \in \mathcal{J}} |S^n_{z^J}|/|\mathcal{J}| = 0.98|S^n_{z^{\mathcal{J}}}|/|\mathcal{J}|$$

It follows that:

$$\textstyle\sum_{Q \in \mathcal{Q}} |Q_{z^{\mathcal{J}}}| \ge 0.8|\mathcal{J}| \cdot 2^{-d}|S^n_z| \ge 0.8 \cdot 2^{-d} \cdot 0.98|S^n_{z^{\mathcal{J}}}| \ge 0.7 \cdot 2^{-d}|S^n_{z^{\mathcal{J}}}|$$

We have

$$\textstyle\sum_{Q \in \mathcal{Q}} |F'_0 \cap Q_{z^{\mathcal{J}}}| \le |F'_0 \cap P_1 \cap S^n_{z^{\mathcal{J}}}| \le 0.02 \cdot 2^{-d}|S^n_{z^{\mathcal{J}}}| \le 0.03 \sum_{Q \in \mathcal{Q}} |Q_{z^{\mathcal{J}}}|$$

so there exists a $Q \in \mathcal{Q}$ such that $|F_0' \cap Q_{z^{\mathcal{J}}}| \le 0.03|Q_{z^{\mathcal{J}}}| \le 0.3|Q_{z^{\mathcal{J}}}|$, so $|F_1' \cap Q_{z^{\mathcal{J}}}| \ge 0.7|Q_{z^{\mathcal{J}}}|$. Define R to be this Q, with associated (a,b,c) and w, and redefine $\mathcal{J} = \big\{\{j\} : j > n/2 \text{ and } c_j = *\big\}$, which doesn't change $R_{z^{\mathcal{J}}}$ since R is (a,b,c)-balanced. In summary, letting $k = 3d^2 - w$:

$$z = 1^{n/2}0^{n/2} \qquad z \text{ agrees with } c \qquad R \text{ is } (a,b,c)\text{-balanced} \qquad |R_z| \ge 2^{-k}|S_z^{a,b}| \qquad |F_1' \cap R_{z^{\mathcal{J}}}| \ge 0.7|R_{z^{\mathcal{J}}}|$$

Iterative phase: We describe a process that iteratively updates $z \in \{0,1\}^n$, a structure (a,b,c) of width w, a rectangle $R \subseteq S^n$, and $k \ge 0$, maintaining these invariants, where $\mathcal{J} = \big\{\{j\} : j > n/2 \text{ and } c_j = *\big\}$:

$$|z_{\rightarrow}| = 0 \qquad z \text{ agrees with } c \qquad R \text{ is } (a,b,c)\text{-balanced} \qquad |R_z| \ge 2^{-k}|S_z^{a,b}| \qquad |F_1' \cap R_{z^{\mathcal{J}}}| \ge 0.7|R_{z^{\mathcal{J}}}|$$

The initial $z = 1^{n/2}0^{n/2}$, (a,b,c), w, R, and $k = 3d^2 - w$ are from the end of the preprocessing phase. Each iteration extends (a,b,c) and shrinks R to a subrectangle. Each iteration is either *safe*, in which case $\sqrt{n}$ many 1s flip to 0s in $z_{\leftarrow}$ and k increases by $\le d + 13$, or *unsafe*, in which case z doesn't change and k decreases by $\ge$ (increase in w)$/2 > 0$. This continues until $|z_{\leftarrow}| \le n/6$, in other words $(n/3)/\sqrt{n} = \sqrt{n}/3$ safe iterations. Thus at the end, we have $f(z) = 0$ and therefore $R_z \subseteq F_0 \subseteq F_0'$, which leads to a contradiction with $|F_1' \cap R_{z^{\mathcal{J}}}| \ge 0.7|R_{z^{\mathcal{J}}}|$, as we show at the end of the proof. Since the preprocessing and safe iterations increase k by $\le 3d^2 + (d+13)\sqrt{n}/3$ in total, and the preprocessing and unsafe iterations decrease k by $\ge w/2$ in total, and since $k \ge 0$, we always have $w/2 \le 3d^2 + (d+13)\sqrt{n}/3$, which implies $w \le 0.02n$ since $d = 0.01\sqrt{n}$.

A key issue is that to maintain the invariant $|F_1' \cap R_{z^{\mathcal{J}}}| \ge 0.7|R_{z^{\mathcal{J}}}|$, we must consider the behavior of subrectangles with respect to $z^{\mathcal{J}}$, but to maintain the invariant $|z_{\rightarrow}| = 0$, we must apply Lemma 3 with respect to z. Reconciling this involves a subtle back-and-forth between R_z and $R_{z^{\mathcal{J}}}$.

We now describe an iteration. Since $c_i \ne *$ for $\le w \le 0.02n$ many $i \le n/2$, and $z_i = 0$ for $\le n/3$ many $i \le n/2$, we have $c_i = *$ and $z_i = 1$ for $\ge n/2 - 0.02n - n/3 \ge 0.1n$ many $i \le n/2$. Let $\mathcal{I}$ be the set of all sets $I \subseteq \{i \le n/2 : c_i = * \text{ and } z_i = 1\}$ with $|I| = \sqrt{n}$. We have $c_j \ne *$ for $\le w \le 0.02n$ many $j > n/2$, and $\mathcal{J}$ is the set of all sets $J \subseteq \{j > n/2 : c_j = *\}$ with $|J| = 1$. Let $\mathcal{I} \times \mathcal{J} = \{I \cup J : I \in \mathcal{I} \text{ and } J \in \mathcal{J}\}$. Note that $R_z \cup R_{z^{\mathcal{I}}}$ generally consists of invalid inputs (on which we know nothing a priori about D's behavior), but $R_{z^{\mathcal{J}}} \cup R_{z^{\mathcal{I}\times\mathcal{J}}} \subseteq F_1 \subseteq F_1' \cup F_0'$.

