Randomized and Quantum Lifting for One-Way Conservative NOF Model

Haoyu Wang
The Pennsylvania State University, State College, PA, USA

Pei Wu
The Pennsylvania State University, State College, PA, USA

Abstract

We consider lifting theorems that transfer lower bounds for two-party communication problems to multiparty communication problems. In particular, following the deterministic Number-on-Forehead (NOF) lifting framework of Yang and Zhang, we study randomized and quantum one-way NOF lifting for composed problems $F(z, \mathbf{x}) = f(z, G(\mathbf{x}))$.

We work in a one-way NOF model in which only the last player's view is restricted. The other players have their usual NOF views and communicate as usual, but the last player sees only the gadget output $G(\mathbf{x})$, not the gadget input $\mathbf{x}$. This kind of restricted-view has appeared in the NOF literature under the name conservative model. Our main contribution is a pair of lifting theorems for this model. In the randomized setting, we show that lifting follows when each preimage $G^{-1}(v)$, the set of gadget inputs with output v, looks pseudorandom to large cylinder intersections. In the quantum setting, we prove an analogous theorem. Equivalently, conservative protocols for $F(z, \mathbf{x}) = f(z, G(\mathbf{x}))$ can be converted into two-party one-way protocols for $f(z, v)$ with comparable cost, and the error loss controlled by the corresponding pseudorandomness parameters. Thus, this restriction isolates a setting in which both randomized and quantum one-way NOF lifting can be proved by a direct simulation argument.

We prove the required pseudorandomness properties for the generalized inner product gadget over finite fields, using the multiparty character-sum bounds of Yang and Zhang, and for random gadgets, which give non-explicit lifting. As applications, Boolean Hidden Matching yields a randomized-versus-quantum separation in the conservative NOF model, and lifting INDEX gives randomized and quantum conservative NOF lower bounds for $O(\log n)$ players.

2012 ACM Subject Classification Theory of computation → Communication complexity

Keywords and phrases communication complexity, lifting theorem, number-on-forehead model

Digital Object Identifier 10.4230/LIPIcs.MFCS.2026.78

Related Version *Full Version*: `https://pwu.netlify.app/files/nof-lifting.pdf`

Acknowledgements We thank Guangxu Yang for bringing this conservative lifting problem to our attention. We are also grateful for many insightful discussions with him and for his helpful suggestions on the final version.

1 Introduction

Lifting theorems are a central technique of converting lower bounds in simpler or more structured models into explicit communication lower bounds. In two-party communication this perspective is now robust, beginning with Raz–McKenzie [18] and continuing through randomized lifting theorems such as Göös–Pitassi–Watson [11], $\mathbf{P}^{\mathbf{NP}}$ lifting [9], and variants based on low-discrepancy gadgets, rectangle/junta structure, approximate degree, and sunflower decompositions [19, 10, 5, 15]. For the more powerful number-on-forehead (NOF) model, comparable lifting results are still largely missing. This gap is especially striking in the one-way setting, where Yang and Zhang recently proved deterministic lifting theorems using the generalized inner product gadget [21]. We study the next natural cases: randomized and quantum one-way lifting.

This frontier matters because one-way NOF lower bounds sit close to major circuit lower-bound questions. Classical connections show that sufficiently strong NOF lower bounds in the superlogarithmic-player regime would imply consequences such as ACC^0 lower bounds [12, 17], while strong one-way lower bounds for problems such as pointer jumping are tied to Boolean size-depth tradeoffs [4, 20]. The NOF model has long served as a benchmark for lower-bound techniques [1, 14], and one-way lower bounds have also influenced pseudorandomness, cryptography, and streaming [7, 3, 13]. At the same time, direct lower-bound methods in one-way NOF remain limited. Thus a strong explicit lifting theorem in this regime would not bypass the explicit-hard-function barrier; it would meet that barrier head-on by producing exactly the kind of explicit hard NOF problems that current methods struggle to prove directly. This is what makes one-way NOF lifting both important and delicate.

Given an outer one-way problem $f(z, v)$ and a gadget $G : X_1 \times \cdots \times X_k \to \mathcal{V}$, write $\mathbf{x} = (\mathbf{x}_1, \ldots, \mathbf{x}_k)$ and define

$$F(z, \mathbf{x}) = f\left(z, G(\mathbf{x})\right).$$

Throughout the introduction, the underlying two-party one-way problem has Alice holding z and Bob holding v. Alice sends a message to Bob and Bob calculates the $f(z, v)$. In the lifted NOF problem there are k nonterminal senders $P_1, \ldots, P_k$ and terminal Charlie: P_i sees z and $\mathbf{x}_{-i}$ (all gadget inputs except $\mathbf{x}_i$), messages are sent in the order $P_1 \to \cdots \to P_k \to$ Charlie, and in the full model Charlie sees the residual NOF view $(\mathbf{x}_1, \ldots, \mathbf{x}_k)$; communication cost means the final transcript length in the randomized model and the total message length in the quantum model.

