Electronic Colloquium on Computational Complexity, Report No. 47 (2026)

An $\Omega((\log n/\log\log n)^2)$ Cell-Probe Lower Bound for Dynamic Boolean Data Structures

Young Kun Ko

Department of Computer Science and Engineering, Pennsylvania State University

Email: ykko@psu.edu

March 26, 2026

Abstract

We resolve the long-standing open problem of Boolean dynamic data structure hardness, proving an unconditional lower bound of $\Omega((\log n/\log\log n)^2)$ for the Multiphase Problem of Pătraşcu [STOC 2010] (instantiated with Inner Product over $\mathbb{F}_2$). This matches the celebrated barrier for weighted problems established by Larsen [STOC 2012] and closes the gap left by the $\Omega(\log^{1.5} n)$ Boolean bound of Larsen, Weinstein, and Yu [STOC 2018].

The previous barrier was methodological: all prior works relied on "one-way" communication games, where the inability to verify query simulations necessitated complex machinery (such as the Peak-to-Average Lemma) that hit a hard ceiling at $\log^{1.5} n$.

Our key contribution is conceptual: We introduce a 2.5-round Multiphase Communication Game that augments the standard one-way model with a verification round, where Bob confirms the consistency of Alice's simulation against the actual memory. This simple, qualitative change allows us to bypass technical barriers and obtain the optimal bound directly. As a consequence, our analysis naturally extends to other hard Boolean functions, offering a general recipe for translating discrepancy lower bounds into $\Omega((\log n/\log\log n)^2)$ dynamic Boolean data structure lower bounds.

We also argue that this result likely represents the structural ceiling of the Chronogram framework initiated by Fredman and Saks [STOC 1989]: any $\omega(\log^2 n)$ lower bound would require either fundamentally new techniques or major circuit complexity breakthroughs.

ISSN 1433-8092

1 Introduction

Proving unconditional lower bounds for dynamic data structures in the cell-probe model [Yao81] stands as one of the grand challenges in theoretical computer science. In this model, memory is organized into fixed-size cells of $w = \Theta(\log n)$ bits, and we charge unit cost for accessing a cell while permitting arbitrary computation on the probed data for free. Because of this unbounded computational power, the cell-probe model strictly subsumes all realistic architectures; consequently, any lower bound proved here applies universally. However, this generality comes at a steep price: the model's ability to arbitrarily compress and encode information makes proving lower bounds notoriously difficult.

Despite over 35 years of sustained effort since Fredman and Saks' seminal Chronogram method [FS89], progress has been slow. The field advanced from $\Omega(\log n/\log\log n)$ to $\Omega(\log n)$ over 15 years [PD06], then to $\Omega((\log n/\log\log n)^2)$ for *weighted* problems over another 7 years [Lar12], where each query output is $\Omega(\log n)$ bits. For Boolean (decision) problems—where queries return a single bit—even this $\Omega((\log n/\log\log n)^2)$ barrier seemed insurmountable. Larsen's breakthrough technique [Lar12] inherently required $\Omega(\log n)$-bit outputs, leaving the Boolean case explicitly open. This question was listed among Mihai Pătraşcu's five most important open problems in the posthumous compilation by Thorup [Tho13], and stood as perhaps the central challenge in dynamic lower bounds for decades.

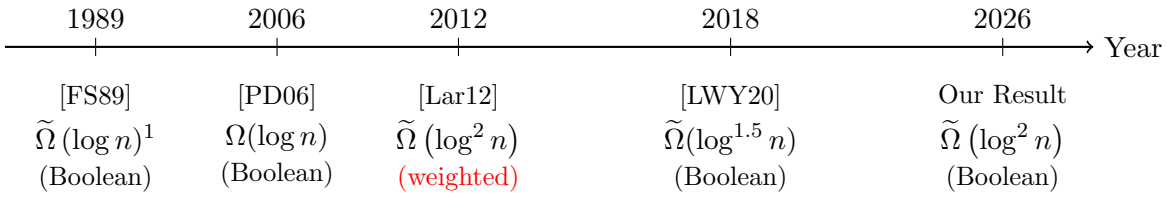

Figure 1: Historical progression of dynamic cell-probe lower bounds.

In this paper, we close this gap. We prove an unconditional lower bound of $\Omega((\log n/\log\log n)^2)$ for Boolean data structures, matching the highest known bound for weighted problems and resolving the open question of Boolean hardness. Our result applies to the Multiphase Problem with Inner Product over $\mathbb{F}_2$, directly implying lower bounds for fundamental problems including dynamic matrix-vector multiplication over $\mathbb{F}_2$, dynamic path parity, and dynamic range counting mod 2.

1.1 Our Contribution

As our hard problem, we consider the seminal Multiphase Problem of Pătraşcu [Pat10]. For a Boolean function $f : \{0,1\}^{2n} \to \{\pm 1\}$, the problem is:

- $\vec{S} = S_1, \ldots, S_m \in \{0,1\}^n$ are pre-processed.
- Updates $X \in \{0,1\}^n$ modify the data structure (t_u-probes per update).
- Per any given $q \in [m]$, output $f(S_q, X)$ using t_{tot} total probes.

Problem 1: Multiphase Problem for f

[1] $\widetilde{\Omega}$ hides a $\mathrm{poly}(\log\log n)$ factor in the denominator

When f is Disjointness or Inner Product over $\mathbb{F}_2$, Pătraşcu conjectured that $\max\{t_u, t_{tot}\} \geq n^{\Omega(1)}$ [Pat10] – the notorious Multiphase Conjecture [Pat10, Tho13, Bra22]. Pătraşcu showed that this conjecture implies polynomial lower bounds for dynamic problems including dynamic s-t reachability. We show the following main theorem for the Multiphase Problem.

Theorem 1.1. *For the Multiphase Problem with f Inner Product over $\mathbb{F}_2$, and $m = n^{1+\Omega(1)}$,*

$$\max\{t_u, t_{tot}\} \geq \Omega\left(\left(\frac{\log n}{\log\log n}\right)^2\right)$$

Formally, we prove a slightly stronger statement where we can allow t_u to be *any poly-logarithmic* function of n, just as in the case of [LWY20]. We provide the full statement and proof in Section 3.

General Lifting Theorem While Theorem 1.1 focuses on the Inner Product over $\mathbb{F}_2$ to resolve the specific open problem posed by Pătraşcu and Larsen, our technique is not limited to the Inner Product over $\mathbb{F}_2$. Our Simulation Theorem (Section 3.1) establishes a general translation from communication complexity to dynamic data structure lower bounds. Our lower bound applies to *any* function f that is "hard." Roughly, functions for which one cannot obtain $n^{-\Omega(1)}$ advantage (i.e., low discrepancy) under *product distributions* with large min-entropy are defined to be hard. This hardness condition is indeed satisfied by the Inner Product over $\mathbb{F}_2$ function, but unfortunately, the Disjointness function does not meet the criterion [BM13]. A naive strategy of sampling and revealing a few coordinates of X already yields non-trivial advantage for Disjointness, violating the hardness condition. We refer the reader to Section B, specifically Definition B.1 for the precise technical definition. We then show a general "lifting" theorem (Theorem B.4) which shows that if f is "hard," then the Multiphase Problem with f must have

$$\max\{t_u, t_{tot}\} \geq \Omega\left(\left(\frac{\log n}{\log\log n}\right)^2\right).$$

We defer the full proof to Section B to preserve the clarity of the main argument.

1.2 Applications

Due to the standard reductions given by Pătraşcu in [Pat10], this directly implies lower bounds for the following problems.

- A matrix $M \in \mathbb{F}_2^{m \times n}$ is given and pre-processed.
- $X \in \{0,1\}^n$ is updated dynamically. Output $\langle M_q, X\rangle$ for any given $q \in [m]$.

Problem 2: Dynamic Matrix-Vector Multiplication over $\mathbb{F}_2$

- A directed graph $G = (V, E)$ is initially given. Updates add and remove edges in the graph.
- For a given $(u, v) \in V \times V$, output the parity of the number of paths between u and v. For k-Path Parity Problem, output the parity of the number of paths of length exactly k.

Problem 3: Dynamic (k-) Path Parity

- A matrix of integers is preprocessed. Updates increment all values in a specified row or column.
- For a given query, output the parity of the number of maximum values in the matrix.

Problem 4: Erickson's Problem, Counting Version

Corollary 1.2. *Problem 2, Problem 3, Problem 4 require* $\max\{t_u, t_{tot}\} \geq \Omega\left(\left(\frac{\log n}{\log\log n}\right)^2\right)$

1.3 Previous Works

To put our technical contribution into perspective, we briefly summarize nearly 40 years of developments in dynamic cell-probe lower bounds. Readers who are familiar with the developments can skip to Section 1.4 for our technical contribution.

1.3.1 Explicit Quests for Poly-logarithmic Lower Bounds

Chronogram Method The seminal work of Fredman and Saks [FS89] introduced the Chronogram method. At a high-level, the Chronogram method divides the sequence of n updates X into ℓ epochs, $\{X^{(i)}\}_{i=1}^{\ell}$, where $X^{(i)}$ consists of n_i bits and $n_i = |X^{(i)}| = \beta^i$, where β is a parameter set per problem in question (roughly poly(wt_u)). We will be then processing the updates in the reverse order, that is, the larger epochs are processed first, denoting the updates at each epoch i as U_i respectively.

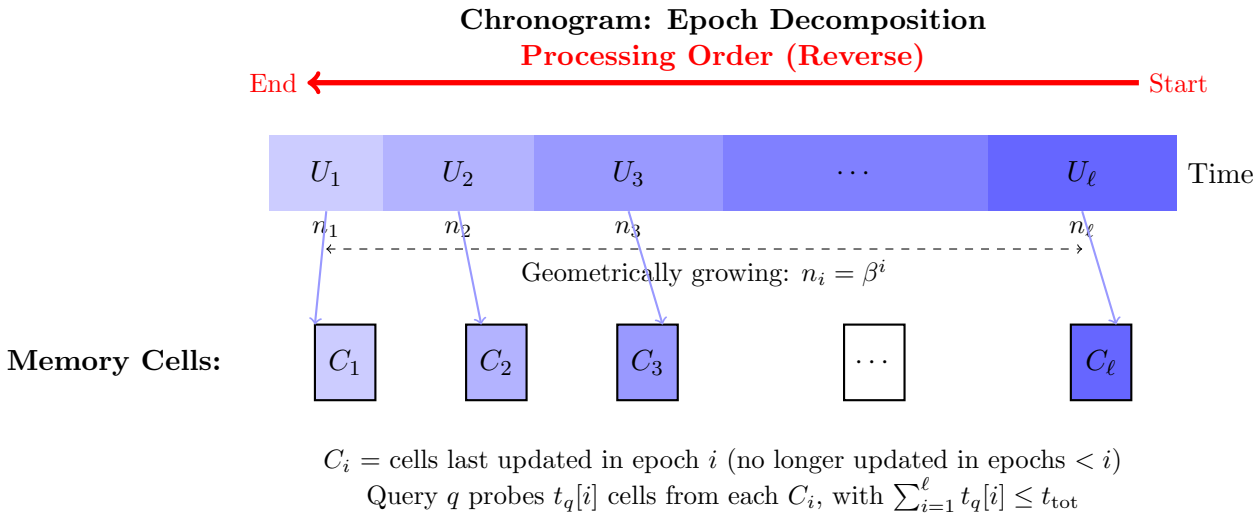

Figure 2: The Chronogram technique decomposes n updates into $\ell = \Theta(\log_\beta n)$ epochs with geometrically growing sizes $n_i = \beta^i$. Crucially, epochs are **processed in reverse order** (largest first). Each epoch i has associated cells C_i that were last updated in that epoch. A query algorithm for $q \in \mathcal{Q}$ probes $t_q[i]$ cells from each C_i.

The main observation by Fredman and Saks is that we can decompose the updated cells depending on the latest epoch that performed the update. That is $C_1, \ldots, C_\ell$, where each $C_i \subseteq U_i$ contains the cells last updated by epoch i, no longer updated in epochs $< i$. The key point is

that there must exist $i \in [\ell]$ such that the query algorithm probes t_{tot}/ℓ cells from C_i on average. That is $\mathbb{E}_{q\sim\mathcal{Q}}[t_q[i]] \le O(t_{tot}/\ell)$. This was elegantly put in [LY25] as "static" data structure with pre-initialized memory and a cache, where pre-initialized memory refers to $C_{>i}$ and cache refers to $C_{<i}$. The goal then is to show a lower bound on t_{tot}/ℓ, which is the average number of probes into C_i. Fredman and Saks proved an $\Omega(1)$ lower bound on t_{tot}/ℓ, leading to $\max\{t_u, t_{tot}\} \ge \Omega(\log n/\log\log n)$. Then it took more than 15 years for further quantitative improvement. A more careful analysis by considering the information transfer between the epochs [PD06] led to shaving the $\log\log n$ factor in the denominator.

Chronogram + Cell-sampling The breakthrough work of Larsen [Lar12] then successfully merged the cell-sampling technique [Sie04, PTW10] with the Chronogram technique [FS89] to give an $\Omega((\log n/\log\log n)^2)$ bound with the following rough idea. Recall that after the decomposition using the Chronogram method, the goal is to show a lower bound on t_{tot}/ℓ, which is the number of probes into C_i. As ℓ would always be roughly $\Theta(\log n/\log(t_u w))$, if we can show, say, $t_{tot}/\ell \ge \widetilde{\Omega}(\log n)$, this would give an $\widetilde{\Omega}(\log^2 n)$ bound on t_{tot}.

To show such lower bound on t_{tot}/ℓ, Larsen [Lar12] utilizes the cell-sampling method [Sie04, PTW10]. The main idea behind cell-sampling is the following. If there exists a too-good-to-be-true (i.e., short) t_{tot} query algorithm, then naively sampling some $p := (\text{poly}\log n)^{-1}$ fraction of the cells would give a non-trivial advantage (of roughly $p^{t_{tot}/\ell}$) in answering the queries. An equivalent way to frame this argument is to find a small subset $C_0 \subset C_i$ such that C_0 along with C_{-i} will answer $n^{-o(1)}$ fraction of possible queries, without having to know the whole C_i. We can generate such C_0 by simply sampling each cell in C_i at random with probability p. By the rule of expectation, there must exist a setting of such C_0 which can answer $n^{-o(1)}$ fraction of possible queries, say $\mathcal{Q}^* \subset \mathcal{Q}$.

An elegant way to formulate the underlying combinatorial problem is through the following one-way communication simulation, as the ultimate goal is to show such one-way communication cannot exist.

- Fix $\vec{S}$ known to both Alice and Bob. Bob is given all the updates $\{X^{(i)}\}_{i=1}^{\ell}$, but not the desired query $Q \in \mathcal{Q}$.
- Alice is given all the updates, except the updates in epoch i (i.e., $X^{(i)}$), and the desired query Q.
- Bob sends a one-way message M of length $|M| \le n_i/\text{poly}\log n$ bits to Alice. Then Alice announces $f(S_Q, X)$.