Since D is a 0.01-error randomized protocol for F', there exists a deterministic protocol P in the support of D such that $P(x,y) \ne F'(x,y)$ with probability ≤ 0.01 over (x,y) sampled from the uniform mixture of the uniform distribution over $R_{z^{\mathcal{J}}}$ and the uniform distribution over $R_{z^{\mathcal{I}\times\mathcal{J}}}$. Hence $P(x,y) \ne F'(x,y)$ for $\le 0.02|R_{z^{\mathcal{J}}}|$ many $(x,y) \in R_{z^{\mathcal{J}}}$ and for $\le 0.02|R_{z^{\mathcal{I}\times\mathcal{J}}}|$ many $(x,y) \in R_{z^{\mathcal{I}\times\mathcal{J}}}$. Let $P_1 = P^{-1}(1)$ and $P_0 = P^{-1}(0)$. Since P has depth d, $P_1 \cap R$ is partitioned into at most 2^d rectangles $R^1, R^2, R^3, \ldots$. Say ℓ is *major* if $|R_z^\ell| \ge 2^{-(d+4)}|R_z|$ and *minor* otherwise. For each major ℓ, we have $|R_z^\ell| \ge 2^{-(k+d+4)}|S_z^{a,b}|$, so by Lemma 3 (applied to the projections of R^ℓ and z to the $*$ coordinates, with $m = n - w$), there exists a set $\mathcal{Q}^\ell$ of pairwise disjoint subrectangles of R^ℓ such that $\sum_{Q\in\mathcal{Q}^\ell} |Q_z| \ge 0.99|R_z^\ell|$ and for each $Q \in \mathcal{Q}^\ell$ there exists a structure (a',b',c') of width w' extending (a,b,c) such that z agrees with c', Q is (a',b',c')-balanced, and $|Q_z| \ge 2^{-((k+d+4)+8-(w'-w))}|S_z^{a',b'}|$. The latter bound implies $w' \le k + d + 12 + w \le 0.04n$. We have

$$\begin{aligned} \textstyle\sum_{\text{minor } \ell} |R_z^\ell| &\le 2^d \cdot 2^{-(d+4)}|R_z| \le 0.07|R_z| \\ \textstyle\sum_{\text{major } \ell} \big(|R_z^\ell| - \sum_{Q\in\mathcal{Q}^\ell} |Q_z|\big) &\le \textstyle\sum_{\text{major } \ell} 0.01|R_z^\ell| \le 0.01|R_z| \end{aligned}$$

and thus, letting $\mathcal{Q} = \bigcup_{\text{major } \ell} \mathcal{Q}^\ell$:

$$\textstyle\sum_{Q\in\mathcal{Q}} |Q_z| = |P_1 \cap R_z| - \sum_{\text{minor } \ell} |R_z^\ell| - \sum_{\text{major } \ell} \big(|R_z^\ell| - \sum_{Q\in\mathcal{Q}^\ell} |Q_z|\big) \ge |P_1 \cap R_z| - 0.08|R_z| \qquad (\star)$$

For each $Q \in \mathcal{Q}$ with associated (a', b', c') and w', and for $J = \{j\} \in \mathcal{J}$, z^J agrees with c' iff $c'_j = *$, which holds for $\geq n/2 - w' \geq 0.92(n/2) \geq 0.92|\mathcal{J}|$ many $J \in \mathcal{J}$. If z^J agrees with c', then $|Q_{z^J}| \geq 0.99|Q|/2^{n-w'} \geq 0.98|Q_z|$ since z agrees with c' and Q is (a', b', c')-balanced. Thus:

$$|Q_{z^{\mathcal{J}}}| \;=\; \textstyle\sum_{J \in \mathcal{J}} |Q_{z^J}| \;\geq\; \sum_{J \in \mathcal{J} \,:\, z^J \text{ agrees with } c'} |Q_{z^J}| \;\geq\; 0.92|\mathcal{J}| \cdot 0.98|Q_z| \;\geq\; 0.9|\mathcal{J}| \cdot |Q_z| \qquad (\dagger)$$

It follows that:

$$|P_1 \cap R_{z^{\mathcal{J}}}| \;\geq\; \textstyle\sum_{Q \in \mathcal{Q}} |Q_{z^{\mathcal{J}}}| \;\geq\; 0.9|\mathcal{J}| \sum_{Q \in \mathcal{Q}} |Q_z| \;\geq\; 0.9|\mathcal{J}|\big(|P_1 \cap R_z| - 0.08|R_z|\big)$$

By the symmetry between outputting 1 and outputting 0, we also have:

$$|P_0 \cap R_{z^{\mathcal{J}}}| \;\geq\; 0.9|\mathcal{J}|\big(|P_0 \cap R_z| - 0.08|R_z|\big)$$