The easy direction is immediate: any ordinary two-party one-way protocol for f gives a one-way NOF protocol for F, by having the last sender compute Alice's message from z and send it to Charlie, and having Charlie use the gadget value $v = G(\mathbf{x})$ to perform Bob's decision. A full lifting theorem would prove the converse: every efficient one-way NOF protocol for F could be converted into an efficient ordinary two-party one-way protocol for f, where Alice has z and Bob has v. The obstacle is that in the full model Charlie retains more information than the gadget value $v = G(\mathbf{x})$. This overlap of information may allow communication strategies that are not captured by a two-party simulation using only v.

A terminal-conservative model

We study a *terminal-conservative* version of one-way NOF. The players $P_1, \ldots, P_k$ keep their usual NOF visibility and still communicate in order, but the terminal player Charlie sees only the gadget output

$$v := G(\mathbf{x}_1, \ldots, \mathbf{x}_k).$$

In particular, Charlie has no residual NOF view of the gadget inputs.

Thus the model is not intended as a replacement for the full one-way NOF model. It is an intermediate benchmark that isolates the terminal obstruction, namely the difference between Charlie seeing the entire NOF view $\mathbf{x}$ and seeing only the gadget value $G(\mathbf{x})$. This is a minimal terminal restriction: only Charlie's NOF view is limited, while the prefix of the protocol remains fully NOF. Conservative viewpoints have appeared before in one-way multiparty lower bounds and their applications, for instance in work on pointer jumping, pseudorandomness, and streaming algorithms [6, 4, 20, 7, 13]. Here the role of conservativity is different. Once Charlie's view is replaced by the single value v, the lifting problem becomes a clean question about how much the information reaching Charlie changes when we condition

on the *fiber* event $G(\mathbf{X}) = v$. In the randomized setting this is a question about the transcript distribution that reaches Charlie; in the quantum setting it is a question about the final message state that reaches Charlie.

2 Main results

We prove that in the terminal-conservative model described above, the randomized and quantum lifting theorems do hold. That is, every sufficiently efficient conservative protocol for a lift $F(z, \mathbf{x}) = f(z, G(\mathbf{x}))$ can be converted into an ordinary two-party one-way protocol for $f(z, v)$, with error loss controlled by the corresponding mixing property of the gadget. In lower-bound form, our theorems have the shape

$$\mathrm{R}_{\varepsilon}^{\rightarrow,\mathrm{cons}}(F) \geq \mathrm{R}_{\varepsilon+\delta}^{\rightarrow}(f) \qquad \text{and} \qquad \mathrm{Q}_{\varepsilon}^{\rightarrow,\mathrm{cons}}(F) \geq \mathrm{Q}_{\varepsilon+\delta}^{\rightarrow}(f),$$

provided the gadget-induced extra error loss is at most δ. All quantum results assume no prior entanglement.

The main contribution of this paper is to identify a pseudorandomness condition that makes one-way lifting go through once Charlie's NOF view becomes conservative, and to prove randomized and quantum lifting theorems from this condition. In the terminal-conservative one-way NOF model, a *fiber* of G is $G^{-1}(v)$ for any $v \in \mathcal{V}$, we show informally:

1. If every fiber of G is pseudorandom against *cylinder intersections*, then randomized protocols for F lift to ordinary one-way randomized protocols for f.
2. If every fiber of G is pseudorandom against *generalized cylinder intersections*, then quantum protocols for F lift to ordinary one-way quantum protocols for f, and the two-party message length is the final message length of the NOF protocol.

Both hypotheses hold for the generalized inner product (GIP) gadget with suitable block length, and they hold non-explicitly for random gadgets in a much larger player regime. We will elaborate on these results.

We view our results as accomplishing a natural intermediate goal. They do not resolve full one-way NOF lifting, but they isolate the terminal obstruction above and show that, once this obstruction is removed, the remaining one-way NOF chain can still be handled. With the explicit generalized inner product gadget, the resulting lower bounds apply in the familiar logarithmic-player regime with $k = O(\log n)$ nonterminal senders for standard instantiations. With non-explicit random gadgets, the same lifting theorems give benchmark lower bounds for superlogarithmically many senders.