Protocol 1: One-way Communication Simulation

As a one-way message, Bob will send the small sub-sampled subset $\widetilde{C}_i$ along with $C_{<i}$. Cell-sampling ensures that $\widetilde{C}_i$ is small, while the Chronogram ensures that $C_{<i}$ is small. Alice then can simulate the queries for $\mathcal{Q}^*$. So for any $Q \in \mathcal{Q}^*$, Alice will be outputting the correct answer, achieving a non-trivial advantage! We then just need to show that a short one-way message M cannot answer an $n^{-o(1)}$ fraction of $\mathcal{Q}$.

Though tempting, this argument has a crucial flaw. $\widetilde{C}_i$ cannot identify $\mathcal{Q}^*$, (i.e., $\mathcal{Q}^*$-identification problem). This occurs because Alice cannot distinguish whether the probed cells are inside $C_i \backslash \widetilde{C}_i$ or absent from C_i entirely. As she cannot identify the set $\mathcal{Q}^*$, there is no guarantee that Alice's guess provides zero advantage over completely random guessing for queries in $\mathcal{Q}\backslash\mathcal{Q}^*$. This technical subtlety is what appears in all subsequent works to prove an $\omega(\log n)$ lower bound

[Pat07, Lar12, LWY20, LY25].

Larsen [Lar12] tackled this technical subtlety by encoding a subset of $\mathcal{Q}^*$ as a part of Bob's message, but this argument crucially requires the output to be $\Omega(\log n)$ bits. To extend the method to the Boolean setting, Larsen, Weinstein, and Yu [LWY20] introduced the so-called Peak-to-Average Lemma, a proof of which requires a technical dive into Chebyshev polynomials. The lemma allows Bob to carefully choose a subset of cells, knowledge of which yields a non-trivial advantage (of $n^{-o(1)}$) but with a $\sqrt{\log n}$ parameter loss. No improvement can be made to the lemma, as the lemma is tight (Appendix B of [LWY20]).

1.3.2 Previous Work on the Multiphase Problem

Pătraşcu envisioned an approach [Pat10, Tho13] to break out of the Chronogram Method and its extensions (all the methods in Section 1.3.1), providing a new angle on dynamic Boolean cell-probe lower bounds.

His ambitious goal was to directly prove a polynomial lower bound by considering Problem 1. He conjectured that Problem 1 requires $n^{\Omega(1)}$ for $m = \text{poly}(n)$, even for f being Disjointness. This is the notorious Multiphase Conjecture. Pătraşcu then showed reductions to various dynamic problems such as dynamic reachability, among others.

It is noteworthy to point out that Pătraşcu [Pat10] actually opened the whole area of Fine-Grained Complexity of Dynamic Problems using the Multiphase Problem (Problem 1). He showed that the 3SUM Conjecture[2] implies the Multiphase Conjecture. We refer the reader to the survey [Wil17] for the context of Multiphase Conjecture in the area of Fine-Grained Complexity of Dynamic Problems.

While the problem is conjectured to be polynomially hard, the best unconditional lower bound stood at merely $\Omega(\log n)$ for over a decade against the easier bit-probe model (i.e., the word size $w = 1$) [BL15, CGL15, KW20].[3] Pătraşcu's proposed approach was to consider the following communication game, which is now commonly referred to as the Multiphase Communication Game.

- Alice holds $\vec{S} \in (\{0,1\}^n)^m$, and $Q \in [m]$. Bob holds $X \in \{0,1\}^n$ and $Q \in [m]$. Merlin holds $\vec{S}$ and X.
- Merlin sends U to Bob of length $s = O(n \cdot t_u \cdot w)$.
- Alice and Bob engage in standard two-party $\widetilde{O}(t_{tot})$ bits communication to output $f(S_Q, X)$.

Protocol 2: Multiphase Communication Game

The communication model then can simulate the update and query algorithms, as Merlin can simulate all the update algorithms, with $s = w \cdot n \cdot t_u$. Then Alice and Bob can simulate the query algorithm using $w \cdot t_{tot} = \widetilde{O}(t_{tot})$ communications to output $f(S_Q, X)$.

Pătraşcu believed that if $s = m^{0.99}$, then Merlin's advice should not matter. Thus Alice and Bob must spend roughly the standard communication complexity of f. However, this crude intuition was falsified in [CEEP12], which showed examples of f with very efficient protocols. For example, if f is Disjointness, there exists Merlin's message U with $s = \tilde{O}(\sqrt{n})$ such that Alice and Bob only

[2]The Conjecture states that 3SUM problem on n integers from $\{-n^4, \ldots, +n^4\}$ cannot be solved in $O(n^{2-\varepsilon})$ for any $\varepsilon > 0$.

[3]While [BL15, CGL15, KW20] do not explicitly mention the lower bound, one can simulate a t-round adaptive algorithm with 2^t-round non-adaptive algorithms under the bit-probe model.

communicate $\widetilde{O}(\sqrt{n})$ bits, in stark contrast to the $\Omega(n)$ communication complexity of Disjointness [KS92, Raz92, BYJKS04].

In fact, as pointed out in [KW20, Ko25a], even a lower bound against 3-round communication between Alice and Bob (Alice, Bob then Alice speaks) would imply a breakthrough in circuit complexity, namely circuit lower bounds for random linear operators [JS10, Juk12, Juk13, Dru12]. Nevertheless, Ko and Weinstein [KW20] developed an information-theoretic framework to handle 2-rounds (Alice, then Bob speaks) communication, for the zero-error or small-error regime. This framework was further extended by Ko [Ko25a] to handle low advantage regime, where the performance of Bob's final output is compared against a random guess.

Recently, Ko [Ko25b] successfully applied the information-theoretic framework [KW20, Ko25a] with the one-way simulation theorem of Larsen, Weinstein, and Yu [LWY20], to give an $\widetilde{\Omega}(\log^{3/2}(n))$ lower bound for Problem 1 when f is Inner Product over $\mathbb{F}_2$. As the work was directly applying the one-way simulation theorem of Larsen, Weinstein and Yu [LWY20], then using the information-theoretic methods to lower bound the one-way communication, the only possible lower bound was $\widetilde{\Omega}(\log^{3/2}(n))$.

1.4 Technical Contribution: The 2.5-Round Communication Game

We resolve the Boolean hardness question by introducing a fundamentally different communication model that eliminates the technical barriers faced by all previous approaches.

The Core Challenge. All previous super-logarithmic lower bounds [Lar12, LWY20, LY25] rely on the Chronogram and cell-sampling techniques, which reduce the problem to proving that no short *one-way* message from Bob to Alice can help answer an $n^{-o(1)}$ fraction of queries in Protocol 1. However, as discussed in Section 1.3.1, there is a fatal technical subtlety: Alice does not know *which queries* she can answer correctly (the set $\mathcal{Q}^*$), because she cannot distinguish between:

- Probed cells missing from Bob's randomly sampled subset;
- Probed cells that were never written to memory at all

This ambiguity destroys the advantage argument. Larsen, Weinstein, and Yu [LWY20] resolved this using the Peak-to-Average Lemma, a sophisticated application of Chebyshev polynomials, but this incurs a $\sqrt{\log n}$ parameter loss, yielding only $\widetilde{\Omega}(\log^{1.5}(n))$. The lemma is provably tight [LWY20, Appendix B].

Our Key Insight. The one-way communication prevents Alice from verifying whether her simulation is correct. But if we add just *an additional round* – letting Bob verify and certify Alice's guess – the entire technical barrier disappears.

We introduce a *2.5-round Multiphase Communication Game*:

1. **Round 0 (Merlin → Bob):** Merlin (holding $\vec{S}, X$) sends update information U to Bob
2. **Round 0.5 (Bob → Alice):** Bob (holding X) forwards a message $\Phi(U)$ to Alice (depends only on U and Bob's randomness, not the query)
3. **Round 1 (Alice → Bob):** Query Q is revealed to Alice; Alice sends her simulation transcript A_Q to Bob
4. **Round 2 (Bob outputs):** Bob verifies A_Q against U and outputs final answer

The protocol structure is illustrated in Figure 3.

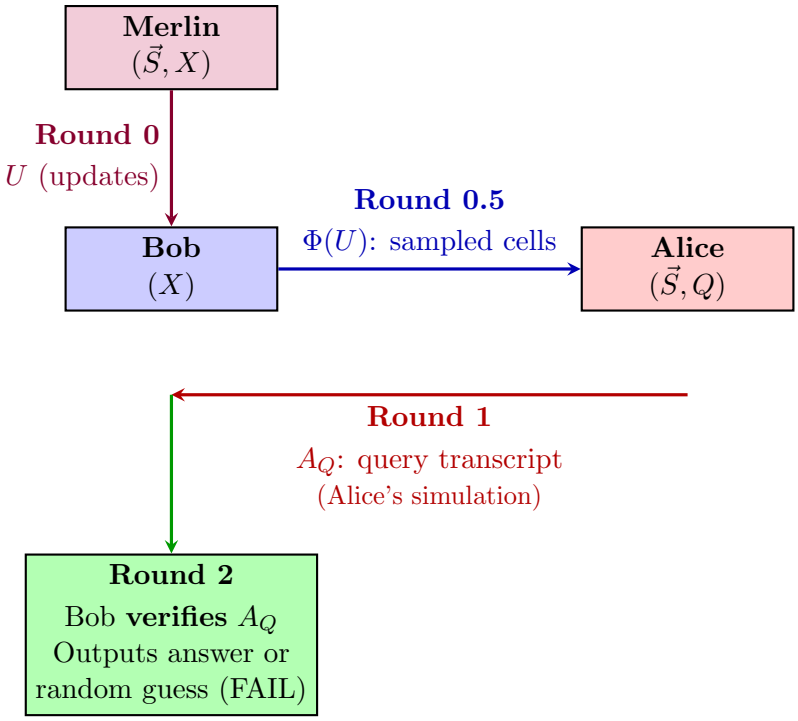

Figure 3: Our 2.5-round Multiphase Communication Game. The crucial difference from prior work is the **verification step** (Round 2): Bob checks if Alice's transcript A_Q is consistent with the actual memory U. The 0.5-round message $\Phi(U)$ is sent independently of query Q, making this analyzable with information-theoretic techniques from [KW20, Ko25a].

Verification Step The verification step is crucial:

- Alice simulates the query algorithm and sends the full transcript to Bob.
- Bob checks if Alice's simulation is *consistent* with actual updated memory U.
- If Alice probes the wrong cells, namely $C_{>i}$ instead of C_i due to sampling error, her transcript will not match U.
- Bob detects this inconsistency and outputs FAIL, which then results in a random guess.
- Only when Alice's simulation is correct does Bob output a meaningful answer.

This completely eliminates the $\mathcal{Q}^*$ ambiguity: Bob's verification determines whether to use Alice's simulation or default to a random guess, so there is no need for Alice to identify $\mathcal{Q}^*$. We delegate verification to Bob. We no longer need the Peak-to-Average Lemma, and can achieve the full $\Omega((\log n/\log\log n)^2)$ bound.

Our Second Contribution: Handling 2.5-Round Protocols. Conceptually, the above simulation is simple. Yet, for the past decade, we have lacked technical tools to give a lower bound for such 2.5-round protocols against small non-trivial advantage.

While 3-round communication lower bounds remain beyond current techniques (and would imply major circuit lower bounds [JS10, Dru12, Juk13, DGW19]), our key observation is that the information-theoretic framework introduced by Ko and Weinstein [KW20], further refined by

Ko [Ko25a] for small advantage regime, can handle exactly this 2.5-round structure. The key is that Bob's "0.5-round" message $\Phi(U)$ is independent of the query Q. This allows us to apply the combinatorial lemmas from [KW20, Ko25a], and we can extract a random variable Z from the 2.5-round protocol such that (a) the min-entropy of S_Q and X conditioned on Z is large; (b) while maintaining $I(S_Q; X|Z)$ to be small.

The Complete Argument. Our proof proceeds in two steps:

1. **Simulation (Section 3.1):** We show that any dynamic data structure with $t_u = \text{poly}\log(n)$ and $t_{tot} = o((\log n/\log\log n)^2)$ can be simulated by a 2.5-round Multiphase Communication Game with non-trivial advantage $n^{-o(1)}$.
2. **Communication Lower Bound (Section 3.2):** We prove that no such 2.5-round protocol can achieve advantage better than $n^{-\Omega(1)}$, yielding a contradiction.

We note that the two main components of our proof — the simulation theorem (Section 3.1) and the communication lower bound (Section 3.2) — are self-contained and can be verified independently.

1.5 Why is $\widetilde{\Omega}(\log^2(n))$ the barrier?

A natural question arises:

> Can this approach be extended to prove higher lower bounds for dynamic Boolean problems, i.e., $\omega(\log^2 n)$?

We argue that our result likely matches the "structural ceiling" of the current techniques, specifically the *Chronogram* framework.

The core of the Chronogram technique relies on decomposing the timeline of updates into a hierarchy of ℓ distinct epochs, where the duration of epoch i grows geometrically. This construction naturally yields a hierarchy of depth $\ell \approx \Theta\left(\frac{\log n}{\log\log n}\right)$. The lower bound is then obtained by constructing a hard distribution of updates and queries that forces the data structure to probe $\widetilde{\Omega}(\log n)$ distinct cells at *each* epoch.

Another perspective on the Chronogram framework is that it reduces dynamic cell-probe lower bound to a static cell-probe lower bound (with pre-initialized memory and cache [LY25]) with ℓ-factor difference. As ℓ is fixed, if we are to show $\omega(\log^2 n)$ lower bound, we must show $\omega(\log n)$ lower bound for a single epoch $i \in [\ell]$.

Unfortunately, the barriers to static cell-probe lower bounds are well-known. The best *explicit* static cell-probe lower bound we can show is described as a ceiling known as the logarithmic barrier [MNSW98, Sie04, PD06, PTW08, PTW10, Pă11, KPI25]

$$t \geq \Omega\left(\frac{\log \frac{|\mathcal{Q}|}{n}}{\log \frac{s}{n}}\right) \tag{1}$$

where s is the number of cells used by the static cell-probe data structure, and $|\mathcal{Q}|$ is the number of possible queries. Even if we allow *semi-explicit* static cell-probe lower bound, allowing queries to be non-explicit linear functions, only a lower bound of

$$t \geq \Omega(\min\{\log(|\mathcal{Q}|/s), n/\log s\}) \tag{2}$$

is known against a weaker bit-probe model [Ko25a]. Both (1) and (2) are merely logarithmic in our regime of interest, since both s and $|\mathcal{Q}|$ are polynomial in n. And due to a well-known connection to circuit lower bounds [JS10, Juk12, Juk13, Dru12, DGW19, KPI25, Ko25a], showing $t \geq \omega(\log n)$ when $|\mathcal{Q}|$ is poly(n) would be a major circuit complexity breakthrough.

To conclude, any $\omega(\log^2 n)$ Boolean lower bound would require either completely breaking away from the *Chronogram* framework, which has been the main recipe for the past ≈ 37 years, or a major circuit complexity breakthrough.