We have $|R_z| \geq 0.99|R|/2^{n-w} \geq 0.98|R_{z^J}|$ for each $J \in \mathcal{J}$ since R is (a, b, c)-balanced, so:

$$|R_z| \;\geq\; 0.98 \textstyle\sum_{J \in \mathcal{J}} |R_{z^J}|/|\mathcal{J}| \;=\; 0.98|R_{z^{\mathcal{J}}}|/|\mathcal{J}| \qquad (\ddagger)$$

It follows that

$$|P_0 \cap R_{z^{\mathcal{J}}}| \;\geq\; 0.9|\mathcal{J}|\big(|P_0 \cap R_z|/|R_z| - 0.08\big)|R_z| \;\geq\; 0.8\big(|P_0 \cap R_z|/|R_z| - 0.08\big)|R_{z^{\mathcal{J}}}|$$

and thus:

$$|F'_0 \cap R_{z^{\mathcal{J}}}| \;\geq\; |P_0 \cap R_{z^{\mathcal{J}}}| - |F'_1 \cap P_0 \cap R_{z^{\mathcal{J}}}| \;\geq\; 0.8\big(|P_0 \cap R_z|/|R_z| - 0.08\big)|R_{z^{\mathcal{J}}}| - 0.02|R_{z^{\mathcal{J}}}|$$

The invariant $|F'_1 \cap R_{z^{\mathcal{J}}}| \geq 0.7|R_{z^{\mathcal{J}}}|$ implies $|F'_0 \cap R_{z^{\mathcal{J}}}| \leq 0.3|R_{z^{\mathcal{J}}}|$, so combining yields:

$$0.3 \;\geq\; 0.8\big(|P_0 \cap R_z|/|R_z| - 0.08\big) - 0.02 \;\geq\; 0.8|P_0 \cap R_z|/|R_z| - 0.1$$

Rearranging then yields $|P_0 \cap R_z| \leq 0.5|R_z|$, so $|P_1 \cap R_z| \geq 0.5|R_z|$. As we showed in $(\star)$, this implies

$$\textstyle\sum_{Q \in \mathcal{Q}} |Q_z| \;\geq\; |P_1 \cap R_z| - 0.08|R_z| \;\geq\; 0.5|R_z| - 0.08|R_z| \;\geq\; 0.4|R_z|$$

Say $Q \in \mathcal{Q}$ is *good* if $w' - w \leq 3d$ (for the w' associated with Q) and *bad* otherwise. This iteration is *safe* if $\sum_{\text{good } Q \in \mathcal{Q}} |Q_z| \geq 0.2|R_z|$ and *unsafe* otherwise, in which case $\sum_{\text{bad } Q \in \mathcal{Q}} |Q_z| \geq 0.2|R_z|$.

Unsafe iteration: As we showed in $(\dagger)$ and $(\ddagger)$:

$$\textstyle\sum_{\text{bad } Q \in \mathcal{Q}} |Q_{z^{\mathcal{J}}}| \;\geq\; 0.9|\mathcal{J}| \sum_{\text{bad } Q \in \mathcal{Q}} |Q_z| \;\geq\; 0.9|\mathcal{J}| \cdot 0.2|R_z| \;\geq\; 0.9 \cdot 0.2 \cdot 0.98|R_{z^{\mathcal{J}}}| \;\geq\; 0.1|R_{z^{\mathcal{J}}}|$$

We have

$$\textstyle\sum_{\text{bad } Q \in \mathcal{Q}} |F'_0 \cap Q_{z^{\mathcal{J}}}| \;\leq\; |F'_0 \cap P_1 \cap R_{z^{\mathcal{J}}}| \;\leq\; 0.02|R_{z^{\mathcal{J}}}| \;\leq\; 0.2 \sum_{\text{bad } Q \in \mathcal{Q}} |Q_{z^{\mathcal{J}}}|$$

so there exists a bad $Q \in \mathcal{Q}$ with associated (a', b', c') and w' such that $|F'_0 \cap Q_{z^{\mathcal{J}}}| \leq 0.2|Q_{z^{\mathcal{J}}}| \leq 0.3|Q_{z^{\mathcal{J}}}|$, so $|F'_1 \cap Q_{z^{\mathcal{J}}}| \geq 0.7|Q_{z^{\mathcal{J}}}|$. We conclude the iteration by updating $(a, b, c) \leftarrow (a', b', c')$ and $w \leftarrow w'$ and $R \leftarrow Q$ and $k \leftarrow k + d + 12 - (w' - w)$ and $\mathcal{J} \leftarrow \big\{\{j\} \;:\; j > n/2 \text{ and } c'_j = *\big\}$. The invariants are maintained. As we wanted for an unsafe iteration, z doesn't change and k decreases by (increase in w) $- d - 12 \geq$ (increase in w)$/2$ since (increase in w) $> 3d$ since Q is bad.