2.1 Randomized lifting

The generalized inner product is defined as:

$$\mathrm{GIP}_{q,r}^{(k)}(\mathbf{x}_1, \ldots, \mathbf{x}_k) = \sum_{t=1}^{r} \prod_{i=1}^{k} \mathbf{x}_{i,t} \pmod{q}.$$

Our randomized lifting theorem reads

▶ **Theorem 1** (Randomized lifting via GIP (informal Theorem 15)). *Given $k \geq 2$, let $q > 2k$ be prime. Let Z be an arbitrary finite set. For any $f\colon Z \times \mathbb{F}_q \to \{0,1\}$, and $F = f \circ \mathrm{GIP}_{q,r}^{(k)}$ where $r \geq 2^k \log_{q/2k}\left(2^{\mathrm{R}_{\varepsilon+\delta}^{\rightarrow}(f)} q/\delta\right)$, we have $\mathrm{R}_{\varepsilon}^{\rightarrow,\mathrm{cons}}(F) \geq \mathrm{R}_{\varepsilon+\delta}^{\rightarrow}(f)$.*

For the most natural regime where $k \ll q$, the gadget input of F has length $O(2^k \cdot (\log|Z| + \log q))$. For standard outer problems such as the index function, choosing the GIP parameters so that the loss is constant gives polynomial communication lower bounds while keeping the total lifted input length polynomial, as long as the number of nonterminal senders satisfies $k = O(\log n)$, where n denotes the resulting total input length. This is the familiar logarithmic-player regime caused by the 2^k dependence in the GIP block length.

▶ **Theorem 2** (Explicit $O(\log n)$-player lower bound). *For any k, there is a family of functions F_k such that for the $(k+1)$-player communication game*

$$\mathrm{R}^{\to,\mathrm{cons}}(F_k) = \Omega\left(\frac{n}{k2^k}\right).$$

We also record another modest application: Take Boolean Hidden Matching as the outer function, its one-way quantum-classical separation is inherited in the conservative model.

▶ **Theorem 3** (A quantum-classical separation (informal)). *For any $k \geq 2$, there is a family of functions F_k for $(k+1)$-player conservative NOF model, such that*

$$\mathrm{Q}^{\to,\mathrm{cons}}_{1/3}(F) = O(\log n), \qquad \mathrm{R}^{\to,\mathrm{cons}}_{1/3}(F) \geq \widetilde{\Omega}\left(\sqrt{\frac{n}{k2^k}}\right).$$

For the full one-way NOF communication, an exponential separation for the *search* problem was recently established by an exciting work of Yang and Zhang [22], while here we consider *decision* problem.

As alluded above, the proof principle is terminal mixing. Fix the public randomness and a complete communication transcript t. The set of gadget inputs $\mathbf{x}$ that produce t is a cylinder intersection; we call it the *transcript cell* of t. For a value v, the *fiber* $G^{-1}(v)$ is the set of gadget inputs consistent with v. If every fiber looks nearly uniform to cylinder-intersection tests, then conditioning on $G(\mathbf{X}) = v$ barely changes the distribution of transcript cells. The desired mixing statement is that, for every transcript cell S and every value v,

$$\Pr[\mathbf{X} \in S \mid G(\mathbf{X}) = v] \approx \Pr[\mathbf{X} \in S].$$

In words, conditioning on the fiber should barely change the distribution of the transcript cell. This is the basic *fiber-mixing* phenomenon. In the full model, however, transcript mixing is not enough: Charlie still sees his NOF view of the gadget input, so knowing the transcript and v does not determine what additional information he retains about the location of $\mathbf{x}$ inside the fiber $G^{-1}(v)$. Even perfect transcript mixing therefore need not control Charlie's total information. The same terminal obstruction persists in the quantum case, where Charlie's decision is made from the final received state together with his remaining input.