2 Preliminaries

2.1 Information Theory

In this section, we provide the necessary background on information theory and information complexity that are used in this paper. For comprehensive background, we direct the reader to [CT06]. Unless noted otherwise, all logarithms are base 2.

Definition 2.1 (Entropy)**.** *The entropy of a random variable X is defined as*

$$H(X) := \sum_x \Pr[X = x] \log \frac{1}{\Pr[X = x]}.$$

Similarly, the conditional entropy is defined as

$$H(X|Y) := \mathbb{E}_Y \left[\sum_x \Pr[X = x|Y = y] \log \frac{1}{\Pr[X = x|Y = y]} \right].$$

Fact 2.2 (Conditioning Decreases Entropy)**.** *For any random variables X and Y*

$$H(X) \geq H(X|Y)$$

With entropy defined, we can also quantify the correlation between two random variables, or how much information one random variable conveys about the other.

Definition 2.3 (Mutual Information)**.** *Mutual information between X and Y (conditioned on Z) is defined as*

$$I(X;Y|Z) := H(X|Z) - H(X|YZ).$$

Similarly, we can also define how much one distribution conveys information about the other distribution.

Definition 2.4 (KL-Divergence)**.** *KL-Divergence between two distributions μ and ν is defined as*

$$\mathsf{D}_{KL}(\mu||\nu) := \sum_x \mu(x) \log \frac{\mu(x)}{\nu(x)}.$$

To bound mutual information, it suffices to bound KL-divergence, due to the following fact.

Fact 2.5 (KL-Divergence and Mutual Information)**.** *The following equality between mutual information and KL-Divergence holds*

$$I(A;B|C) = \mathbb{E}_{B,C} \left[\mathsf{D}_{KL}(A|_{B=b,C=c}||A|_{C=c}) \right].$$

Fact 2.6 (Pinsker's Inequality)**.** *For any two distributions P and Q,*

$$\|P - Q\|_{TV} = \frac{1}{2}\|P - Q\|_1 \leq \sqrt{\frac{1}{2\log e} D(P||Q)}$$

We also make use of the following facts on Mutual Information throughout the paper.

Fact 2.7 (Chain Rule)**.** *For any random variables A, B, C and D*

$$I(AD; B|C) = I(D; B|C) + I(A; B|CD).$$

Fact 2.8. *For any random variables A, B, C and D, if $I(B; D|C) = 0$*

$$I(A; B|C) \leq I(A; B|CD).$$

Proof. By the chain rule and non-negativity of mutual information,

$$I(A; B|C) \leq I(AD; B|C) = I(B; D|C) + I(A; B|CD) = I(A; B|CD).$$

□

Fact 2.9. *For any random variables A, B, C and D, if $I(B; D|AC) = 0$*

$$I(A; B|C) \geq I(A; B|CD).$$

Proof. By the chain rule and non-negativity of mutual information,

$$I(A; B|CD) \leq I(AD; B|C) = I(A; B|C) + I(B; D|AC) = I(A; B|C).$$

□

We will also use the following version of Chernoff bound.

Fact 2.10 (Chernoff bound)**.** *Let $X_1, \ldots, X_n$ be n independent random variables with $X_i \in \{0, 1\}$ and $\Pr[X_i = 1] = p$ for all $i \in [n]$. Then for any $\varepsilon > 0$ with $\varepsilon < 1 - p$, we have*

$$\Pr\left[\sum_{i\in[n]} X_i \geq (p + \varepsilon)n\right] \leq \exp\left(-\frac{n}{\log_2 e} \cdot D\left(\mathsf{Ber}(p + \varepsilon)||\mathsf{Ber}(p)\right)\right)$$

where $\mathsf{Ber}(p)$ refers to the Bernoulli distribution with probability p.

2.2 Min-Entropy

Definition 2.11. *We define the Rényi entropy $H_2(A)$ and min-entropy $H_\infty(A)$ as*

$$H_2(A) := -\log\left(\sum_a \Pr[A = a]^2\right)$$
$$H_\infty(A) := -\log\left(\max_a \Pr[A = a]\right)$$

Fact 2.12 (Rényi Entropy)**.** *Let A be a random variable. Then*

$$H(A) \geq H_2(A) \geq H_\infty(A)$$

In particular, for any fixed b we have

$$H_2(A|B=b) \geq H_\infty(A|B=b)$$

We use the following lemma on "average" min-entropy.

Definition 2.13 (Average Min-Entropy)**.**

$$\widetilde{H}_\infty(A|B) := -\log\left(\mathbb{E}_{b\sim B}\left[\max_a \Pr[A=a|B=b]\right]\right) = -\log\left(\mathbb{E}_{b\sim B}\left[2^{-H_\infty(A|B=b)}\right]\right)$$

Lemma 2.14 (Lemma 2.2 of [DORS08])**.** *Let A, B, C be random variables. Then if B has at most 2^λ possible values, then*

$$\widetilde{H}_\infty(A|B,C) \geq \widetilde{H}_\infty(A,B|C) - \lambda \geq \widetilde{H}_\infty(A|C) - \lambda.$$

In particular,

$$\widetilde{H}_\infty(A|B) \geq \widetilde{H}_\infty(A,B) - \lambda \geq H_\infty(A) - \lambda.$$

Claim 2.15.

$$\widetilde{H}_\infty(A|B,C) \leq \widetilde{H}_\infty(A|B)$$

Proof. We first proceed with showing the following inequality,

$$\mathbb{E}_{c\sim C|_{B=b}}\left[\max_a \Pr[A=a|B=b,C=c]\right] \geq \max_a \Pr[A=a|B=b]. \tag{3}$$

which is a standard fact about the max function. Let $a^* := \arg\max_a \Pr[A=a|B=b]$. Then

$$\Pr[A=a^*|B=b] = \mathbb{E}_{c\sim C|_{B=b}}\left[\Pr[A=a^*|B=b,C=c]\right] \leq \mathbb{E}_{c\sim C|_{B=b}}\left[\max_a \Pr[A=a|B=b,C=c]\right]$$

With (3) established, we are ready to prove the claim. Recall that

$$\widetilde{H}_\infty(A|B,C) := -\log\left(\mathbb{E}_{b,c\sim B,C}\left[\max_a \Pr[A=a|B=b,C=c]\right]\right)$$

Taking expectation over B on both sides of (3), we have

$$\mathbb{E}_{b,c\sim B,C}\left[\max_a \Pr[A=a|B=b,C=c]\right] \geq \mathbb{E}_{b\sim B}\left[\max_a \Pr[A=a|B=b]\right]$$

Therefore, we get

$$\begin{aligned}\widetilde{H}_\infty(A|B,C) &= -\log\left(\mathbb{E}_{b,c\sim B,C}\left[\max_a \Pr[A=a|B=b,C=c]\right]\right)\\ &\leq -\log\left(\mathbb{E}_{b\sim B}\left[\max_a \Pr[A=a|B=b]\right]\right) = \widetilde{H}_\infty(A|B)\end{aligned}$$

□

Claim 2.16 (Claim 2.12 of [Ko25a])**.** *Let $\mathcal{D}$ be a distribution and $\mathcal{U}$ a uniform distribution over some $\mathcal{S} \subset \{0,1\}^n$. Then if $D(\mathcal{D}||\mathcal{U}) < t$ with $t > 1$, then for every $\alpha > 2$ there exists an event E such that*

$$\begin{aligned}\mathcal{D}(E) &\geq 1 - \frac{1}{\alpha}\\ H_\infty(\mathcal{D}|_E) &\geq \log|\mathcal{S}| - 2\alpha t\end{aligned}$$

3 Main Proof

In this section, we prove our main theorem, a slightly stronger statement than in Section 1.1.

Theorem 1.1. *For the Multiphase Problem with f Inner Product over $\mathbb{F}_2$, with $m = n^{1+\Omega(1)}$, if $t_u \leq \log^{\kappa} n$ for some large constant $\kappa > 0$, then*

$$t_{tot} \geq \Omega\left(\left(\frac{\log n}{\log\log n}\right)^2\right)$$

Before we delve into the proof of the main theorem, we introduce formal notation and the model necessary for the proof.

Epochs To give a super-logarithmic lower bound, the first main technical component is the Chronogram technique [FS89], where we divide the sequence of n updates into epochs, each containing $n_i := \beta^i$ updates, with $\sum_{i=1}^{\ell} n_i = n$. Then observe that $\ell := \log_\beta n = \frac{\log n}{\log \beta}$.

For each epoch of n_i updates, denoted as $X^{(i)}$, the update algorithms will use $t_u n_i$ cell-probe operations (write operations) to overwrite the memory. We denote the epochs of updates as $\{U_i\}_{i=1}^{\ell}$, each of size $|U_i| = w \cdot t_u n_i$, and we process the updates in reverse order, that is, the larger epochs get processed first.

The essence of the Chronogram technique is that every query algorithm can be decomposed in the following manner. Let C_i denote the cells last updated in epoch i. The query algorithm for the query q will then probe into $C_1, \ldots, C_\ell$. We will denote $t_q[i]$ as the number of probes the query for $q \in \mathcal{Q}$ makes into C_i. Then it must be the case that

$$\sum_{i=1}^{\ell} t_q[i] \leq t_{tot}$$

Communication Model We define the following 2.5-round Multiphase Communication Game, as an extension of 1.5-round Multiphase Communication Game introduced in [CEEP12]. This replaces the one-way communication model used in [LWY20, LY25] for the lower bound.

- Alice holds $\vec{S}$. Bob holds X. Merlin holds $\vec{S}$ and X.
- Merlin sends U to Bob.
- As the 0.5-round message, Bob simply forwards $\Phi(U)$, a message that depends only on U and independent randomness, to Alice.
- $q \in \mathcal{Q}$ is then revealed to both Alice and Bob. Alice sends a message A_q to Bob. Then Bob outputs the estimate $B_q \in \{\pm 1\}$ for $f(S_q, X)$.

Protocol 3: 2.5-round Multiphase Communication Game

Advantage of the Protocol We will be considering a fixed $\vec{S}$ for the simulation theorem, while for the lower bound analysis, we will assume that these $\vec{S}$ are distributed uniformly at random. Regardless of the chosen $\vec{S}$, we will be using a uniform distribution over X as the update, and a

uniform distribution over $\mathcal{Q}$ as the possible query. And for the sake of simplicity, we restrict to balanced functions f.[4] That is, for any S_Q,

$$\mathbb{E}_X [f(S_Q, X)] = 0$$

Under the distribution, we will measure the advantage of the 2.5-round protocol Π.

Definition 3.1. *The advantage of 2.5-round protocol $\Pi = (\Phi(U), A_Q, B_Q)$ over the distribution Q over the queries is defined as*

$$\mathsf{adv}(G_f, \Pi) := \mathbb{E}_{Q,\Phi(U),A_Q,B_Q} \left[\mathbb{E}_{(S_Q,X)|\Phi(U),A_Q,B_Q} [B_Q \cdot f(S_Q, X)] \right]$$

where $B_Q \in \{\pm 1\}$ is Bob's final estimate.

For the rest of the section, we prove the simulation theorem (Section 3.1) showing any efficient data structure yields an efficient 2.5-round protocol achieving good advantage. This results in a contradiction via information-theoretic arguments (Section 3.2).

3.1 Simulation Theorem

First, we show the following simulation theorem, which argues that an efficient dynamic data structure implies an efficient 2.5-round Multiphase Communication Game protocol Π with large advantage.

Theorem 3.2 (New Simulation Theorem)**.** *Fix $\vec{S}$. If there exists a data structure for the Multiphase problem f with t_{tot} query time, and t_u update time, then for any $p \in (0, 1/3)$ with $p \leq \frac{1}{4t_u w}$, there exists a 2.5-round Multiphase Communication Game protocol Π with*

$$|U| \leq w \cdot t_u n + \log \ell, \ |\Phi(U)| \leq n - (1 - 2p \cdot w t_u - o(1))\sqrt{n}, \ |A_q| \leq O(t_{tot} \cdot w)$$

while achieving the advantage

$$\mathsf{adv}(G_f, \Pi) \geq \Omega\left(\left(\exp\left(-\frac{200 \cdot t_{tot}}{\ell} \cdot \ln(t_{tot}) - \frac{100 \cdot t_{tot}}{\ell} \cdot \ln \frac{1}{p} \right) \right) - \exp\left(-\Omega(pn)\right) \right)$$

Proof. Suppose there exists a dynamic data structure for the Multiphase Problem f with t_{tot} query time and t_u update time. We want to then simulate the data structure with 2.5-round Multiphase Communication Game, in the following manner.

[4]While it is possible to extend the definition and our technique to non-balanced functions, doing so would significantly compromise the simplicity of the argument. Consequently, we restrict our analysis to balanced functions.

- First Merlin chooses $i \in [2\ell/3, \ell]$, which satisfies

$$\mathbb{E}_{q \in \mathcal{Q}|\vec{S},X}\left[t_q[i]\right] \leq 10 \cdot t_{tot}/\ell.$$

  Note that by a simple averaging argument, such i is guaranteed to exist. Merlin then forwards $U = U_1, \ldots, U_\ell$ along with the index i to Bob. Bob from U can construct $C_1, \ldots, C_\ell$.

- As the 0.5-round message, Bob sends the following. For C_i, he samples each cell with probability p at random, and creates $\widetilde{C}_i$. If $\left|\widetilde{C}_i\right| > 2p \cdot wt_u \cdot n_i$, then Bob simply aborts, and outputs FAIL. Otherwise, forward $X^{(>i)}, C_{<i}$ and $\widetilde{C}_i$ along with i (which is evident in the message already) to Alice. Observe that the message only depends on U, i and Bob's randomness, no dependence on q.

- Alice does the following.
  - Using $\vec{S}$, and $X^{(>i)}$, the first $\ell - i$ epochs of updates, Alice constructs $U_{>i}$ from $X^{(>i)}$.
  - Choose distinct probe times uniformly at random $r_1 < \ldots < r_{\tilde{t}_q} \in [t_{tot}]$ where $\tilde{t}_q \leq \frac{100 \cdot t_{tot}}{\ell}$ from $\binom{t_{tot}}{\leq \frac{100 \cdot t_{tot}}{\ell}}$ possible choices.
  - Alice simulates the query algorithm for $q \in \mathcal{Q}$ under $\vec{S}$, generating the query transcript

$$A_q := ((a_1, c_1), \ldots, (a_{t_{tot}}, c_{t_{tot}}), z_{out})$$

    where a_i refers to the address and c_i refers to its content, z_{out} refers to the final output of the query algorithm, with the following caveat. For the probe time r_j, check if its address a_{r_j} is in $\widetilde{C}_i$. If the address does not exist in $\widetilde{C}_i$, abort the simulation. Signal FAIL to Bob. Then Bob also signals FAIL. Otherwise, proceed.
  - If successful, send the query transcript A_q to Bob, along with the indices $r_1 < \ldots < r_{\tilde{t}_q}$.