Safe iteration: For each good $Q \in \mathcal{Q}$ with associated (a', b', c') and w', if we sample a uniformly random $I \in \mathcal{I}$ and a uniformly random permutation of I's elements, then

$$\begin{aligned}
\mathbf{Pr}[z^I \text{ doesn't agree with } c'] &= \mathbf{Pr}\big[(\exists i \in I) :\ c'_i = 1\big] \\
&= \mathbf{Pr}\big[(\exists i\ :\ c_i = * \text{ and } c'_i = 1)\ (\exists e \in [\sqrt{n}]) :\ I\text{'s } e\text{th element is } i\big] \\
&\le \textstyle\sum_{i\,:\,c_i = * \text{ and } c'_i = 1} \sum_{e \in [\sqrt{n}]} \mathbf{Pr}[I\text{'s } e\text{th element is } i] \\
&\le (w' - w) \cdot \sqrt{n} \cdot 1/0.1n \\
&\le 3d \cdot 10/\sqrt{n} \\
&= 0.3
\end{aligned}$$

since I's eth element is uniformly distributed over a set of $\ge 0.1n$ many i, and since $w' - w \le 3d$ since Q is good. If z^I agrees with c', then for $J = \{j\} \in \mathcal{J}$, $z^{I \cup J}$ agrees with c' iff $c'_j = *$, which holds for $\ge n/2 - w' \ge 0.92(n/2) \ge 0.92|\mathcal{J}|$ many $J \in \mathcal{J}$. Thus $z^{I \cup J}$ agrees with c' for $\ge 0.7|\mathcal{I}| \cdot 0.92|\mathcal{J}| \ge 0.62|\mathcal{I} \times \mathcal{J}|$ many $I \cup J \in \mathcal{I} \times \mathcal{J}$. If $z^{I \cup J}$ agrees with c', then $|Q_{z^{I \cup J}}| \ge 0.99|Q|/2^{n-w'} \ge 0.98|Q_z|$ since z agrees with c' and Q is (a', b', c')-balanced. Thus:

$$\begin{aligned}
|Q_{z^{\mathcal{I} \times \mathcal{J}}}| \ = \ \textstyle\sum_{I \cup J \in \mathcal{I} \times \mathcal{J}} |Q_{z^{I \cup J}}| \ &\ge \ \textstyle\sum_{I \cup J \in \mathcal{I} \times \mathcal{J}\,:\, z^{I \cup J} \text{ agrees with } c'} |Q_{z^{I \cup J}}| \ \ge \ 0.62|\mathcal{I} \times \mathcal{J}| \cdot 0.98|Q_z| \\
&\ge \ 0.6|\mathcal{I} \times \mathcal{J}| \cdot |Q_z|
\end{aligned}$$

It follows that:

$$\textstyle\sum_{\text{good } Q \in \mathcal{Q}} |Q_{z^{\mathcal{I} \times \mathcal{J}}}| \ \ge \ 0.6|\mathcal{I} \times \mathcal{J}| \sum_{\text{good } Q \in \mathcal{Q}} |Q_z| \ \ge \ 0.6|\mathcal{I} \times \mathcal{J}| \cdot 0.2|R_z| \ = \ 0.12|\mathcal{I} \times \mathcal{J}| \cdot |R_z|$$

We have $|R_z| \ge 0.99|R|/2^{n-w} \ge 0.98|R_{z^{I \cup J}}|$ for each $I \cup J \in \mathcal{I} \times \mathcal{J}$ since z and $z^{I \cup J}$ agree with c and R is (a, b, c)-balanced, so:

$$|R_z| \ \ge \ 0.98 \textstyle\sum_{I \cup J \in \mathcal{I} \times \mathcal{J}} |R_{z^{I \cup J}}|/|\mathcal{I} \times \mathcal{J}| \ = \ 0.98|R_{z^{\mathcal{I} \times \mathcal{J}}}|/|\mathcal{I} \times \mathcal{J}|$$

It follows that:

$$\textstyle\sum_{\text{good } Q \in \mathcal{Q}} |Q_{z^{\mathcal{I} \times \mathcal{J}}}| \ \ge \ 0.12|\mathcal{I} \times \mathcal{J}| \cdot |R_z| \ \ge \ 0.12 \cdot 0.98|R_{z^{\mathcal{I} \times \mathcal{J}}}| \ \ge \ 0.1|R_{z^{\mathcal{I} \times \mathcal{J}}}|$$

We have

$$\textstyle\sum_{\text{good } Q \in \mathcal{Q}} |F'_0 \cap Q_{z^{\mathcal{I} \times \mathcal{J}}}| \ \le \ |F'_0 \cap P_1 \cap R_{z^{\mathcal{I} \times \mathcal{J}}}| \ \le \ 0.02|R_{z^{\mathcal{I} \times \mathcal{J}}}| \ \le \ 0.2 \textstyle\sum_{\text{good } Q \in \mathcal{Q}} |Q_{z^{\mathcal{I} \times \mathcal{J}}}|$$

so there exists a good $Q \in \mathcal{Q}$ with associated (a', b', c') and w' such that $|F'_0 \cap Q_{z^{\mathcal{I} \times \mathcal{J}}}| \le 0.2|Q_{z^{\mathcal{I} \times \mathcal{J}}}| \le 0.3|Q_{z^{\mathcal{I} \times \mathcal{J}}}|$, so $|F'_1 \cap Q_{z^{\mathcal{I} \times \mathcal{J}}}| \ge 0.7|Q_{z^{\mathcal{I} \times \mathcal{J}}}|$. Hence there exists an $I \in \mathcal{I}$ such that $|F'_1 \cap Q_{(z^I)^{\mathcal{J}}}| \ge 0.7|Q_{(z^I)^{\mathcal{J}}}|$ and z^I agrees with c' (since $Q_{(z^I)^{\mathcal{J}}} = \emptyset$ if z^I doesn't agree with c'). Also:

$$|Q_{z^I}| \ \ge \ 0.98|Q_z| \ \ge \ 0.98 \cdot 2^{-(k+d+12)}|S_z^{a',b'}| \ \ge \ 0.98 \cdot 2^{-(k+d+12)} \cdot 0.98|S_{z^I}^{a',b'}| \ \ge \ 2^{-(k+d+13)}|S_{z^I}^{a',b'}|$$