A key notion in the randomized analysis is *fiber discrepancy*. For a gadget $G : X \to \mathcal{V}$, it is the largest possible bias

$$|\Pr[\mathbf{X} \in S \mid G(\mathbf{X}) = v] - \Pr[\mathbf{X} \in S]|$$

over all gadget values v and all cylinder intersections $S \subseteq X$. Thus fiber discrepancy is exactly the quantitative form of the fiber-mixing condition for transcript cells, because every deterministic one-way transcript cell is a cylinder intersection. If G has fiber discrepancy Δ_G and $F = f \circ G$, then a C-bit public-coin conservative protocol for F yields a C-bit public-coin ordinary one-way protocol for f with additive error loss at most $2^C\Delta_G$. Equivalently,

$$\mathrm{R}^{\to,\mathrm{cons}}_{\varepsilon}(F) \geq \mathrm{R}^{\to}_{\varepsilon+\delta}(f)$$

whenever $2^{\mathrm{R}^{\rightarrow}_{\varepsilon+\delta}(f)}\Delta_G \le \delta$. The factor 2^C is the natural loss for a black-box simulation that uses only a uniform fiber-discrepancy bound and then sums over transcript cells: after fixing the public randomness, the transcript lies in $\{0,1\}^{\le C}$, each transcript cell is a cylinder intersection, and summing over all cells gives total-variation loss $\le 2^C\Delta_G$. This is precisely the fiber-mixing principle above: after conditioning on $G(\mathbf{X}) = v$, the terminal transcript distribution is close to the unconditional one, so the ordinary one-way simulation can reproduce Charlie's randomized view using only the outer value v.

This black-box loss of the factor 2^C is nevertheless harmless for the explicit GIP gadget in the intended parameter range, because its fiber discrepancy is exponentially small in the gadget block length. For a prime q and block length r, the generalized inner product gadget is

$$\mathrm{GIP}^{(k)}_{q,r}(\mathbf{x}_1,\dots,\mathbf{x}_k) = \sum_{t=1}^{r}\prod_{j=1}^{k} x_{j,t} \in \mathbb{F}_q, \qquad \mathbf{x}_j \in \mathbb{F}_q^r.$$

For $G = \mathrm{GIP}^{(k)}_{q,r}$, adapting the character-sum estimate of Yang–Zhang [21, Lemma 3.2], one can show $\Delta_G \le 4q\,(k/q)^{r/2^{k-1}}$. Thus the loss term is on the order of $2^C\Delta_G \lesssim 2^C q\,(k/q)^{r/2^{k-1}}$. If the outer problem requires $C = \mathrm{R}^{\rightarrow}_{\varepsilon+\delta}(f)$ bits, then fixed loss δ is achieved by taking, up to constants,

$$r \gtrsim \frac{2^k\,(C + \log(q/\delta))}{\log(q/k)}.$$

2.2 Quantum lifting

Our quantum lifting theorem reads

▶ **Theorem 4** (Quantum one-way lifting via GIP (informal)). *Given $k \ge 2$, let $q > 2k$ be prime. Let Z be a finite set. For any $f\colon Z \times \mathbb{F}_q \to \{0,1\}$, and $F = f \circ \mathrm{GIP}^{(k)}_{q,r}$ where $r \ge 2^k \log_{q/(k-1)}\left(2^{2\mathrm{Q}^{\rightarrow}_{\varepsilon+\delta}(f)+2}q/\delta\right)$, we have*

$$\mathrm{Q}^{\rightarrow,\mathrm{cons}}_{\varepsilon}(F) \ge \mathrm{Q}^{\rightarrow}_{\varepsilon+\delta}(f).$$

The parameters in the quantum lifting theorem are similar to those of our randomized lifting theorem. Thus the quantum lifting and randomized lifting behave similarly using the GIP gadget. We can think of the gadget input of F of length $O(2^k\cdot(\log|Z| + \log q))$, for the natural regime $k \ll q$. For the index function, analogous to Theorem 2, choosing the GIP parameters so that the fiber discrepancy loss is constant gives polynomial quantum communication lower bounds in the terminal-conservative model for $k = O(\log n)$ nonterminal senders, again with n denoting the resulting total input length.

The quantum analogue replaces fiber mixing by *final-state mixing*. For fixed outer input z and gadget value v, let $\rho_{z,\mathbf{x}}$ denote the final message state on gadget input $\mathbf{x}$, let

$$\rho_{z,v} := \mathbb{E}_{\mathbf{X}\sim\mathrm{Uni}_{X_v}}[\rho_{z,\mathbf{X}}], \qquad \sigma_z := \mathbb{E}_{\mathbf{Y}\sim\mathrm{Uni}_X}[\rho_{z,\mathbf{Y}}].$$

The ordinary one-way simulation has Alice send the unconditional state σ_z, while Bob uses v to perform Charlie's terminal measurement. The analysis therefore bounds, for the relevant terminal effect E_v,

$$\left|\mathrm{Tr}\left(E_v(\sigma_z - \rho_{z,v})\right)\right|.$$

Thus the quantum theorem is again a terminal-mixing theorem; only the object being mixed changes from a transcript distribution to a density matrix.