- Then Bob simply verifies A_q. That is, check if (a_τ, c_τ) matches with U for all $\tau \in [t_{tot}]$, along with the indices $r_1 < \ldots < r_{\tilde{t}_q}$.[5] Check if (a_{r_j}, c_{r_j}) for all $j \in [\tilde{t}_q]$ indeed exists in C_i, and for $\tau \in [t_{tot}] \backslash \{r_1, \ldots, r_{\tilde{t}_q}\}$ the cell address a_τ does not exist in C_i. If yes, then declare z_{out} as the answer B_q. Otherwise, output FAIL.

- If the protocol signals FAIL, Bob outputs an independent random guess as B_q.

Protocol 4: Simulation Protocol Π

The cost guarantee of the protocol is straightforward. Merlin's message is simply the update with an index $i \in [2\ell/3, \ell]$. Therefore $|U| \leq t_u wn + \log \ell = O(t_u wn)$. We bound the length of Bob's 0.5-round message.

$$\begin{aligned} |\Phi(U)| &= \left|X^{(>i)}\right| + |C_{<i}| + \left|\widetilde{C}_i\right| \leq \sum_{k>i} n_k + \sum_{k<i} (wt_u) \cdot n_k + 2p \cdot wt_u \cdot n_i \\ &\leq (n - n_i) + 2p \cdot wt_u \cdot n_i + o(n_i) \end{aligned} \tag{4}$$

where the upper bound follows the guarantee of the epoch size with $n_i := \beta^i = \left((t_u w)^{\Theta(1)}\right)^i$. $\sum_{k<i} (wt_u) \cdot n_k \leq o(n_i)$ as it is a geometric series. As Merlin chooses $i \in [2\ell/3, \ell]$, $n_i = \beta^i \geq$

[5] Note that if the cell a_τ is never updated by U, Alice's content c_τ must be correct, as Alice holds $\vec{S}$.

$\beta^{2\ell/3} \geq 2^{\log n/2} = \sqrt{n}$. Therefore, assuming $1 - 2p \cdot wt_u - o(1) > 0$, as we will choose the parameters accordingly, (4) becomes

$$(4) \leq n - (1 - 2p \cdot wt_u - o(1))n_i \leq n - (1 - 2p \cdot wt_u - o(1))\sqrt{n}. \tag{5}$$

Next, we bound the length of Alice's message,

$$|A_q| = 2w \cdot t_{tot} + 1 + \tilde{t}_q \log(t_{tot}) \leq 3w \cdot t_{tot}. \tag{6}$$

(5) and (6) give the desired bound on the cost of Π. Now we proceed to showing the lower bound of $\mathsf{adv}(G_f, \Pi)$ by considering the probability of Alice outputting the correct transcript.

Claim 3.3.

$$\mathsf{adv}(G_f, \Pi) \geq \Omega\left(\left(\exp\left(-\frac{200 \cdot t_{tot}}{\ell} \cdot \ln(t_{tot}) - \frac{100 \cdot t_{tot}}{\ell} \cdot \ln\frac{1}{p}\right)\right) - \exp\left(-\Omega(pn)\right)\right)$$

Proof. Recall that we have fixed $\vec{S}$. Merlin chose $i \in [2\ell/3, \ell]$ such that

$$\mathbb{E}_{\mathcal{Q}|\vec{S},X}\left[t_q[i]\right] \leq 10 \cdot t_{tot}/\ell.$$

If the chosen query $q \in \mathcal{Q}$ has $t_q[i] > \frac{100 t_{tot}}{\ell}$, then our simulation will always output FAIL. As Alice's guess $\tilde{t}_q < t_q[i]$, there must exist a probe where Alice should be probing C_i, but Alice is probing otherwise. The transcript probes into C_{-i} (in fact into $C_{>i}$, as then such cell cannot exist in $C_{<i}$) instead. Bob will catch such A_q as he has a complete knowledge of $C_1, \ldots, C_i, \ldots, C_\ell$. Therefore, Bob will always output FAIL, yielding zero advantage for this set of queries. But due to Markov's argument, there are at most a $1/10$ fraction of such queries in $\mathcal{Q}$.

For the rest of the queries, it is guaranteed that $t_q[i] \leq \frac{100 t_{tot}}{\ell}$. Note that a non-trivial guess would only be given when Alice guesses $r_1 < \ldots < r_{\tilde{t}_q}$'s correctly, and Bob actually successfully sampled these cells in $\widetilde{C}_i$ as well. Otherwise, Bob will reject Alice's guess, and output FAIL, leading to zero advantage.

Therefore, to analyze the advantage, we simply need to lower bound the probability of Alice transmitting the correct query transcript, in which case Bob outputs the correct guess.

The probability that Alice guesses $r_1 < \ldots < r_{\tilde{t}_q}$'s correctly is lower bounded by the term

$$\binom{t_{tot}}{\leq \frac{100 \cdot t_{tot}}{\ell}}^{-1} \geq \left((t_{tot}+1)^{-\left(\frac{100 \cdot t_{tot}}{\ell}\right)}\right) \geq \exp\left(-\frac{200 t_{tot}}{\ell} \cdot \ln(t_{tot})\right). \tag{7}$$

where the first inequality follows from a standard sums of binomial coefficients bound, (i.e., $\binom{n}{\leq r} \leq (n+1)^r$).

Given that Alice guessed $r_1 < \ldots < r_{\tilde{t}_q}$'s correctly (observe that otherwise, Bob would output FAIL), Alice will then transmit the correct transcript if and only if all the required cells in C_i are included in Bob's message $\widetilde{C}_i$. For any other probes, Alice, due to $\Phi(U)$, can simulate the queries that are from $C_1, \ldots, C_{i-1}, C_{i+1}, \ldots, C_\ell$. The only part of her query that she cannot simulate is those from C_i, unless they are included in $\widetilde{C}_i$.

The probability of $a_{r_1}, \ldots, a_{r_{\tilde{t}_q}}$ (as they are conditioned to be in C_i) being included in $\widetilde{C}_i$ then depends on Bob's private randomness. This is independent of Alice's private randomness. The probability is lower bounded by

$$p^{\left(\frac{100 \cdot t_{tot}}{\ell}\right)} - \exp\left(-\Omega(n \cdot D(\mathsf{Ber}(2p)||\mathsf{Ber}(p)))\right) \geq \exp\left(\frac{100 \cdot t_{tot}}{\ell} \cdot \ln p\right) - \exp(-\Omega(pn))$$

where a standard estimate $D(\mathsf{Ber}(2p)||\mathsf{Ber}(p)) = \Theta(p)$ holds.

Multiplying the two probabilities, we get the probability of Alice correctly guessing and Bob sampling "correct" cells in $\widetilde{C}_i$ as

$$\mathsf{adv}(G_f, \Pi) \geq \Omega\left(\exp\left(-\frac{200t_{tot}}{\ell} \cdot \ln(t_{tot}) - \frac{100 \cdot t_{tot}}{\ell} \cdot \ln\frac{1}{p}\right)\right) - \exp\left(-\Omega(pn)\right) \tag{8}$$

which then completes the proof of the claim. □

(5), (6) and Claim 3.3 complete the proof of the simulation theorem.

□

Now we would like to select a range of parameters to derive a contradiction.

Corollary 3.4. *Set* $t_{tot} = o\left(\left(\frac{\log n}{\log\log n}\right)^2\right)$, $t_u = \log^\kappa(n)$ *for some constant* $\kappa > 3$, $\beta = (w \cdot t_u)^{\Theta(1)}$, $p := \beta^{-1}/2$. *Then*

$$|U| \leq O(n\log^{\kappa+1}(n)),\ |\Phi(U)| \leq n - \frac{\sqrt{n}}{2},\ |A_q| \leq o(\log^3(n))$$

while having

$$\mathsf{adv}(G_f, \Pi) \geq n^{-o(1)}.$$

Proof. If we choose $\ell := \log_\beta(n) = \frac{\log n}{\log\beta}$, $\beta = (t_u w)^{\Theta(1)}$, and $t_{tot} = o\left(\left(\frac{\log n}{\log\log n}\right)^2\right)$, and with the sampling probability $p := \beta^{-1}/2$, as t_u will be in the poly-logarithmic regime,

$$\begin{aligned}
&|U| \leq O(wnt_u) \leq O(n\log^{\kappa+1}(n)) \\
&|\Phi(U)| \leq n - (1-o(1))\sqrt{n} \leq n - \frac{\sqrt{n}}{2} \\
&|A_q| \leq O(t_{tot} \cdot w) \leq o(\log^3 n),
\end{aligned}$$

while the advantage (8) becomes

$$(8) \geq \Omega\left(\exp\left(-o(\log n)\right)\right) - \exp\left(-\Omega(n/\mathrm{poly}\log(n))\right) \geq n^{-o(1)}.$$

□

3.2 2.5-round Multiphase Communication Game Lower Bound

The goal of this section is to show that such an advantage is impossible, using the framework of [KW20, Ko25a] and finally [Ko25b]. The key idea, developed across [KW20, Ko25a, Ko25b], is to extract a random variable Z containing the output Z_{out} from the 2.5-round protocol such that (a) the min-entropy of S_Q and X conditioned on Z is large; (b) while maintaining $I(S_Q; X|Z)$ to be small. Then it must be the case that $\mathbb{E}_{(S_Q,X)|Z}\left[Z_{out} \cdot f(S_Q, X)\right]$ is small. We follow the analogous argument, by selecting the Z as the following

$$Z := \Phi(U), A_{\mathcal{Q}_{all}}, S_{<Q}, B_Q, Q$$

where Q is chosen uniformly at random from $\mathcal{Q} = [m]$ with $m = n^{1+\Omega(1)}$. $A_{\mathcal{Q}_{all}}$ refers to A_q for all $q \in \mathcal{Q}$, and $S_{<Q}$ refers to $S_1, \ldots, S_{Q-1}$. Note that B_Q essentially acts as the final output of the random variable. We need to include A_q for all $q \in \mathcal{Q}$ to apply direct-sum techniques.

First, we start by showing that Corollary 3.4 implies the following claim on the advantage conditioned on Z.

Claim 3.5.

$$\mathbb{E}_Z\left[\left|\mathbb{E}_{(S_Q,X)|Z}\left[\chi_{S_Q}(X)\right]\right|\right] \geq n^{-o(1)}$$

where $\chi_{S_Q}(X) := (-1)^{\langle S_Q, X\rangle}$.

Proof. As Q is chosen uniformly at random, Corollary 3.4 guarantees that for any fixed $\vec{S}$,

$$\mathbb{E}_{\Phi(U),A_Q,B_Q,Q|\vec{S}}\left[B_Q \cdot \chi_{S_Q}(X)\right] \geq n^{-o(1)}$$

This then implies

$$\begin{aligned}
n^{-o(1)} &\leq \mathbb{E}_{\Phi(U),A_Q,B_Q,Q,\vec{S}}\left[\mathbb{E}_{X|\Phi(U),A_Q,B_Q,Q,\vec{S}}\left[B_Q \cdot \chi_{S_Q}(X)\right]\right] \\
&= \mathbb{E}_{\Phi(U),A_Q,B_Q,Q,S_{<Q},S_Q}\left[\mathbb{E}_{X|\Phi(U),A_Q,B_Q,Q,S_{<Q},S_Q}\left[B_Q \cdot \chi_{S_Q}(X)\right]\right] \\
&= \mathbb{E}_{\Phi(U),A_Q,B_Q,Q,S_{<Q}}\left[\mathbb{E}_{(S_Q,X)|\Phi(U),A_Q,B_Q,Q,S_{<Q}}\left[B_Q \cdot \chi_{S_Q}(X)\right]\right] \\
&\leq \mathbb{E}_{\Phi(U),A_Q,B_Q,Q,S_{<Q}}\left[\left|\mathbb{E}_{(S_Q,X)|\Phi(U),A_Q,B_Q,Q,S_{<Q}}\left[\chi_{S_Q}(X)\right]\right|\right]
\end{aligned}$$

But then

$$\begin{aligned}
n^{-o(1)} &\leq \mathbb{E}_{\Phi(U),A_Q,B_Q,Q,S_{<Q}}\left[\left|\mathbb{E}_{(S_Q,X)|\Phi(U),A_Q,B_Q,Q,S_{<Q}}\left[\chi_{S_Q}(X)\right]\right|\right] \\
&\leq \mathbb{E}_{\Phi(U),A_{\mathcal{Q}_{all}},B_Q,Q,S_{<Q}}\left[\left|\mathbb{E}_{(S_Q,X)|\Phi(U),A_{\mathcal{Q}_{all}},B_Q,Q,S_{<Q}}\left[\chi_{S_Q}(X)\right]\right|\right] \\
&= \mathbb{E}_Z\left[\left|\mathbb{E}_{(S_Q,X)|Z}\left[\chi_{S_Q}(X)\right]\right|\right]
\end{aligned}$$

where the inequality follows from Jensen's inequality on the convex function, $|\cdot|$.

□

We now show that Claim 3.5 leads to a contradiction.

3.2.1 Small Information on S_Q

First, we would like to show that the min-entropy of S_Q conditioned on Z is large. The statement is not true in general. However, a simple Markov argument allows us to "extract" a good event E_Q. We start with the following standard claim on the mutual information.

Claim 3.6.

$$I(S_Q; \Phi(U), A_{\mathcal{Q}_{all}}, S_{<Q}, Q) \leq 4w \cdot t_{tot}$$

Proof. Due to a standard direct sum trick, as Q is chosen independently at random, $S_1, \ldots, S_m$ are i.i.d, we know

$$\begin{aligned}
I(S_Q; \Phi(U), A_{\mathcal{Q}_{all}}, S_{<Q}, Q) &= \underbrace{I(S_Q; S_{<Q}, Q)}_{=0} + I(S_Q; \Phi(U), A_{\mathcal{Q}_{all}} | S_{<Q}, Q) \\
&= \mathbb{E}_Q\left[I(S_Q; \Phi(U), A_{\mathcal{Q}_{all}} | S_{<Q})\right]
\end{aligned}$$

Then we can bound $\mathbb{E}_Q\left[I(S_Q; \Phi(U), A_{\mathcal{Q}_{all}} | S_{<Q})\right]$ as

$$\begin{aligned}
\mathbb{E}_Q\left[I(S_Q; \Phi(U), A_{\mathcal{Q}_{all}} | S_{<Q})\right] = \frac{1}{m} \cdot I(\vec{S}; \Phi(U), A_{\mathcal{Q}_{all}}) &\leq \underbrace{\frac{|\Phi(U)|}{m}}_{\leq \frac{n}{m} = n^{-\Omega(1)} = o(1)} + \frac{m\,|A_q|}{m} \\
&= o(1) + 3w \cdot t_{tot} \leq 4w \cdot t_{tot}
\end{aligned}$$

where the first inequality follows from $I(\vec{S}; \Phi(U), A_{\mathcal{Q}_{all}}) \leq H(\Phi(U), A_{\mathcal{Q}_{all}}) \leq |\Phi(U)| + m\,|A_q|$, completing the proof of the claim. □

Unfortunately, we cannot simply use the mutual information, and the related KL divergence for our proof. Since we are considering "small" advantage regime, we need to argue that the min-entropy of S_Q conditioned on Z, B_Q is large as in [Ko25a]. We will use the following lemma to extract "good" event in terms of min-entropy.