We conclude the iteration by updating $z \leftarrow z^I$ and $(a, b, c) \leftarrow (a', b', c')$ and $w \leftarrow w'$ and $R \leftarrow Q$ and $k \leftarrow k + d + 13$ and $\mathcal{J} \leftarrow \big\{\{j\}\ :\ j > n/2 \text{ and } c'_j = *\big\}$. The invariants are maintained. As we wanted for a safe iteration, $\sqrt{n}$ many 1s flip to 0s in $z_{\leftarrow}$ and k increases by $\le d + 13$.

Contradiction: After the last iteration, $f(z) = 0$ and therefore $R_z \subseteq F_0 \subseteq F'_0$. Since D is a 0.01-error randomized protocol for F', there exists a deterministic protocol P in the support of D such that $P(x, y) \ne F'(x, y)$ with probability ≤ 0.01 over (x, y) sampled from the uniform mixture of the uniform distribution over R_z and the uniform distribution over $R_{z^{\mathcal{J}}}$. Hence $P(x, y) \ne F'(x, y)$ for $\le 0.02|R_z|$ many $(x, y) \in R_z$ and for $\le 0.02|R_{z^{\mathcal{J}}}|$ many $(x, y) \in R_{z^{\mathcal{J}}}$. Let $P_1 = P^{-1}(1)$ and $P_0 = P^{-1}(0)$. We argued in the iterative phase that the invariant $|F'_1 \cap R_{z^{\mathcal{J}}}| \ge 0.7|R_{z^{\mathcal{J}}}|$ and $|F'_1 \cap P_0 \cap R_{z^{\mathcal{J}}}| \le 0.02|R_{z^{\mathcal{J}}}|$ imply $|P_1 \cap R_z| \ge 0.5|R_z|$ in this case. This contradicts $|P_1 \cap R_z| = |F'_0 \cap P_1 \cap R_z| \le 0.02|R_z|$.

AI usage statement

The author did not use AI for anything.

References

[AGL26] Hugo Aaronson, Tom Gur, and Jiawei Li. Pseudo-deterministic quantum algorithms. In *Proceedings of the 53rd International Colloquium on Automata, Languages, and Programming (ICALP)*, pages 3:1–3:22. Schloss Dagstuhl, 2026. doi:10.4230/LIPICS.ICALP.2026.3 [p. 1]

[ARW17] Amir Abboud, Aviad Rubinstein, and Ryan Williams. Distributed PCP theorems for hardness of approximation in P. In *Proceedings of the 58th Symposium on Foundations of Computer Science (FOCS)*, pages 25–36. IEEE, 2017. doi:10.1109/FOCS.2017.12 [p. 2]

[AW09] Scott Aaronson and Avi Wigderson. Algebrization: A new barrier in complexity theory. *ACM Transactions on Computation Theory*, 1(1):2:1–2:54, 2009. doi:10.1145/1490270.1490272 [p. 2]

[BBGT25] Rishabh Bhadauria, Alexander Block, Prantar Ghosh, and Justin Thaler. SNARK lower bounds via communication complexity. In *Proceedings of the 23rd International Conference on Theory of Cryptography (TCC)*, pages 417–451. Springer, 2025. doi:10.1007/978-3-032-12287-2_15 [p. 2]

[BF99] Harry Buhrman and Lance Fortnow. One-sided versus two-sided error in probabilistic computation. In *Proceedings of the 16th International Symposium on Theoretical Aspects of Computer Science (STACS)*, pages 100–109. Springer, 1999. doi:10.1007/3-540-49116-3_9 [p. 3]

[BFL91] László Babai, Lance Fortnow, and Carsten Lund. Non-deterministic exponential time has two-prover interactive protocols. *Computational Complexity*, 1:3–40, 1991. doi:10.1007/BF01200056 [p. 3]

[BHHLT26] Ari Blondal, Hamed Hatami, Pooya Hatami, Chavdar Lalov, and Sivan Tretiak. Borsuk–Ulam and replicable learning of large-margin halfspaces. In *Proceedings of the 58th Symposium on Theory of Computing (STOC)*, pages 529–540. ACM, 2026. doi:10.1145/3798129.3800771 [p. 1]

[BKKS23] Vladimir Braverman, Robert Krauthgamer, Aditya Krishnan, and Shay Sapir. Lower bounds for pseudo-deterministic counting in a stream. In *Proceedings of the 50th International Colloquium on Automata, Languages, and Programming (ICALP)*, pages 30:1–30:14. Schloss Dagstuhl, 2023. doi:10.4230/LIPICS.ICALP.2023.30 [p. 1]