The pseudorandom measure for this state-mixing statement is the fiber discrepancy against the *generalized cylinder intersection* Δ_G^{Π}. It measures how much conditioning on a fiber can bias tests of the form

$$\prod_{i=1}^{k} \phi_i(\mathbf{x}_{-i}), \qquad |\phi_i| \le 1,$$

where each factor $\phi_i : X_{-i} \to \mathbb{C}$ is a bounded cylinder function visible to one sender in the one-way chain. These are precisely the tests generated by the quantum expansion of the final message state. If Δ_G^{Π} is small and a conservative one-way quantum protocol for F uses message lengths $c_1, \dots, c_k$, then the protocol yields an ordinary one-way quantum protocol for f that uses only the final c_k qubits, with additive loss

$$2^{2c_{\mathrm{pre}}}\Delta_G^{\Pi}, \qquad c_{\mathrm{pre}} = c_1 + \cdots + c_{k-1}.$$

The factor $2^{2c_{\mathrm{pre}}}$ is the dimension loss from expanding the prefix message spaces; the terminal message itself is not expanded, which is why the conclusion is a final-message lower bound.

We prove that $\mathrm{GIP}_{q,r}^{(k)}$ fools the generalized cylinder intersections appearing in the quantum theorem. In particular,

$$\Delta_G^{\Pi} \lesssim 4q \left(\frac{k}{q}\right)^{r/2^{k-1}}.$$

2.3 Random gadgets as a non-explicit benchmark

Finally, we analyze uniformly random gadgets as a non-explicit benchmark. Here the gadget is a random function

$$G_m : [m]^k \to \mathbb{F}_q,$$

where all values are chosen independently and uniformly. The parameter q is the outer alphabet size, and $\lceil \log m \rceil$ is the per-player gadget input length. For comparison, $\mathrm{GIP}_{q,r}^{(k)}$ has the same outer alphabet size q, per-player domain size $m = q^r$, and per-player gadget input length $\lceil r \log q \rceil$. The random-gadget analysis is a standard random-function discrepancy calculation against the same cylinder and generalized cylinder classes that appear in the lifting theorems, in the spirit of the usual analysis of random NOF functions. Its role is therefore not to provide a new explicit lower-bound method, but to calibrate the framework and expose which parameter losses come from the currently available explicit gadgets.

Suppressing constant error and failure parameters, the comparison is simple. For randomized protocols with communication budget b, a random gadget has sufficiently small fiber discrepancy once

$$m \gtrsim q\, 2^{2b}(k + \log q).$$

For quantum protocols with prefix budget $c_{\mathrm{pre}} \le b$, a random gadget has sufficiently small fiber discrepancy against generalized cylinder intersections, and hence sufficiently small state-mixing error, once

$$m \gtrsim q\, 2^{4b}\left(k(b + \log k) + \log q\right).$$

Equivalently, the quantum benchmark has per-player input length

$$\log m = O(\log q + b + \log k).$$

By contrast, the explicit GIP quantum instantiation requires roughly

$$r \gtrsim 2^{k-1} \frac{2b + \log q}{\log(q/(k-1))}$$

to achieve the same fixed loss. Thus the explicit and random gadgets play complementary roles. The GIP gadget gives explicit lifting theorems, but its block length grows like 2^k, which naturally limits polynomial-size instantiations to $k = O(\log n)$ nonterminal senders. Random gadgets show that this limitation is not inherent to the terminal-conservative lifting argument: non-explicitly, the same argument works without an exponential dependence on k in the per-player input length. For instance, using the index function as the outer problem, the random-gadget benchmark gives unconditional randomized and quantum total-communication lower bounds of order $\Omega(\sqrt{n})$ with $k = \Omega(\sqrt{n}) = \omega(\log n)$ nonterminal senders, where here n denotes the total lifted input length.

▶ **Theorem 5** (Implicit polynomial-player lower bound). *For any $k \geq 2$, there is a family of functions F_k such that for the $(k+1)$-player communication game*

$$\mathrm{R}^{\rightarrow,\mathrm{cons}}(F_k) = \tilde{\Omega}\left(\frac{n}{k}\right).$$

Derandomizing this benchmark would require explicit gadgets with very strong NOF-type pseudorandomness, a task comparable in spirit to proving strong explicit NOF lower bounds rather than a routine extension of the present work.