Lemma 3.7 (S_Q min-entropy)**.** *For every setting of the parameter $\alpha \in (0, \frac{1}{10})$, there exist events E^1_Q and E^2_Q such that*

$$H(E^1_Q|\Phi(U), A_{\mathcal{Q}_{all}}, S_{<Q}, Q) = H(E^2_Q|\Phi(U), A_{\mathcal{Q}_{all}}, S_{<Q}, S_Q, Q) = 0$$

and

$$\Pr\left[E^1_Q\right] \geq 1-\alpha, \quad \Pr\left[E^2_Q \mid \Phi(U), A_{\mathcal{Q}_{all}}, S_{<Q}, Q, E^1_Q = 1\right] \geq 1-\alpha$$
$$H_\infty(S_Q|\Phi(U), A_{\mathcal{Q}_{all}}, S_{<Q}, Q, E_Q = 1) \geq n - \frac{8w \cdot t_{tot}}{\alpha^2}$$

where we denote $E^1_Q = 1, E^2_Q = 1$ as $E_Q = 1$ for short.

Proof. First we define the event E^1_Q, which is defined as a set of $\Phi(U), A_{\mathcal{Q}_{all}}, S_{<Q}, Q$'s such that

$$D(S_Q|_{\Phi(U), A_{\mathcal{Q}_{all}}, S_{<Q}, Q}||S_Q) \leq \frac{4w \cdot t_{tot}}{\alpha}$$

Due to Claim 3.6,

$$I(S_Q; \Phi(U), A_{\mathcal{Q}_{all}}, S_{<Q}, Q) = \mathbb{E}_{\Phi(U), A_{\mathcal{Q}_{all}}, S_{<Q}, Q}\left[D(S_Q|_{\Phi(U), A_{\mathcal{Q}_{all}}, S_{<Q}, Q}||S_Q)\right] \leq 4w \cdot t_{tot}$$

a simple Markov's inequality would imply $\Pr[E^1_Q] \geq (1-\alpha)$. Then if E^1_Q is set to true, we consider a setting of event E^2_Q given by Claim 2.16. As $E^1_Q = 1$ guarantees

$$D(S_Q|_{\Phi(U), A_{\mathcal{Q}_{all}}, S_{<Q}, Q, E^1_Q = 1}||S_Q) = D(S_Q|_{\Phi(U), A_{\mathcal{Q}_{all}}, S_{<Q}, Q}||S_Q) \leq \frac{4w \cdot t_{tot}}{\alpha}$$

where the equality holds as E^1_Q is a deterministic function of $\Phi(U), A_{\mathcal{Q}_{all}}, S_{<Q}, Q$, Claim 2.16 generates an event E^2_Q such that

$$\Pr[E^2_Q \mid \Phi(U), A_{\mathcal{Q}_{all}}, S_{<Q}, Q, E^1_Q = 1] \geq 1-\alpha$$
$$H(E^2_Q|S_Q, \Phi(U), A_{\mathcal{Q}_{all}}, S_{<Q}, Q, E^1_Q = 1) = 0$$
$$H_\infty(S_Q|\Phi(U), A_{\mathcal{Q}_{all}}, S_{<Q}, Q, E^1_Q = 1, E^2_Q = 1) \geq n - \frac{8w \cdot t_{tot}}{\alpha^2}$$

which completes the proof of the lemma. □

3.2.2 Small Information on X

Then we would like to show that $\widetilde{H}_\infty(X|Z, E_Q = 1)$ is large. Here, we remark that we need to have a conditioning $E_Q = 1$ to deduce the contradiction.

Lemma 3.8.

$$\widetilde{H}_\infty(X|Z, E_Q = 1) \geq n - |\Phi(U)| - 10\alpha - 1$$

Proof. Recall that as X is chosen uniformly at random, regardless of chosen Q and $\vec{S}$,

$$H_\infty(X|\vec{S}, Q) = n$$

while Lemma 2.14 implies that

$$\widetilde{H}_\infty(X|\vec{S}, \Phi(U), Q) \geq n - |\Phi(U)|.$$

But $\vec{S}, \Phi(U), Q$ and Alice's independent private randomness determine $A_{\mathcal{Q}_{all}}$. That is $A_{\mathcal{Q}_{all}}$ is determined by Alice's private randomness and $\vec{S}, \Phi(U)$. Therefore,

$$I(X; A_{\mathcal{Q}_{all}}|\vec{S}, \Phi(U), Q) = 0.$$

And $\vec{S}, A_{\mathcal{Q}_{all}}, \Phi(U), Q$ contains $S_Q, \Phi(U), A_{\mathcal{Q}_{all}}, S_{<Q}, Q$, which determines both E_Q^1 and E_Q^2. Therefore,

$$\widetilde{H}_\infty(X|\vec{S}, A_{\mathcal{Q}_{all}}, \Phi(U), E_Q, Q) \geq n - |\Phi(U)|$$

Then by the definition of average min-entropy we have the following equality.

$$\begin{aligned} 2^{-\widetilde{H}_\infty(X|\vec{S}, A_{\mathcal{Q}_{all}}, \Phi(U), E_Q, Q)} &= \Pr[E_Q = 1] \cdot 2^{-\widetilde{H}_\infty(X|\vec{S}, A_{\mathcal{Q}_{all}}, \Phi(U), E_Q = 1, Q)} \\ &\quad + \Pr[E_Q = 0] \cdot 2^{-\widetilde{H}_\infty(X|\vec{S}, A_{\mathcal{Q}_{all}}, \Phi(U), E_Q = 0, Q)} \end{aligned}$$

which implies the following inequality

$$\widetilde{H}_\infty(X|\vec{S}, A_{\mathcal{Q}_{all}}, \Phi(U), E_Q = 1, Q) \geq \log\left(\Pr[E_Q = 1]\right) + \widetilde{H}_\infty(X|\vec{S}, A_{\mathcal{Q}_{all}}, \Phi(U), E_Q, Q) \tag{9}$$

The left hand side term of (9) is upper bounded by

$$\widetilde{H}_\infty(X|\vec{S}, A_{\mathcal{Q}_{all}}, \Phi(U), E_Q = 1, Q) \leq \widetilde{H}_\infty(X|S_{<Q}, A_{\mathcal{Q}_{all}}, \Phi(U), E_Q = 1, Q)$$

due to Claim 2.15.

Lemma 3.7 guarantees that $\Pr[E_Q = 1] \geq (1 - \alpha)^2 \geq 1 - 2\alpha$. Then the right hand side of (9) is lower bounded by

$$\log\left(\Pr[E_Q = 1]\right) + \widetilde{H}_\infty(X|\vec{S}, A_{\mathcal{Q}_{all}}, \Phi(U), E_Q, Q) \geq \log(1 - 2\alpha) + n - |\Phi(U)| \geq n - |\Phi(U)| - 10\alpha.$$

where the last lower bound holds from $\alpha \in (0, 0.1)$, and $\log(1 - 2\alpha) \geq -10\alpha$ in this interval.

This implies the final inequality of

$$\widetilde{H}_\infty(X|S_{<Q}, A_{\mathcal{Q}_{all}}, \Phi(U), E_Q = 1, Q) \geq n - |\Phi(U)| - 10\alpha. \tag{10}$$

Again applying Lemma 2.14 to (10), we get

$$\widetilde{H}_\infty(X|S_{<Q}, A_{\mathcal{Q}_{all}}, \Phi(U), B_Q, E_Q = 1, Q) \geq n - |\Phi(U)| - 10\alpha - 1,$$

which completes the proof of the lemma. □

3.2.3 Small Correlation between S_Q and X

Finally, we show that S_Q and X are weakly correlated after conditioning on Z and $E_Q = 1$. We show the following lemma.

Lemma 3.9.

$$I(S_Q; X|Z, E_Q = 1) \leq \frac{1}{(1-\alpha)^2}\frac{|U|}{m}$$

Proof. We start by just plugging our Z into $I(S_Q; X|Z, E_Q = 1)$.

$$\begin{aligned} I(S_Q; X|Z, E_Q = 1) &\leq I(S_Q; XU|S_{<Q}, A_{\mathcal{Q}_{all}}, \Phi(U), B_Q, E_Q = 1, Q) \\ &\leq I(S_Q; XU|S_{<Q}, A_{\mathcal{Q}_{all}}, \Phi(U), E_Q = 1, Q) \end{aligned}$$

where the last inequality holds from Fact 2.9 with

$$I(S_Q; B_Q|XU, S_{<Q}, A_{\mathcal{Q}_{all}}, \Phi(U), E_Q = 1, Q) = 0,$$

as $U, A_{\mathcal{Q}_{all}}$ and Bob's independent random variable fully determines B_Q. That is depending on U, either A_Q's final output is picked as B_Q, or it is uniformly random $\{\pm 1\}$. Then we can further upper bound the term of interest as

$$\begin{aligned} &I(S_Q; XU|S_{<Q}, A_{\mathcal{Q}_{all}}, \Phi(U), E_Q = 1, Q) = I(S_Q; XU|S_{<Q}, A_{\mathcal{Q}_{all}}, \Phi(U), E_Q^1 = 1, E_Q^2 = 1, Q) \\ &\leq \frac{I(S_Q; XU|S_{<Q}, A_{\mathcal{Q}_{all}}, \Phi(U), E_Q^1 = 1, E_Q^2, Q)}{\Pr[E_Q^2 = 1|S_{<Q}, A_{\mathcal{Q}_{all}}, \Phi(U), E_Q^1 = 1, Q]} \leq \frac{I(S_Q; XU|S_{<Q}, A_{\mathcal{Q}_{all}}, \Phi(U), E_Q^1 = 1, Q)}{1-\alpha} \end{aligned}$$

where the last inequality holds from Fact 2.9 with

$$I(E_Q^2; XU|S_Q, S_{<Q}, A_{\mathcal{Q}_{all}}, \Phi(U), E_Q^1 = 1, Q) \leq H(E_Q^2|S_Q, S_{<Q}, A_{\mathcal{Q}_{all}}, \Phi(U), E_Q^1 = 1, Q) = 0$$

from Lemma 3.7. Now E_Q^1 is fully determined by $S_{<Q}, A_{\mathcal{Q}_{all}}, \Phi(U), Q$, and is 1 with probability at least $1 - \alpha$. Therefore

$$I(S_Q; XU|S_{<Q}, A_{\mathcal{Q}_{all}}, \Phi(U), E_Q^1 = 1, Q) \leq \frac{I(S_Q; XU|S_{<Q}, A_{\mathcal{Q}_{all}}, \Phi(U), Q)}{1-\alpha}.$$

Now finally, using the standard direct-sum technique, and the chain rule of Mutual Information (Fact 2.7), we get

$$\begin{aligned} I(S_Q; XU|S_{<Q}, A_{\mathcal{Q}_{all}}, \Phi(U), Q) &= \frac{1}{m}\sum_{q=1}^{m} I(S_q; XU|S_{<q}, A_{\mathcal{Q}_{all}}, \Phi(U)) = \frac{I(\vec{S}; XU|A_{\mathcal{Q}_{all}}, \Phi(U))}{m} \\ &\leq \frac{I(\vec{S}; XU|\Phi(U))}{m} \leq \frac{I(\vec{S}; XU)}{m} = \frac{I(\vec{S}; X) + I(\vec{S}; U|X)}{m} \leq \frac{|U|}{m} \end{aligned}$$

where the first inequality holds from Fact 2.9 with $I(A_{\mathcal{Q}_{all}}; XU|\vec{S}, \Phi(U)) = 0$. This is true as $\vec{S}, \Phi(U)$ and Alice's independent randomness determines Alice's message $A_{\mathcal{Q}_{all}}$. The second inequality holds again from Fact 2.9 with $I(\Phi(U); \vec{S}|XU) = 0$ as $\Phi(U)$ is fully determined by Bob's independent randomness and U. The final inequality holds from $I(\vec{S}; X) = 0$ and $I(\vec{S}; U|X) \leq |U|$.

Combining the inequalities we get

$$I(S_Q; X|Z, E_Q = 1) \leq \frac{1}{(1-\alpha)^2}\frac{|U|}{m}$$

our desired inequality. □

3.2.4 The main contradiction

We will use the following combinatorial lower bound from [Ko25a] which provides a combinatorial impossibility.

Lemma 3.10 (Lemma 3.10 of [Ko25a])**.** *Let X and Y be a distribution over $\{0,1\}^n$. For any $\gamma \geq 3$, if a random process $Z = z$ and A, which contains z_{out} satisfy the following inequalities*

$$\tilde{H}_\infty(Y|A, Z = z) + \tilde{H}_\infty(X|A, Z = z) \geq n + 2\gamma$$
$$I(Y; X|A, Z = z) \leq 2^{-2\gamma}$$

Then it must be the case that

$$\mathbb{E}_{A|Z=z}\left[\left|\mathbb{E}_{Y,X|_{A=a,Z=z}}\left[\chi_Y(X) \cdot z_{out}|A = a, Z = z\right]\right|\right] < 2^{-\gamma+2}$$

We attach the full proof of Lemma 3.10 in Section A for completeness. The following lemma completes the proof of Theorem 1.1.

Lemma 3.11. *If $m = n^{1+\Omega(1)}$, then no 2.5-round Multiphase Communication Game satisfying the parameters of Corollary 3.4 can exist.*

To see how Lemma 3.11 completes the proof of Theorem 1.1, the choice of parameters gives a 2.5-round protocol Corollary 3.4. However, Lemma 3.11 then argues that such protocol cannot exist. Therefore, this provides the claimed lower bound on t_{tot}.

Proof of Lemma 3.11. Recall that Corollary 3.4 implies Claim 3.5 or

$$\mathbb{E}_Z\left[\left|\mathbb{E}_{(S_Q,X)|Z}\left[\chi_{S_Q}(X)\right]\right|\right] \geq n^{-o(1)}.$$

with the parameters

$$|U| \leq O(n\log^{\kappa+1}(n)),\ |\Phi(U)| \leq n - \frac{\sqrt{n}}{2},\ |A_q| \leq o(\log^3(n)).$$

On the other hand, from Lemma 3.7, Lemma 3.8, Lemma 3.9, we get the following set of inequalities:

$$\widetilde{H}_\infty(X|Z, E_Q = 1) \geq n - |\Phi(U)| - 10\alpha - 1 \tag{11}$$
$$\widetilde{H}_\infty(S_Q|Z, E_Q = 1) \geq n - \frac{8w \cdot t_{tot}}{\alpha^2} - 1 \tag{12}$$
$$I(S_Q; X|Z, E_Q = 1) \leq \frac{1}{(1-\alpha)^2}\frac{|U|}{m} \tag{13}$$

where (12) simply follows from

$$\begin{aligned}\widetilde{H}_\infty(S_Q|Z, E_Q = 1) &= \widetilde{H}_\infty(S_Q|B_Q, \Phi(U), A_{\mathcal{Q}_{all}}, S_{<Q}, Q, E_Q = 1)\\ &\geq \widetilde{H}_\infty(S_Q|\Phi(U), A_{\mathcal{Q}_{all}}, S_{<Q}, Q, E_Q = 1) - 1 \geq n - \frac{8w \cdot t_{tot}}{\alpha^2} - 1\end{aligned}$$

where the first inequality holds from Lemma 2.14 and the second inequality follows from Lemma 3.7.