[CCMT14] Amit Chakrabarti, Graham Cormode, Andrew McGregor, and Justin Thaler. Annotations in data streams. *ACM Transactions on Algorithms*, 11(1):7:1–7:30, 2014. doi:10.1145/2636924 [p. 2]

[CDM25] Arkadev Chattopadhyay, Yogesh Dahiya, and Meena Mahajan. Pseudo-deterministic query complexity of search problems. *Computational Complexity*, 34(2):20, 2025. doi:10.1007/S00037-025-00266-7 [p. 1]

[CFKMP21] Arkadev Chattopadhyay, Yuval Filmus, Sajin Koroth, Or Meir, and Toniann Pitassi. Query-to-communication lifting using low-discrepancy gadgets. *SIAM Journal on Computing*, 50(1):171–210, 2021. doi:10.1137/19M1310153 [p. 5]

[Che20] Lijie Chen. On the hardness of approximate and exact (bichromatic) maximum inner product. *Theory of Computing*, 16:1–50, 2020. doi:10.4086/TOC.2020.V016A004 [p. 2]

[CLORS26] Lijie Chen, Zhenjian Lu, Igor Oliveira, Hanlin Ren, and Rahul Santhanam. Polynomial-time pseudodeterministic construction of primes. *Journal of the ACM*, 73(2):14:1–14:43, 2026. doi:10.1145/3803408 [p. 1]

[DPV18] Peter Dixon, Aduri Pavan, and N. V. Vinodchandran. On pseudodeterministic approximation algorithms. In *Proceedings of the 43rd International Symposium on Mathematical Foundations of Computer Science (MFCS)*, pages 61:1–61:11. Schloss Dagstuhl, 2018. doi:10.4230/LIPICS.MFCS.2018.61 [p. 1]

[DPV21] Peter Dixon, Aduri Pavan, and N. V. Vinodchandran. Complete problems for multi-pseudodeterministic computations. In *Proceedings of the 12th Innovations in Theoretical Computer Science Conference (ITCS)*, pages 66:1–66:16. Schloss Dagstuhl, 2021. doi:10.4230/LIPICS.ITCS.2021.66 [p. 1]

[DPWV22] Peter Dixon, Aduri Pavan, Jason Vander Woude, and N. V. Vinodchandran. Pseudodeterminism: Promises and lowerbounds. In *Proceedings of the 54th Symposium on Theory of Computing (STOC)*, pages 1552–1565. ACM, 2022. doi:10.1145/3519935.3520043 [p. 1]

[FFKL03] Stephen Fenner, Lance Fortnow, Stuart Kurtz, and Lide Li. An oracle builder's toolkit. *Information and Computation*, 182(2):95–136, 2003. doi:10.1016/S0890-5401(03)00018-X [p. 3]

[Gav25] Dmytro Gavinsky. Unambiguous parity-query complexity. *Random Structures and Algorithms*, 66(3), 2025. doi:10.1002/RSA.70010 [pp. 1, 6]

[GG11] Eran Gat and Shafi Goldwasser. Probabilistic search algorithms with unique answers and their cryptographic applications. Technical Report TR11-136, Electronic Colloquium on Computational Complexity (ECCC), 2011. URL: https://eccc.weizmann.ac.il/report/2011/136/ [p. 1]

[GG17] Shafi Goldwasser and Ofer Grossman. Bipartite perfect matching in pseudo-deterministic NC. In *Proceedings of the 44th International Colloquium on Automata, Languages, and Programming (ICALP)*, pages 87:1–87:13. Schloss Dagstuhl, 2017. doi:10.4230/LIPICS.ICALP.2017.87 [p. 1]

[GG21] Sumanta Ghosh and Rohit Gurjar. Matroid intersection: A pseudo-deterministic parallel reduction from search to weighted-decision. In *Proceedings of the 25th International Conference on Randomization and Computation (RANDOM)*, pages 41:1–41:16. Schloss Dagstuhl, 2021. doi:10.4230/LIPICS.APPROX/RANDOM.2021.41 [p. 1]

[GGH18] Shafi Goldwasser, Ofer Grossman, and Dhiraj Holden. Pseudo-deterministic proofs. In *Proceedings of the 9th Innovations in Theoretical Computer Science Conference (ITCS)*, pages 17:1–17:18. Schloss Dagstuhl, 2018. doi:10.4230/LIPICS.ITCS.2018.17 [p. 1]

[GGH19] Michel Goemans, Shafi Goldwasser, and Dhiraj Holden. Doubly-efficient pseudo-deterministic proofs. Technical Report TR19-135, Electronic Colloquium on Computational Complexity (ECCC), 2019. URL: https://eccc.weizmann.ac.il/report/2019/135/ [p. 1]

[GGKS20] Ankit Garg, Mika Göös, Pritish Kamath, and Dmitry Sokolov. Monotone circuit lower bounds from resolution. *Theory of Computing*, 16:1–30, 2020. doi:10.4086/TOC.2020.V016A013 [p. 5]

[GGMW20] Shafi Goldwasser, Ofer Grossman, Sidhanth Mohanty, and David Woodruff. Pseudo-deterministic streaming. In *Proceedings of the 11th Innovations in Theoretical Computer Science Conference (ITCS)*, pages 79:1–79:25. Schloss Dagstuhl, 2020. doi:10.4230/LIPICS.ITCS.2020.79 [p. 1]