3 Preliminaries

We use the following conventions throughout the paper. For an integer m, write $[m] = \{1, \ldots, m\}$. Unless otherwise indicated, logarithms are base two. All sets are finite. For a finite set A, we write Uni_A for the uniform distribution on A. For distributions P, Q on the same finite set, their total variation distance is

$$\mathrm{TV}(P, Q) := \frac{1}{2} \sum_{\omega} |P(\omega) - Q(\omega)|.$$

All randomized protocols are public-coin protocols. All quantum protocols are without prior entanglement; local ancillas are allowed and are not counted as communication. All error guarantees are worst-case, restricted to promised inputs when a promise is present. We use $\tilde{O}(\cdot), \tilde{\Omega}(\cdot)$ to hide polylogarithmic factors.

3.1 Lifted problems and gadget notation

Fix $k \geq 2$. In this paper k denotes the number of gadget coordinates, or equivalently the number of nonterminal NOF senders; including the terminal player, Charlie, the protocol has $k+1$ players. Let

$$X = X_1 \times \cdots \times X_k$$

be the gadget input space. We write

$$\mathbf{x} = (\mathbf{x}_1, \ldots, \mathbf{x}_k) \in X, \qquad \mathbf{x}_{-i} := (\mathbf{x}_1, \ldots, \mathbf{x}_{i-1}, \mathbf{x}_{i+1}, \ldots, \mathbf{x}_k),$$

and

$$X_{-i} := \prod_{j \neq i} X_j.$$

Thus $\mathbf{x}_{-i}$ is the number-on-the-forehead view of the gadget input available to the ith nonterminal sender.

Let $G : X \to \mathcal{V}$ be a surjective gadget. For $v \in \mathcal{V}$, its fiber is

$$X_v := G^{-1}(v) = \{\mathbf{x} \in X : G(\mathbf{x}) = v\}.$$

Surjectivity is only a notational convenience: it ensures that every X_v is nonempty. Given an outer Boolean function $f : Z \times \mathcal{V} \to \{0,1\}$, its lift by G is

$$F : Z \times X \to \{0,1\}, \qquad F(z, \mathbf{x}) := f\big(z, G(\mathbf{x})\big).$$

For partial functions or promise relations, the lifted promise is obtained by requiring $(z, G(\mathbf{x}))$ to be a promised outer input. Correctness is then required only on this lifted promise.

3.2 Randomized one-way protocols

▶ **Definition 6** (Conservative one-way blackboard NOF protocol). *A conservative one-way blackboard protocol for $F = f \circ G$ has nonterminal players $P_1, \dots, P_k$ and a terminal player, Charlie. The nonterminal players speak once in the order*

$$P_1 \to P_2 \to \cdots \to P_k \to \textit{Charlie}.$$

Communication takes place on a public blackboard. The blackboard content after round i is denoted by τ_i, with τ_0 equal to the empty string. The protocol has a public randomness space $\mathcal{R}$, message maps

$$M_i : Z \times X_{-i} \times \mathcal{R} \times \{0,1\}^* \to \{0,1\}^* \qquad (i \in [k]),$$

and a decoder

$$\mathsf{DEC} : \mathcal{V} \times \mathcal{R} \times \{0,1\}^* \to \{0,1\}.$$

On input $(z, \mathbf{x})$ and public coins $r \in \mathcal{R}$, player P_i sees $z, \mathbf{x}_{-i}, r$, and the current transcript τ_{i-1}, writes

$$m_i := M_i(z, \mathbf{x}_{-i}, r, \tau_{i-1}),$$

and the new transcript is $\tau_i := \tau_{i-1} m_i$. The terminal player sees only $(v := G(\mathbf{x}), r, \tau_k)$, and outputs $\mathsf{DEC}(v, r, \tau_k)$. The cost of the protocol is $\max_{(z,\mathbf{x}),r} |\tau_k|$.

The adjective "conservative" refers only to the terminal player Charlie: the nonterminal players retain their usual NOF views, while the terminal player does not see any residual NOF view of the gadget inputs beyond $G(\mathbf{x})$.

▶ **Definition 7** (Two-party one-way randomized protocol). *Let $f : Z \times \mathcal{V} \to \{0,1\}$. A public-coin two-party one-way protocol for f consists of a public randomness space $\mathcal{R}$, a deterministic message map*

$$A : Z \times \mathcal{R} \to \{0,1\}^*,$$

and a deterministic decoder

$$B : \mathcal{V} \times \mathcal{R} \times \{0,1\}^* \to \{0,1\}.$$

On input (z, v) and public coins r, Alice sends $A(z, r)$ and Bob outputs $B(v, r, A(z, r))$. The cost is $\max_{z,r} |A(z, r)|$.