Adding (11) and (12), and plugging in the bounds for $|U|, |\Phi(U)|, |A_q|$, we obtain

$$\widetilde{H}_\infty(X|Z, E_Q = 1) + \widetilde{H}_\infty(S_Q|Z, E_Q = 1) \geq \frac{\sqrt{n}}{2} + \left(n - \frac{\log^3(n)}{\alpha^2}\right)$$
$$I(S_Q; X|Z, E_Q = 1) \leq O\left(\frac{1}{(1-\alpha)^2}\frac{n\log^{\kappa+1}(n)}{m}\right)$$

upon which we can invoke Lemma 3.10. By setting $\alpha := n^{-1/5}$, and $m := n^{1+\Omega(1)}$, our γ for Lemma 3.10 becomes $\gamma := \Theta(\log n)$. In particular, we get

$$\widetilde{H}_\infty(X|Z, E_Q = 1) + \widetilde{H}_\infty(S_Q|Z, E_Q = 1) \geq n + n^{\Theta(1)}$$
$$I(S_Q; X|Z, E_Q = 1) \leq 2^{-\Theta(\log n)}$$

Here, we remark that (13) is really the bottleneck for γ. This then implies

$$\mathbb{E}_{Z, E_Q=1}\left[\left|\mathbb{E}_{(S_Q,X)|Z,E_Q=1}\left[\chi_{S_Q}(X)\right]\right|\right] < n^{-\Omega(1)}.$$

However, this contradicts Claim 3.5, due to the following chain of inequalities.

$$\begin{aligned}
n^{-o(1)} &\leq \mathbb{E}_Z\left[\left|\mathbb{E}_{(S_Q,X)|Z}\left[\chi_{S_Q}(X)\right]\right|\right] \\
&\leq \mathbb{E}_Z\left[\Pr[E_Q = 1|Z = z] \cdot \left|\mathbb{E}_{(S_Q,X)|Z=z,E_Q=1}\left[\chi_{S_Q}(X)\right]\right|\right] \\
&+ \underbrace{\mathbb{E}_Z\left[\Pr[E_Q = 0|Z = z] \cdot \left|\mathbb{E}_{(S_Q,X)|Z=z,E_Q=0}\left[\chi_{S_Q}(X)\right]\right|\right]}_{\leq \mathbb{E}_Z\left[\Pr[E_Q=0|Z=z]\right] = \Pr[E_Q=0]} \\
&\leq \mathbb{E}_Z\left[\left|\mathbb{E}_{(S_Q,X)|Z,E_Q=1}\left[\chi_{S_Q}(X)\right]\right|\right] + \Pr[E_Q = 0] \\
&\leq \mathbb{E}_{Z,E_Q=1}\left[\left|\mathbb{E}_{(S_Q,X)|Z,E_Q=1}\left[\chi_{S_Q}(X)\right]\right|\right] + \|Z - Z|_{E_Q=1}\|_1 + \Pr[E_Q = 0] \qquad (14)
\end{aligned}$$

where the last inequality follows from the standard fact $|\mathbb{E}_X[f(X)] - \mathbb{E}_Y[f(Y)]| \leq \|f\|_\infty \cdot \|X - Y\|_1$. But $\|Z - Z|_{E_Q=1}\|_1$ can be upper bounded by

$$\begin{aligned}
&\|Z - Z|_{E_Q=1}\|_1 \\
&\leq \| \left(\Pr[E_Q = 1] \cdot Z|_{E_Q=1} + \Pr[E_Q = 0] \cdot Z|_{E_Q=0}\right) - \left(\Pr[E_Q = 1]Z|_{E_Q=1} + \Pr[E_Q = 0]Z|_{E_Q=1}\right) \|_1 \\
&\leq \Pr[E_Q = 0] \cdot \|Z|_{E_Q=0} - Z|_{E_Q=1}\|_1 \leq 2 \cdot \Pr[E_Q = 0]. \qquad (15)
\end{aligned}$$

Combining (14) with (15), results in the final contradiction, as

$$\begin{aligned}
n^{-o(1)} \leq (14) &\leq \mathbb{E}_{Z,E_Q=1}\left[\left|\mathbb{E}_{(S_Q,X)|Z,E_Q=1}\left[\chi_{S_Q}(X)\right]\right|\right] + 3 \cdot \Pr[E_Q = 0] \\
&\leq n^{-\Omega(1)} + O(\alpha) \leq n^{-\Omega(1)} \qquad (16)
\end{aligned}$$

The final inequality on $\Pr[E_Q = 0] = 1 - \Pr[E_Q = 1]$ follows from Lemma 3.7 as

$$\Pr[E_Q = 1] \geq (1 - \alpha)^2 \geq 1 - 2\alpha.$$

Setting $\alpha := n^{-1/5}$ completes the argument. However, (16) is a contradiction as the inequality states $n^{-o(1)} \leq n^{-\Omega(1)}$.

□

4 Acknowledgment

The author thanks Huacheng Yu for carefully reading an earlier draft of this paper and providing valuable feedback.

References

[BL15] Joshua Brody and Kasper Gren Larsen. Adapt or Die: Polynomial Lower Bounds for Non-Adaptive Dynamic Data Structures. *THEORY OF COMPUTING*, 11:19, 2015.

[BM13] Mark Braverman and Ankur Moitra. An information complexity approach to extended formulations. In *Proceedings of the forty-fifth annual ACM symposium on Theory of Computing*, pages 161–170, Palo Alto California USA, June 2013. ACM.

[Bra22] Mark Braverman. Communication and information complexity. *Proc. Int. Cong. Math. 2022*, 2022.

[BYJKS04] Ziv Bar-Yossef, T.S. Jayram, Ravi Kumar, and D. Sivakumar. An information statistics approach to data stream and communication complexity. *Journal of Computer and System Sciences*, 68(4):702–732, June 2004.

[CEEP12] Arkadev Chattopadhyay, Jeff Edmonds, Faith Ellen, and Toniann Pitassi. A Little Advice Can Be Very Helpful. In *Proceedings of the Twenty-Third Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 615–625. Society for Industrial and Applied Mathematics, January 2012.

[CGL15] Raphael Clifford, A. Grønlund, and K. G. Larsen. New Unconditional Hardness Results for Dynamic and Online Problems. In *2015 IEEE 56th Annual Symposium on Foundations of Computer Science*, pages 1089–1107, October 2015.

[CT06] Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory (Wiley Series in Telecommunications and Signal Processing)*. Wiley-Interscience, New York, NY, USA, 2006.

[DGW19] Zeev Dvir, Alexander Golovnev, and Omri Weinstein. Static data structure lower bounds imply rigidity. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2019, pages 967–978, Phoenix, AZ, USA, June 2019. Association for Computing Machinery.

[DORS08] Yevgeniy Dodis, Rafail Ostrovsky, Leonid Reyzin, and Adam Smith. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. *SIAM Journal on Computing*, 38(1):97–139, January 2008.

[Dru12] Andrew Drucker. Limitations of Lower-Bound Methods for the Wire Complexity of Boolean Operators. In *2012 IEEE 27th Conference on Computational Complexity*, pages 170–180, June 2012.

[FS89] Michael L. Fredman and Michael E. Saks. The Cell Probe Complexity of Dynamic Data Structures. In *Proceedings of the 21st Annual ACM Symposium on Theory of Computing*, pages 345–354, 1989.

[JS10] S. Jukna and G. Schnitger. Circuits with arbitrary gates for random operators, 2010. Version Number: 1.

[Juk12] Stasys Jukna. *Boolean function complexity: advances and frontiers*, volume 27. Springer Science & Business Media, 2012.

[Juk13] Stasys Jukna. Complexity of Linear Boolean Operators. *Foundations and Trends® in Theoretical Computer Science*, 9(1):1–123, 2013.

[Ko25a] Young Kun Ko. Lower Bounds for Linear Operators, 2025. Version Number: 1.

[Ko25b] Young Kun Ko. Unifying the Landscape of Super-Logarithmic Dynamic Cell-Probe Lower Bounds, 2025. Version Number: 1.

[KPI25] Oliver Korten, Toniann Pitassi, and Russell Impagliazzo. Stronger Cell Probe Lower Bounds via Local PRGs, March 2025. ISSN: 1433-8092.

[KS92] Bala Kalyanasundaram and Georg Schnitger. The Probabilistic Communication Complexity of Set Intersection. *SIAM Journal on Discrete Mathematics*, 5(4):545–557, November 1992.

[KW20] Young Kun Ko and Omri Weinstein. An Adaptive Step Toward the Multiphase Conjecture. In *2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*, pages 752–761, Durham, NC, USA, November 2020. IEEE.

[Lar12] Kasper Green Larsen. The Cell Probe Complexity of Dynamic Range Counting. In *Proceedings of the Forty-fourth Annual ACM Symposium on Theory of Computing*, STOC '12, pages 85–94, New York, NY, USA, 2012. ACM.

[LWY20] Kasper Green Larsen, Omri Weinstein, and Huacheng Yu. Crossing the Logarithmic Barrier for Dynamic Boolean Data Structure Lower Bounds. *SIAM Journal on Computing*, 49(5):STOC18–323–STOC18–367, January 2020.

[LY25] Kasper Green Larsen and Huacheng Yu. Super-Logarithmic Lower Bounds for Dynamic Graph Problems. *SIAM Journal on Computing*, pages FOCS23–42–FOCS23–69, February 2025.

[MNSW98] Peter Bro Miltersen, Noam Nisan, Shmuel Safra, and Avi Wigderson. On Data Structures and Asymmetric Communication Complexity. *J. Comput. Syst. Sci.*, 57(1):37–49, 1998.

[Pat07] Mihai Patrascu. Lower Bounds for 2-dimensional Range Counting. In *Proceedings of the Thirty-ninth Annual ACM Symposium on Theory of Computing*, STOC '07, pages 40–46, New York, NY, USA, 2007. ACM.

[Pat10] Mihai Patrascu. Towards polynomial lower bounds for dynamic problems. In Leonard J. Schulman, editor, *Proceedings of the 42nd ACM Symposium on Theory of Computing, STOC 2010, Cambridge, Massachusetts, USA, 5-8 June 2010*, pages 603–610. ACM, 2010.

[PD06] Mihai Patrascu and Erik D. Demaine. Logarithmic Lower Bounds in the Cell-Probe Model. *SIAM J. Comput.*, 35(4):932–963, April 2006.

[PTW08] Rina Panigrahy, Kunal Talwar, and Udi Wieder. A Geometric Approach to Lower Bounds for Approximate Near-Neighbor Search and Partial Match. In *2008 49th Annual IEEE Symposium on Foundations of Computer Science*, pages 414–423, Philadelphia, PA, USA, October 2008. IEEE.

[PTW10] Rina Panigrahy, Kunal Talwar, and Udi Wieder. Lower Bounds on Near Neighbor Search via Metric Expansion. In *FOCS 2010*, pages 805–814, 2010.

[Pă11] Mihai Pătraşcu. Unifying the Landscape of Cell-Probe Lower Bounds. *SIAM J. Comput.*, 40(3):827–847, 2011.

[Raz92] A.A. Razborov. On the distributional complexity of disjointness. *Theoretical Computer Science*, 106(2):385–390, December 1992.

[Sie04] Alan Siegel. On Universal Classes of Extremely Random Constant-Time Hash Functions. *SIAM J. Comput.*, 33(3):505–543, 2004.

[Sko19] Maciej Skorski. Strong Chain Rules for Min-Entropy under Few Bits Spoiled. In *2019 IEEE International Symposium on Information Theory (ISIT)*, pages 1122–1126, Paris, France, July 2019. IEEE.

[Tho13] Mikkel Thorup. Mihai PăTraşCu: Obituary and Open Problems. *SIGACT News*, 44(1):110–114, March 2013.

[Wai19] Martin J. Wainwright. *High-Dimensional Statistics: A Non-Asymptotic Viewpoint*. Cambridge University Press, 1 edition, February 2019.

[Wil17] Virginia Vassilevska Williams. On some fine-grained questions in algorithms and complexity. In *ICM 2018*, 2017.

[Yao81] Andrew Chi-Chih Yao. Should Tables Be Sorted? *J. ACM*, 28(3):615–628, July 1981.

A Omitted Proof of Claims and Lemmas

To make the presentation self-contained, we attach the missing proofs of claims and lemmas.

Claim 2.16. *Let $\mathcal{D}$ be a distribution and $\mathcal{U}$ a uniform distribution over some $\mathcal{S} \subset \{0,1\}^n$. Then if $D(\mathcal{D}||\mathcal{U}) < t$ with $t > 1$, then for every $\alpha > 2$ there exists an event E such that*

$$\mathcal{D}(E) \geq 1 - \frac{1}{\alpha}$$
$$H_\infty(\mathcal{D}|_E) \geq \log|\mathcal{S}| - 2\alpha t$$

Proof. We partition X depending on $\mathcal{D}(X)$. Let E denote the set of X such that

$$\log\frac{\mathcal{D}(X)}{\mathcal{U}(X)} < \alpha t$$

Since $D(\mathcal{D}||\mathcal{U}) < t$, by Markov's inequality $1 - \mathcal{D}(E) < 1/\alpha$. With $\alpha > 2$, for any X that is in the support of $\mathcal{D}|_E$, we have

$$\mathcal{D}|_E(X) = \frac{\mathcal{D}(X)}{\mathcal{D}(E)} \leq 2 \cdot \mathcal{D}(X) \leq 2^{\alpha t+1} \cdot \mathcal{U}(X) = 2^{-\log|\mathcal{S}|+\alpha t+1} \leq 2^{-\log|\mathcal{S}|+2\alpha t}$$

which then gives $H_\infty(\mathcal{D}|_E) \geq \log|\mathcal{S}| - 2\alpha t$. □

Towards the proof of Lemma 3.10, we need the following well-known fact about the Hadamard matrix.

Claim A.1 (Lindsey's Lemma)**.** *Let H be a Hadamard matrix. Let μ and ν be distributions, written as vectors. Then*

$$\mu^T H \nu \leq \|\mu\|_2 \|\nu\|_2 \cdot 2^{n/2}$$

Also Fact 2.12 implies the following simple proposition about ℓ_2^2 norm of the distribution versus its min-entropy.