[GGR13] Oded Goldreich, Shafi Goldwasser, and Dana Ron. On the possibilities and limitations of pseudodeterministic algorithms. In *Proceedings of the 4th Innovations in Theoretical Computer Science Conference (ITCS)*, pages 127–138. ACM, 2013. doi:10.1145/2422436.2422453 [p. 1]

[GGS23] Ofer Grossman, Meghal Gupta, and Mark Sellke. Tight space lower bound for pseudo-deterministic approximate counting. In *Proceedings of the 64th Symposium on Foundations of Computer Science (FOCS)*, pages 1496–1504. IEEE, 2023. doi:10.1109/FOCS57990.2023.00091 [p. 1]

[GHRSSY26] Mika Göös, Nathaniel Harms, Artur Riazanov, Anastasia Sofronova, Dmitry Sokolov, and Weiqiang Yuan. Pseudodeterministic communication complexity. In *Proceedings of the 58th Symposium on Theory of Computing (STOC)*, pages 2030–2039. ACM, 2026. doi:10.1145/3798129.3800907 [pp. 1, 2, 5, 6]

[GIPS21] Shafi Goldwasser, Russell Impagliazzo, Toniann Pitassi, and Rahul Santhanam. On the pseudo-deterministic query complexity of NP search problems. In *Proceedings of the 36th Computational Complexity Conference (CCC)*, pages 36:1–36:22. Schloss Dagstuhl, 2021. doi:10.4230/LIPICS.CCC.2021.36 [p. 1]

[GKPW19] Mika Göös, Pritish Kamath, Toniann Pitassi, and Thomas Watson. Query-to-communication lifting for P^{NP}. *Computational Complexity*, 28(1):113–144, 2019. doi:10.1007/s00037-018-0175-5 [p. 5]

[GL19] Ofer Grossman and Yang Liu. Reproducibility and pseudo-determinism in log-space. In *Proceedings of the 30th Symposium on Discrete Algorithms (SODA)*, pages 606–620. ACM–SIAM, 2019. doi:10.1137/1.9781611975482.38 [p. 1]

[GLMWZ16] Mika Göös, Shachar Lovett, Raghu Meka, Thomas Watson, and David Zuckerman. Rectangles are nonnegative juntas. *SIAM Journal on Computing*, 45(5):1835–1869, 2016. doi:10.1137/15M103145X [pp. 5, 6, 7]

[Gol25] Oded Goldreich. Multi-pseudodeterministic algorithms. In *Computational Complexity and Local Algorithms*, pages 22–43. Springer, 2025. doi:10.1007/978-3-031-88946-2_2 [p. 1]

[Göö15] Mika Göös. Lower bounds for clique vs. independent set. In *Proceedings of the 56th Symposium on Foundations of Computer Science (FOCS)*, pages 1066–1076. IEEE, 2015. doi:10.1109/FOCS.2015.69 [p. 5]

[GPW18a] Mika Göös, Toniann Pitassi, and Thomas Watson. Deterministic communication vs. partition number. *SIAM Journal on Computing*, 47(6):2435–2450, 2018. doi:10.1137/16M1059369 [p. 5]

[GPW18b] Mika Göös, Toniann Pitassi, and Thomas Watson. The landscape of communication complexity classes. *Computational Complexity*, 27(2):245–304, 2018. doi:10.1007/s00037-018-0166-6 [p. 2]

[GPW20] Mika Göös, Toniann Pitassi, and Thomas Watson. Query-to-communication lifting for BPP. *SIAM Journal on Computing*, 49(4):FOCS17-441–FOCS17-461, 2020. doi:10.1137/17M115339X [p. 5]

[GR15] Tom Gur and Ran Raz. Arthur–Merlin streaming complexity. *Information and Computation*, 243:145–165, 2015. doi:10.1016/j.ic.2014.12.011 [p. 2]

[GR18] Tom Gur and Ron Rothblum. Non-interactive proofs of proximity. *Computational Complexity*, 27(1):99–207, 2018. doi:10.1007/S00037-016-0136-9 [p. 2]

[GS24] Prantar Ghosh and Vihan Shah. New lower bounds in Merlin–Arthur communication and graph streaming verification. In *Proceedings of the 15th Innovations in Theoretical Computer Science Conference (ITCS)*, pages 53:1–53:22. Schloss Dagstuhl, 2024. doi:10.4230/LIPICS.ITCS.2024.53 [p. 2]

[HMWYZ25] Mi-Ying (Miryam) Huang, Xinyu Mao, Shuo Wang, Guangxu Yang, and Jiapeng Zhang. A min-entropy approach to multi-party communication lower bounds. In *Proceedings of the 40th Computational Complexity Conference (CCC)*, pages 33:1–33:29. Schloss Dagstuhl, 2025. doi:10.4230/LIPICS.CCC.2025.33 [p. 5]

[HN12] Trinh Huynh and Jakob Nordström. On the virtue of succinct proofs: Amplifying communication complexity hardness to time-space trade-offs in proof complexity. In *Proceedings of the 44th Symposium on Theory of Computing (STOC)*, pages 233–248. ACM, 2012. doi:10.1145/2213977.2214000 [p. 1]