For $\eta \in [0,1]$, let $\mathrm{R}^{\to}_{\eta}(f)$ denote the minimum cost of a public-coin two-party one-way protocol for f with worst-case error at most η. Let $\mathrm{R}^{\to,\mathrm{cons}}_{\eta}(F)$ denote the corresponding minimum cost in the conservative one-way blackboard NOF model. The same notation is used for partial Boolean functions, with the error guarantee required only on promised inputs.

3.3 Cylinder intersections and fiber discrepancy

▶ **Definition 8** (Cylinder and cylinder intersection). *A set $C_i \subseteq X$ is an i-cylinder if membership in C_i does not depend on the ith coordinate. Equivalently, C_i is the preimage of a subset of X_{-i} under the projection $X \to X_{-i}$.*

A cylinder intersection is a set of the form $C_1 \cap \cdots \cap C_k$, where C_i is an i-cylinder for every $i \in [k]$. We write $\mathrm{CI}(X)$ for the family of cylinder intersections in X.

Cylinder intersections are the basic combinatorial objects behind randomized NOF lifting. After the public randomness and the outer input z are fixed, every deterministic transcript cell of a conservative blackboard protocol is a cylinder intersection: the condition that P_i writes a prescribed message depends only on $\mathbf{x}_{-i}$ and on the previous transcript.

▶ **Definition 9** (Fiber discrepancy against cylinder intersections). *Let $G : X \to \mathcal{V}$ be surjective. The fiber discrepancy of G against cylinder intersections is*

$$\Delta_G := \sup_{v \in \mathcal{V}} \sup_{S \in \mathrm{CI}(X)} \left| \Pr_{\mathbf{X} \sim \mathrm{Uni}_{X_v}} [\mathbf{X} \in S] - \Pr_{\mathbf{X} \sim \mathrm{Uni}_X} [\mathbf{X} \in S] \right|.$$

Thus Δ_G measures how well each fiber X_v looks like the whole gadget domain X to every NOF transcript cell. This is the pseudorandomness notion used in the randomized lifting theorem.

3.4 Finite-field gadgets and Fourier correlation

For the explicit gadget instantiations we work over a prime field $\mathbb{F}_q$. We fix a nontrivial additive character $\chi : \mathbb{F}_q \to \mathbb{C}$; for example, after identifying $\mathbb{F}_q$ with $\mathbb{Z}/q\mathbb{Z}$, one may take $\chi(t) = \exp(2\pi i t/q)$. We use the orthogonality identity

$$\frac{1}{q} \sum_{\alpha \in \mathbb{F}_q} \chi(\alpha t) = \mathbf{1}[t = 0].$$

For $\mathbf{x}_i = (x_{i,1}, \ldots, x_{i,r}) \in \mathbb{F}_q^r$, define the generalized inner product gadget

$$\mathrm{GIP}^{(k)}_{q,r}(\mathbf{x}_1, \ldots, \mathbf{x}_k) := \sum_{t=1}^{r} \prod_{i=1}^{k} x_{i,t} \in \mathbb{F}_q.$$

▶ **Definition 10** (Fourier correlation). *Let $G : X \to \mathbb{F}_q$ be a gadget. Its Fourier correlation against cylinder intersections is*

$$\mathrm{FCorr}(G) := \sup_{\alpha \in \mathbb{F}_q^{\times}} \sup_{S \in \mathrm{CI}(X)} \left| \mathbb{E}_{\mathbf{X} \sim \mathrm{Uni}_X} \left[\mathbf{1}[\mathbf{X} \in S]\, \chi\big(\alpha G(\mathbf{X})\big) \right] \right|.$$

For the GIP gadget, Yang–Zhang's character-sum estimate [21, Lemma 3.2] bounds this quantity by $\gamma_k(q, r)$. Fourier inversion then converts this correlation bound into a bound on the fiber discrepancy Δ_G.

3.5 Quantum one-way protocols

▶ **Definition 11** (Conservative one-way quantum protocol). *A conservative one-way quantum protocol for $F = f \circ G$ has nonterminal players $P_1, \dots, P_k$ and terminal player Charlie. Let $c_1, \dots, c_k$ be the message lengths and set $d_i := 2^{c_i}$. The incoming register to P_1 is the one-dimensional register $\mathcal{H}_0$, and the outgoing register of P_i is $\mathcal{H}_i \cong \mathbb{C}^{d_i}$.*

For each $i \in [k]$ and each local view $(z, \mathbf{x}_{-i})$, player P_i applies a completely positive trace-preserving map

$$\Lambda_i^{(z,\mathbf{x}_{-i})} : \mathcal{D}(\mathcal{H}_{i-1}) \to \mathcal{D}(\mathcal{H}_i).$$

The players act in the order

$$P_1 \to P_2 \to \cdots \to P_k \to \text{Charlie}.$$

The terminal player sees only $v := G(\mathbf{x})$ and the final message register $\mathcal{H}_k$, and outputs a bit using a binary measurement depending on v. The cost is $c_1 + \cdots + c_k$.