Proposition A.2.

$$\mathbb{E}_{b\sim B}\left[\sum_a \Pr[A = a|B = b]^2\right] \leq 2^{-\tilde{H}_\infty(A|B)}$$

Proof.

$$\sum_a \Pr[A = a|B = b]^2 = 2^{-H_2(A|B=b)} \leq 2^{-H_\infty(A|B=b)}$$

Therefore,

$$\mathbb{E}_{b\sim B}\left[\sum_a \Pr[A = a|B = b]^2\right] \leq \mathbb{E}_{b\sim B}\left[2^{-H_\infty(A|B=b)}\right] = 2^{-\tilde{H}_\infty(A|B)}$$

where the last equality holds from the definition of average min-entropy. □

Now we are ready to prove Lemma 3.10. We prove an equivalent statement.

Lemma 3.10. *No setting of a random variable $Z = z$ and A, which contains z_{out} can simultaneously satisfy all three of the following inequalities for any $\gamma \geq 3$*

$$\mathbb{E}_{A|Z=z}\left[\left|\mathbb{E}_{Y,X|_{A=a,Z=z}}\left[\chi_Y(X) \cdot z_{out}|A = a, Z = z\right]\right|\right] \geq 2^{-\gamma+2} \tag{17}$$
$$\tilde{H}_\infty(Y|A, Z = z) + \tilde{H}_\infty(X|A, Z = z) \geq n + 2\gamma \tag{18}$$
$$I(Y; X|A, Z = z) \leq 2^{-2\gamma} \tag{19}$$

Proof. For the sake of contradiction, suppose such z and A exists. First as z_{out} is ± 1, the absolute value of the guess does not change. That is

$$\left|\mathbb{E}_{Y,X|_{A=a,Z=z}}\left[\chi_Y(X)\cdot z_{out}|A=a,Z=z\right]\right| = \left|\mathbb{E}_{Y,X|_{A=a,Z=z}}\left[\chi_Y(X)|A=a,Z=z\right]\right| \tag{20}$$

Then we can use the ℓ_1 bound to have

$$\left|\mathbb{E}_{Y,X|_{A=a,Z=z}}\left[\chi_Y(X)|A=a,Z=z\right]\right| \le |Y|_{A=a,Z=z}\cdot H\cdot X|_{A=a,Z=z}| \tag{21}$$

$$+\|Y|_{A=a,Z=z}\times X|_{A=a,Z=z} - (Y,X)|_{A=a,Z=z}\|_1 \tag{22}$$

We bound the expectation of (22). Our KL-divergence term is then equal to the mutual information between Y and X conditioned on $Z=z$. Namely, using the chain rule for the KL divergence,

$$\begin{aligned}
&D((Y,X)|_{A=a,Z=z}||Y|_{A=a,Z=z}\times X|_{A=a,Z=z})\\
&= \underbrace{D(X|_{A=a,Z=z}||X|_{A=a,Z=z})}_{=0} + \mathbb{E}_{x\sim X|_{A=a,Z=z}}\left[D(Y|_{X=x,A=a,Z=z}||Y|_{A=a,Z=z})\right]\\
&= I(Y;X|A=a,Z=z)
\end{aligned}$$

Then, due to Pinsker's inequality (Fact 2.6), we have

$$\|Y|_{A=a,Z=z}\times X|_{A=a,Z=z} - (Y,X)|_{A=a,Z=z}\|_1 \le 2\sqrt{I(Y;X|A=a,Z=z)}$$

Taking expectation over A and applying Jensen's inequality,

$$\mathbb{E}_{A|_{Z=z}}\left[\|Y|_{A=a,Z=z}\times X|_{A=a,Z=z} - (Y,X)|_{A=a,Z=z}\|_1\right] \le 2\sqrt{I(Y;X|A,Z=z)} \le 2^{-\gamma+1} \tag{23}$$

where the last bound holds from (19).

Next, we bound (21). Due to Claim A.1 and Cauchy-Schwarz Inequality,

$$\begin{aligned}
&\mathbb{E}_{A|_{Z=z}}\left[|Y|_{A=a,Z=z}\cdot H\cdot X|_{A=a,Z=z}|\right] \le \mathbb{E}_{A|_{Z=z}}\left[2^{n/2}\cdot\|Y|_{A=a,Z=z}\|_2\cdot\|X|_{A=a,Z=z}\|_2\right]\\
&\le 2^{n/2}\cdot\sqrt{\mathbb{E}_{A|_{Z=z}}\left[\|Y|_{A=a,Z=z}\|_2^2\right]\cdot\mathbb{E}_{A|_{Z=z}}\left[\|X|_{A=a,Z=z}\|_2^2\right]}
\end{aligned}$$

Proposition A.2 implies

$$\begin{aligned}
\mathbb{E}_{A|_{Z=z}}\left[\|Y|_{A=a,Z=z}\|_2^2\right] &\le 2^{-\tilde{H}_\infty(Y|A,Z=z)}\\
\mathbb{E}_{A|_{Z=z}}\left[\|X|_{A=a,Z=z}\|_2^2\right] &\le 2^{-\tilde{H}_\infty(X|A,Z=z)}
\end{aligned}$$

which would in turn imply

$$\begin{aligned}
&\sqrt{\mathbb{E}_{A|_{Z=z}}\left[\|Y|_{A=a,Z=z}\|_2^2\right]\cdot\mathbb{E}_{A|_{Z=z}}\left[\|X|_{A=a,Z=z}\|_2^2\right]} \le 2^{-(\tilde{H}_\infty(Y|A,Z=z)+\tilde{H}_\infty(X|A,Z=z))/2}\\
&\le 2^{-\frac{n+2\gamma}{2}} = 2^{-n/2}\cdot 2^{-\gamma}
\end{aligned}$$

which then implies (21) is upper bounded by

$$(21) \le 2^{n/2}\cdot 2^{-n/2}\cdot 2^{-\gamma} = 2^{-\gamma} \tag{24}$$

Therefore, we get

$$\mathbb{E}_{A|Z=z}\left[\left|\mathbb{E}_{Y,X|_{A=a,Z=z}}\left[\chi_Y(X)\cdot z_{out}|A=a,Z=z\right]\right|\right] \le \frac{3}{2^\gamma} \tag{25}$$

which contradicts (17). □

B Lifting Theorem

We consider the following "hard" functions, which are roughly f with a small discrepancy under a product distribution.

Definition B.1 (Hard Functions)**.** *Let X be a uniform distribution over $\{0,1\}^n$, and let S be an independently distributed random variable with min-entropy $H_\infty(S)$. We say $f : \{0,1\}^{2n} \to \{\pm 1\}$ is hard if for any random variables A such that*

$$\begin{aligned}
&(S,X)|_A = X|_A \times S|_A \\
&\widetilde{H}_\infty(X|A) \geq \frac{\sqrt{n}}{3} \\
&\widetilde{H}_\infty(S|A) \geq H_\infty(S) - o(\log^3(n))
\end{aligned}$$

it must be the case that

$$\mathbb{E}_A \left[\left| \mathbb{E}_{(S,X)|_A} \left[f(S,X) \right] \right| \right] \leq n^{-\Omega(1)}$$

Intuitively, "hard" functions are those that exhibit small discrepancy under some product distribution with X set to be a uniform distribution. For instance, Inner Product over $\mathbb{F}_2$ satisfies the definition, as its discrepancy is exponentially small. Unfortunately, Disjointness does not satisfy the definition. One can obtain good advantage by sampling and revealing a few coordinates. (See [BM13])

For example, suppose Alice has S and Bob has X. Bob does the following. Consider the coordinates where X equals 1. Sample each coordinate with probability ε. Then send these coordinates X_0 to Alice. The message length is roughly $O(\varepsilon n \log n)$. Alice simply checks Disjointness with the sampled coordinates X_0. If S and X_0 are not disjoint, declare the inputs are not disjoint. Otherwise flip a random coin to output 1 with probability $\Pr_{(S,X)} [\mathsf{DISJ}(S,X) = 1]$. One can verify that such a strategy ensures roughly $\Omega(\varepsilon)$ advantage over random guessing. That is a $\widetilde{O}(n^{1-\delta})$ length message already gives $\Omega(n^\delta)$ advantage over random guessing.

One key ingredient necessary for our general proof is the following technical theorem regarding the min-entropy.

Theorem B.2 (Theorem 1 and Corollary 1 of [Sko19])**.** *Let $\mathcal{X}$ be a fixed alphabet, and $X = (X_1, \ldots, X_t)$ be a sequence of (possibly correlated) random variables each over $\mathcal{X}$, equipped with a distribution μ. Then for any $\varepsilon \in (0,1)$ and $\delta > 0$, there exists a collection $\mathcal{B}$ of disjoint sets on $\mathcal{X}^t$ such that*

- *$\mathcal{B}$ can be indexed by a small number of bits, namely*

$$\log |\mathcal{B}| = t \cdot O\left(\log\log|\mathcal{X}| + \log\log \varepsilon^{-1} + \log(t/\delta) \right)$$

- *$\mathcal{B}$ almost covers the domain*

$$\sum_{B \in \mathcal{B}} \mu(B) \geq 1 - \varepsilon$$

- *Conditioned on $\mathcal{B}$, block distributions $X_i | X_{<i}$ are nearly flat. That is*

$$\forall x, x' \in B, \quad 2^{-O(\delta)} \leq \frac{\mu(x_i|x_{<i})}{\mu(x'_i|x'_{<i})} \leq 2^{O(\delta)}$$

- *For every $B \in \mathcal{B}$, for every index $i \in [t]$, and for every set $I \subset [i-1]$, we have*

1. *The chain rule for min-entropy*

$$H_\infty(X_i|X_I, B) + H_\infty(X_I|B) = H_\infty(X_i, X_I|B) \pm O(\delta)$$

2. *The average and worst-case min-entropy almost match*

$$\widetilde{H}_\infty(X_i|X_I, B) = H_\infty(X_i|X_I, B) \pm O(\delta)$$

Remark B.3. *The proof of the theorem invokes the standard ℓ_∞ covering-number bound for the probability simplex. Skórski [Sko19] cites an unpublished note for this bound; for an accessible reference see Chapter 5, Example 5.6 of [Wai19].*

While the standard chain rule does not hold for min-entropy, Theorem B.2 essentially allows us to maintain a chain rule structure by "paying" for partitions and discarding a small set of inputs. Then we are ready to prove the following general lifting theorem, which is a strengthening of Theorem 1.1 using Theorem B.2.

Theorem B.4 (Lifting Theorem)**.** *For the Multiphase Problem with f satisfying Definition B.1, and $m = n^{1+\Omega(1)}$,*

$$\max\{t_u, t_{tot}\} \geq \Omega\left(\left(\frac{\log n}{\log\log n}\right)^2\right)$$

Proof. Our simulation theorem Section 3.1 guarantees a 2.5-round Multiphase communication protocol Π with exactly the same parameters as in Corollary 3.4. But on top of the usual simulation, we will also consider an independent random permutation $\sigma \in \mathrm{Sym}([m])$ known to all players, to "average out" the advantage per coordinate. When conditioned on σ, σ permutes the query indices so that $f_\sigma(S_q, X) := f(S_{\sigma(q)}, X)$. By the same choice of parameters, we get

$$|U| \leq O(n\log^{\kappa+1}(n)),\ |\Phi(U)| \leq n - \frac{\sqrt{n}}{2},\ |A_q| \leq o(\log^3(n))$$

while having

$$\mathsf{adv}(G_{f_\sigma}, \Pi) = \mathsf{adv}(G_f, \Pi) \geq n^{-o(1)}.$$

This holds as the whole protocol for f_σ is constructed via the following argument. Construct the same protocol up to the 0.5-round message for $\vec{S} = (S_1, \ldots, S_m)$. Given query $q \in \mathcal{Q}$, Alice simply sends $A_{\sigma(q)}$, and Bob outputs accordingly.

A useful property here is that

$$\begin{aligned}
&\mathbb{E}_{A_q, \Phi(U), B_q|\sigma, \vec{S}}\left[\mathbb{E}\left[B_q \cdot f_\sigma(S_q, X)|A_q, \Phi(U), B_q, \sigma, \vec{S}\right]\right] \\
&= \mathbb{E}_{A_{\sigma(q)}, \Phi(U), B_{\sigma(q)}|id, \vec{S}}\left[\mathbb{E}\left[B_{\sigma(q)} \cdot f(S_{\sigma(q)}, X)|A_{\sigma(q)}, \Phi(U), B_{\sigma(q)}, \vec{S}, id\right]\right]
\end{aligned}$$

where the second case refers to choosing the permutation as the identity. By taking expectation over uniformly random σ, for any fixed $q \in \mathcal{Q} = [m]$, we get

$$\begin{aligned}
&\mathbb{E}_{A_q, \Phi(U), B_q, \sigma|\vec{S}}\left[\mathbb{E}\left[B_q \cdot f_\sigma(S_q, X)|A_q, \Phi(U), B_q, \sigma, \vec{S}\right]\right] \\
&= \mathbb{E}_{A_Q, \Phi(U), B_Q, Q|id, \vec{S}}\left[\mathbb{E}\left[B_Q \cdot f(S_Q, X)|A_Q, \Phi(U), B_Q, \vec{S}, Q, id\right]\right] \geq n^{-o(1)}
\end{aligned} \tag{26}$$

Intuitively, introducing a random permutation averages out the advantage across the coordinates q, ensuring no single coordinate disproportionately affects the overall advantage. Such a step is

technically necessary, as unlike in the proof of Theorem 1.1, we will be fixing a single q in the later part of the proof.

Again, we would like to extract a random variable Z from a 2.5-round protocol Π to derive a combinatorial contradiction. As a "hard" distribution, analogous to the proof of Theorem 1.1, we will be selecting each S_q's independently at random according to the distribution given in Definition B.1, and X, a uniformly random distribution.

Our proof is analogous to that of Lemma 3.11, essentially selecting the same Z, with the following caveat. Recall that in the proof of Lemma 3.11, we have selected Z as $A_{\mathcal{Q}_{all}}, \Phi(U), S_{<Q}, Q, B_Q$. We add an additional "partitioning" of $\vec{S}$, $\mathcal{B}$ guaranteed by Theorem B.2 with $\{X_i\}_{i\in[m]} := (S_{\sigma(1)}, \ldots, S_{\sigma(m)})$ in the notation of Theorem B.2, conditioned on $A_{\mathcal{Q}_{all}}, \Phi(U), \sigma$.