[Juk12] Stasys Jukna. *Boolean Function Complexity: Advances and Frontiers*, volume 27 of *Algorithms and Combinatorics*. Springer, 2012. doi:10.1007/978-3-642-24508-4 [p. 3]

[Kla03] Hartmut Klauck. Rectangle size bounds and threshold covers in communication complexity. In *Proceedings of the 18th Conference on Computational Complexity (CCC)*, pages 118–134. IEEE, 2003. doi:10.1109/CCC.2003.1214415 [p. 2]

[KN97] Eyal Kushilevitz and Noam Nisan. *Communication Complexity*. Cambridge University Press, 1997. doi:10.1017/CBO9780511574948 [p. 3]

[Koz06] Dexter Kozen. *Theory of Computation*. Texts in Computer Science. Springer, 2006. doi:10.1007/1-84628-477-5 [p. 2]

[Lau83] Clemens Lautemann. BPP and the polynomial hierarchy. *Information Processing Letters*, 17(4):215–217, 1983. doi:10.1016/0020-0190(83)90044-3 [p. 3]

[LMMPZ22] Shachar Lovett, Raghu Meka, Ian Mertz, Toniann Pitassi, and Jiapeng Zhang. Lifting with sunflowers. In *Proceedings of the 13th Innovations in Theoretical Computer Science Conference (ITCS)*, pages 104:1–104:24. Schloss Dagstuhl, 2022. doi:10.4230/LIPICS.ITCS.2022.104 [p. 5]

[LOS21] Zhenjian Lu, Igor Oliveira, and Rahul Santhanam. Pseudodeterministic algorithms and the structure of probabilistic time. In *Proceedings of the 53rd Symposium on Theory of Computing (STOC)*, pages 303–316. ACM, 2021. doi:10.1145/3406325.3451085 [p. 1]

[MV96] Andrei Muchnik and Nikolai Vereshchagin. A general method to construct oracles realizing given relationships between complexity classes. *Theoretical Computer Science*, 157(2):227–258, 1996. doi:10.1016/0304-3975(95)00161-1 [p. 3]

[OS17] Igor Oliveira and Rahul Santhanam. Pseudodeterministic constructions in subexponential time. In *Proceedings of the 49th Symposium on Theory of Computing (STOC)*, pages 665–677. ACM, 2017. doi:10.1145/3055399.3055500 [p. 1]

[OS18] Igor Oliveira and Rahul Santhanam. Pseudo-derandomizing learning and approximation. In *Proceedings of the 22nd International Conference on Randomization and Computation (RANDOM)*, pages 55:1–55:19. Schloss Dagstuhl, 2018. doi:10.4230/LIPICS.APPROX-RANDOM.2018.55 [p. 1]

[PSS14] Periklis Papakonstantinou, Dominik Scheder, and Hao Song. Overlays and limited memory communication. In *Proceedings of the 29th Conference on Computational Complexity (CCC)*, pages 298–308. IEEE, 2014. doi:10.1109/CCC.2014.37 [p. 3]

[PSS23] Toniann Pitassi, Morgan Shirley, and Adi Shraibman. The strength of equality oracles in communication. In *Proceedings of the 14th Innovations in Theoretical Computer Science Conference (ITCS)*, pages 89:1–89:19. Schloss Dagstuhl, 2023. doi:10.4230/LIPICS.ITCS.2023.89 [p. 3]

[PSW21] Toniann Pitassi, Morgan Shirley, and Thomas Watson. Nondeterministic and randomized boolean hierarchies in communication complexity. *Computational Complexity*, 30(2):10, 2021. doi:10.1007/S00037-021-00210-5 [pp. 3, 5]

[RM99] Ran Raz and Pierre McKenzie. Separation of the monotone NC hierarchy. *Combinatorica*, 19(3):403–435, 1999. doi:10.1007/S004930050062 [p. 5]

[RY20] Anup Rao and Amir Yehudayoff. *Communication Complexity and Applications*. Cambridge University Press, 2020. doi:10.1017/9781108671644 [p. 3]

[Wat16] Thomas Watson. Nonnegative rank vs. binary rank. *Chicago Journal of Theoretical Computer Science*, 2016(2):1–13, 2016. doi:10.4086/cjtcs.2016.002 [p. 5]

[Wat20a] Thomas Watson. Quadratic simulations of Merlin–Arthur games. *ACM Transactions on Computation Theory*, 12(2):14:1–14:11, 2020. doi:10.1145/3389399 [pp. 3, 5, 6]

[Wat20b] Thomas Watson. A $\mathrm{ZPP}^{\mathrm{NP}[1]}$ lifting theorem. *ACM Transactions on Computation Theory*, 12(4):27:1–27:20, 2020. doi:10.1145/3428673 [p. 5]

[Wat26] Thomas Watson. *Complexity in Computer Science*. Cambridge University Press, 2026. doi:10.1017/9781009752329 [p. 3]

[YZ24] Guangxu Yang and Jiapeng Zhang. Communication lower bounds for collision problems via density increment arguments. In *Proceedings of the 56th Symposium on Theory of Computing (STOC)*, pages 630–639. ACM, 2024. doi:10.1145/3618260.3649607 [p. 5]

[ZP03] Stathis Zachos and Aris Pagourtzis. Combinatory complexity: Operators on complexity classes. In *Proceedings of the 4th Panhellenic Logic Symposium (PLS)*, 2003 [p. 2]