We will choose $\varepsilon := 2^{-n^{\Omega(1)}}$ and $\delta := \frac{1}{\mathrm{poly}(n)} \ll \frac{1}{m}$ for our choice of ε and δ in Theorem B.2. Then Theorem B.2 would guarantee a partitioning of $(S_{\sigma(1)}, \ldots, S_{\sigma(m)})$ such that

$$\log|\mathcal{B}| = m \cdot O(\log\log(2^n) + \log\log 2^{n^{\Omega(1)}} + \log(\mathrm{poly}(m))) = m \cdot O(\log n)$$

where conditioned on a valid partition in $\mathcal{B}$, near chain rule holds for min-entropy. But with a slight abuse of notation, we will also include $\mathcal{B}$ as the case where $\vec{S}$ is not included in any of the partitions (i.e., spoiled set B_{spoil}). Then $G_{\mathcal{B}} = 1$ refers to the event of valid "choosing" $\mathcal{B}$, i.e., choosing $B \in \mathcal{B}\backslash\{B_{spoil}\}$, to derive the contradiction. Theorem B.2 implies the near chain rule property:

$$\sum_{q=1}^{m}\left[\widetilde{H}_\infty(S_{\sigma(q)}|S_{\sigma(<q)}, A_{\mathcal{Q}_{all}}, \mathcal{B}, \Phi(U), \sigma, G_{\mathcal{B}}=1)\right] = \widetilde{H}_\infty(\vec{S}|A_{\mathcal{Q}_{all}}, \mathcal{B}, \Phi(U), \sigma, G_{\mathcal{B}}=1) \pm m\cdot O(\delta) \tag{27}$$

Then our new Z would be

$$Z := A_{\mathcal{Q}_{all}}, \Phi(U), \mathcal{B}, S_{\sigma(<Q)}, Q, B_Q, \sigma, G_{\mathcal{B}} = 1$$

where $S_{\sigma(<Q)} := S_{\sigma(1)}, \ldots, S_{\sigma(Q-1)}$.

We first bound $\widetilde{H}_\infty(S_{\sigma(Q)}|Z)$ for a random Q, or equivalently, $\widetilde{H}_\infty(S_{\sigma(Q)}) - \widetilde{H}_\infty(S_{\sigma(Q)}|Z)$. From Theorem B.2 and Lemma 2.14, we have

$$\widetilde{H}_\infty(\vec{S}|A_{\mathcal{Q}_{all}}, \mathcal{B}, \Phi(U), \sigma) \geq \widetilde{H}_\infty(\vec{S}|\sigma) - m|A_q| - O(m\log n) - |\Phi(U)| \geq m\cdot H_\infty(S_Q) - 1.5m|A_q| \tag{28}$$

as $|\mathcal{B}| \leq O(m\log n)$ and $|\Phi(U)| \leq n \ll m$. So the term is dominated by $m|A_q|$. As $S_1, \ldots, S_m$ are chosen independently at random, $S_{\sigma(1)}, \ldots, S_{\sigma(m)}$ are chosen independently at random as well, resulting in the final inequality. Then further conditioning on $G_{\mathcal{B}} = 1$, and using the observation, we can still deduce

$$\begin{aligned}\widetilde{H}_\infty(\vec{S}|A_{\mathcal{Q}_{all}}, \mathcal{B}, \Phi(U), \sigma, G_{\mathcal{B}}=1) &\geq \log(\Pr[G_{\mathcal{B}}=1]) + \widetilde{H}_\infty(\vec{S}|A_{\mathcal{Q}_{all}}, \mathcal{B}, \Phi(U), \sigma, G_{\mathcal{B}}) \\ &\geq -O(\varepsilon) + \widetilde{H}_\infty(\vec{S}|A_{\mathcal{Q}_{all}}, \mathcal{B}, \Phi(U), \sigma) \\ &\geq m\cdot H_\infty(S_Q) - 1.5m|A_q| - O(\varepsilon) \geq m\cdot H_\infty(S_Q) - 1.75m|A_q|\end{aligned}$$

as $\Pr[G_{\mathcal{B}}=0] \leq \varepsilon$, which is guaranteed to be exponentially small due to our choice of parameters. The second inequality holds as $\mathcal{B}$ determines $G_{\mathcal{B}}$. The subtraction terms are indeed dominated by $m|A_q|$ terms. Then applying (27), we obtain that for a random q,

$$\begin{aligned}&H_\infty(S_{\sigma(q)}) - \mathbb{E}_{q\in[m]}\left[\widetilde{H}_\infty(S_{\sigma(q)}|S_{\sigma(<q)}, A_{\mathcal{Q}_{all}}, \mathcal{B}, \Phi(U), \sigma, G_{\mathcal{B}}=1)\right] \\ &\leq H_\infty(S_{\sigma(q)}) - \frac{m\cdot H_\infty(S_{\sigma(q)}) - 1.75m|A_q| + O(m\cdot\delta)}{m} \leq 2|A_q|.\end{aligned} \tag{29}$$

Next we bound the average min-entropy of X. Due to the same argument as in Lemma 3.8,

$$\begin{aligned}\widetilde{H}_\infty(X|\vec{S}, A_{\mathcal{Q}_{all}}, \mathcal{B}, \Phi(U), \sigma, G_{\mathcal{B}} = 1) &\geq \log\left(\Pr[G_{\mathcal{B}} = 1]\right) + \widetilde{H}_\infty(X|\vec{S}, A_{\mathcal{Q}_{all}}, \mathcal{B}, \Phi(U), \sigma, G_{\mathcal{B}}) \\ &\geq -O(\varepsilon) + \widetilde{H}_\infty(X|\vec{S}, A_{\mathcal{Q}_{all}}, \Phi(U), \sigma) \\ &\geq n - |\Phi(U)| - O(\varepsilon)\end{aligned}$$

where the second inequality holds as $\vec{S}, A_{\mathcal{Q}_{all}}, \Phi(U), \sigma$ fully determines the partition $\mathcal{B}$ and $G_{\mathcal{B}}$, again a property guaranteed by Theorem B.2, as $\mathcal{B}$ forms a partition over $\vec{S}$ while conditioned on $\Phi(U), A_{\mathcal{Q}_{all}}, \sigma$. The third inequality holds due to the same argument from Lemma 3.8. In particular,

$$\widetilde{H}_\infty(X|\vec{S}, A_{\mathcal{Q}_{all}}, \Phi(U), \sigma) = \widetilde{H}_\infty(X|\vec{S}, \Phi(U), \sigma) \geq \widetilde{H}_\infty(X|\vec{S}, \sigma) - |\Phi(U)| = n - |\Phi(U)|\,.$$

Then for any fixed q, Claim 2.15 implies

$$\widetilde{H}_\infty(X|S_{\sigma(<q)}, A_{\mathcal{Q}_{all}}, \mathcal{B}, \Phi(U), \sigma, G_{\mathcal{B}} = 1) \geq \widetilde{H}_\infty(X|\vec{S}, A_{\mathcal{Q}_{all}}, \mathcal{B}, \Phi(U), \sigma, G_{\mathcal{B}} = 1) \geq n - |\Phi(U)| - O(\varepsilon)$$

therefore

$$\widetilde{H}_\infty(X|S_{\sigma(<q)}, A_{\mathcal{Q}_{all}}, \mathcal{B}, \Phi(U), \sigma, G_{\mathcal{B}} = 1, B_q) \geq n - |\Phi(U)| - 1 - O(\varepsilon) \geq n - |\Phi(U)| - 2 \tag{30}$$

where the last extra -1 term follows from Lemma 2.14 applied upon $\widetilde{H}_\infty(X|S_{\sigma(<q)}, A_{\mathcal{Q}_{all}}, \mathcal{B}, \Phi(U), \sigma, G_{\mathcal{B}} = 1)$ term.

Finally, we are left with bounding the correlation term. The steps are analogous to the proof of Lemma 3.9.

$$\begin{aligned}&I(S_{\sigma(Q)}; X|Q, S_{\sigma(<Q)}, A_{\mathcal{Q}_{all}}, \mathcal{B}, \Phi(U), \sigma, G_{\mathcal{B}} = 1, B_Q) \\ &\leq I(S_{\sigma(Q)}; UX|Q, S_{\sigma(<Q)}, A_{\mathcal{Q}_{all}}, \mathcal{B}, \Phi(U), \sigma, G_{\mathcal{B}} = 1, B_Q) \\ &\leq I(S_{\sigma(Q)}; UX|Q, S_{\sigma(<Q)}, A_{\mathcal{Q}_{all}}, \mathcal{B}, \Phi(U), \sigma, G_{\mathcal{B}} = 1) = \frac{1}{m} I(\vec{S}; UX|A_{\mathcal{Q}_{all}}, \mathcal{B}, \Phi(U), \sigma, G_{\mathcal{B}} = 1) \\ &\leq \frac{1}{m \cdot \Pr[G_{\mathcal{B}} = 1]} I(\vec{S}; UX|A_{\mathcal{Q}_{all}}, \mathcal{B}, \Phi(U), \sigma, G_{\mathcal{B}}) \leq \frac{2 \cdot I(\vec{S}; UX|A_{\mathcal{Q}_{all}}, \Phi(U), \sigma)}{m} \\ &\leq \frac{2I(\vec{S}; UX|\Phi(U), \sigma)}{m} \leq \frac{2 \cdot I(\vec{S}; UX|\sigma)}{m} = \frac{2 \cdot \Big(I(\vec{S}; X|\sigma) + I(\vec{S}; U|X, \sigma)\Big)}{m} \leq \frac{2|U|}{m}.\end{aligned} \tag{31}$$

The only difference from the proof of Lemma 3.9 is the introduction of $G_{\mathcal{B}}, \mathcal{B}$ and σ. Fact 2.9 allows us to remove any additional random variables. That is

$$I(\vec{S}; UX|A_{\mathcal{Q}_{all}}, \mathcal{B}, \Phi(U), \sigma, G_{\mathcal{B}}) \leq I(\vec{S}; UX|A_{\mathcal{Q}_{all}}, \sigma, \Phi(U))$$

as $I(\mathcal{B}, G_{\mathcal{B}}; UX|A_{\mathcal{Q}_{all}}, \Phi(U), \sigma, \vec{S}) = 0$ with $A_{\mathcal{Q}_{all}}, \Phi(U), \sigma$ inducing a partition on $\vec{S}$. Also

$$I(\vec{S}; UX|A_{\mathcal{Q}_{all}}, \Phi(U), \sigma) \leq I(\vec{S}; UX|\Phi(U), \sigma)$$

as $I(A_{\mathcal{Q}_{all}}; UX|\Phi(U), \sigma, \vec{S}) = 0$.

Then due to Markov's argument, there must exist $q \in [m]$ such that

$$\widetilde{H}_\infty(S_{\sigma(q)}|A_{\mathcal{Q}_{all}}, \Phi(U), \mathcal{B}, S_{\sigma(<q)}, B_q, \sigma, G_{\mathcal{B}} = 1) \geq H_\infty(S_Q) - o(\log^3(n)) \tag{32}$$

$$\widetilde{H}_\infty(X|A_{\mathcal{Q}_{all}}, \Phi(U), \mathcal{B}, S_{\sigma(<q)}, B_q, \sigma, G_{\mathcal{B}} = 1) \geq n - |\Phi(U)| - 2 \tag{33}$$

$$I(S_{\sigma(q)}; X|A_{\mathcal{Q}_{all}}, \Phi(U), \mathcal{B}, S_{\sigma(<q)}, B_q, \sigma, G_{\mathcal{B}} = 1) \leq \frac{10|U|}{m}. \tag{34}$$

while we have established in (26) that for any $q \in [m]$ and any $\vec{S}$

$$\mathbb{E}_{A_q,\Phi(U),B_q,\sigma|\vec{S}}\left[\mathbb{E}\left[B_q \cdot f(S_{\sigma(q)},X)|A_q,\Phi(U),B_q,\sigma,\vec{S}\right]\right] \geq n^{-o(1)}$$

This is why we need to introduce a random permutation to average out the advantage. Without the averaging argument, we cannot guarantee that the advantage is high for every $q \in [m]$.

Then via an analogous argument from Claim 3.5

$$\begin{aligned} n^{-o(1)} \leq & \mathbb{E}_{A_q,\Phi(U),S_{\sigma(<q)},B_q,\sigma}\left[\mathbb{E}\left[B_q \cdot f(S_{\sigma(q)},X)|A_q,\Phi(U),S_{\sigma(<q)},B_q,\sigma\right]\right] \\ & \leq \mathbb{E}_{A_q,\Phi(U),S_{\sigma(<q)},B_q,\sigma}\left[\left|\mathbb{E}\left[f(S_{\sigma(q)},X)|A_q,\Phi(U),S_{\sigma(<q)},B_q,\sigma\right]\right|\right] \\ & \leq \mathbb{E}_{A_{\mathcal{Q}_{all}},\mathcal{B},\Phi(U),S_{\sigma(<q)},B_q,\sigma}\left[\left|\mathbb{E}\left[f(S_{\sigma(q)},X)|A_{\mathcal{Q}_{all}},\mathcal{B},\Phi(U),S_{\sigma(<q)},B_q,\sigma\right]\right|\right] \end{aligned} \tag{35}$$

For shorthand, we will denote

$$Z_q := A_{\mathcal{Q}_{all}},\mathcal{B},\Phi(U),S_{\sigma(<q)},B_q,\sigma,G_{\mathcal{B}}=1$$

Again as $\Pr[G_{\mathcal{B}}=0] \leq \varepsilon$, the exact same argument to that of the proof of Lemma 3.11 applied upon (35) gives

$$\mathbb{E}_{Z_q}\left[\left|\mathbb{E}\left[f(S_{\sigma(q)},X)|Z_q\right]\right|\right] \geq n^{-o(1)} - O(\varepsilon) \geq n^{-o(1)}$$

due to our choice of ε, $\varepsilon := 2^{-n^{\Omega(1)}}$.

Now we want to deduce a contradiction. (32) and (33) satisfy the average min-entropy condition. But $(S_{\sigma(q)},X)|_{Z_q}$ is not a product distribution. Nevertheless, (34) guarantees that they are "close" to a product distribution as

$$\mathbb{E}_{Z_q}\left[D((S_{\sigma(q)},X)|_{Z_q}||S_{\sigma(q)}|_{Z_q} \times X|_{Z_q})\right] = I(S_{\sigma(q)};X|Z_q) \leq \frac{10|U|}{m}$$

A standard application of Pinsker's inequality (Fact 2.6) and Jensen's inequality, gives

$$\mathbb{E}_{Z_q}\left[\|S_{\sigma(q)}|_{Z_q} \times X|_{Z_q} - (S_{\sigma(q)},X)|_{Z_q}\|_1\right] \leq 2\sqrt{I(S_{\sigma(q)};X|Z_q)} \leq \sqrt{\frac{40|U|}{m}}.$$

Now if we consider $R_{Z_q} := S_{\sigma(q)}|_{Z_q} \times X|_{Z_q}$, which is forced to be a product distribution,

$$\mathbb{E}_{Z_q}\left[\left|\mathbb{E}_{(S_{\sigma(q)},X)\sim R_{Z_q}}\left[f(S_{\sigma(q)},X)\right]\right|\right] \geq \mathbb{E}_{Z_q}\left[\left|\mathbb{E}_{(S_{\sigma(q)},X)|_{Z_q}}\left[f(S_{\sigma(q)},X)\right]\right|\right] - \sqrt{\frac{40|U|}{m}} \geq n^{-o(1)}$$

But from our definition of hard (Definition B.1) and bounds on average min-entropy ((32),(33)), it must be the case that

$$\mathbb{E}_{Z_q}\left[\left|\mathbb{E}_{(S_{\sigma(q)},X)\sim R_{Z_q}}\left[f(S_{\sigma(q)},X)\right]\right|\right] \leq n^{-\Omega(1)}$$

which is a contradiction. □

ECCC ISSN 1433-8092
https://eccc.weizmann.ac.il