For a fixed protocol and input $(z, \mathbf{x})$, we write $\rho_{z,\mathbf{x}}$ for the final message state received by the terminal player. We also use the average states

$$\rho_{z,v} := \mathbb{E}_{\mathbf{X} \sim \mathrm{Uni}_{X_v}}[\rho_{z,\mathbf{X}}], \qquad \sigma_z := \mathbb{E}_{\mathbf{Y} \sim \mathrm{Uni}_X}[\rho_{z,\mathbf{Y}}].$$

These are the fiber-conditioned and unconditional final-message states, respectively.

▶ **Definition 12** (Two-party one-way quantum protocol). *Let $f : Z \times \mathcal{V} \to \{0,1\}$. A cost-$C$ two-party one-way quantum protocol for f consists of a density operator σ_z on a C-qubit register for each $z \in Z$, and a binary POVM $(E_v, I - E_v)$ for each $v \in \mathcal{V}$. Alice sends σ_z, and Bob measures it using the POVM indexed by v.*

For $\eta \in [0,1]$, let $\mathrm{Q}_\eta^{\to}(f)$ denote the minimum cost of a two-party one-way quantum protocol for f with worst-case error at most η. Let $\mathrm{Q}_\eta^{\to,\mathrm{cons}}(F)$ denote the minimum total cost of a conservative one-way quantum protocol for F with worst-case error at most η. The same notation is used for partial Boolean functions, with the error guarantee required only on promised inputs.

3.6 Generalized cylinder intersections

The quantum lifting theorem uses a second pseudorandomness notion. It tests the fibers of the gadget against bounded products of NOF-local functions, which are exactly the tests produced by expanding the prefix of a conservative quantum protocol.

▶ **Definition 13** (Fiber discrepancy against generalized cylinder intersections). *Let $G : X \to \mathcal{V}$ be surjective. The fiber discrepancy of G against the generalized cylinder intersections is*

$$\Delta_G^{\Pi} := \sup_{v \in \mathcal{V}} \sup_{\substack{\phi_i : X_{-i} \to \mathbb{C} \\ |\phi_i| \le 1 \text{ for every } i \in [k]}} \left| \mathbb{E}_{\mathbf{X} \sim \mathrm{Uni}_{X_v}} \left[\prod_{i=1}^k \phi_i(\mathbf{X}_{-i}) \right] - \mathbb{E}_{\mathbf{X} \sim \mathrm{Uni}_X} \left[\prod_{i=1}^k \phi_i(\mathbf{X}_{-i}) \right] \right|.$$

▶ **Definition 14** (Product Fourier correlation). *For a gadget $G : X \to \mathbb{F}_q$, define*

$$\mathrm{PCorr}(G) := \sup_{\alpha \in \mathbb{F}_q^\times} \sup_{\substack{\phi_i : X_{-i} \to \mathbb{C} \\ |\phi_i| \le 1 \text{ for every } i \in [k]}} \left| \mathbb{E}_{\mathbf{X} \sim \mathrm{Uni}_X} \left[\chi\big(\alpha G(\mathbf{X})\big) \prod_{i=1}^k \phi_i(\mathbf{X}_{-i}) \right] \right|.$$

Product Fourier correlation is used only for gadgets with output alphabet $\mathbb{F}_q$. As in the randomized setting, Fourier inversion converts small $\mathrm{PCorr}(G)$ into small Δ_G^{Π}.

3.7 Matrix units

Whenever a message register is identified with $\mathbb{C}^d$, we fix an orthonormal basis $e_1, \dots, e_d$ and write $E_{ab} := |e_a\rangle\langle e_b|$ for the corresponding matrix units, where $1 \le a, b \le d$. When several message registers are present, we write $E_{ab}^{(i)}$ for the matrix unit in the ith message register. The first subscript is the row index and the second subscript is the column index, so $\mathrm{Tr}\big(E_{uv}^{(i)} E_{ab}^{(i)}\big) = \delta_{v,a}\delta_{u,b}$. For the one-dimensional incoming register before the first sender, we set $d_0 = 1$ and use the single matrix unit $E_{11}^{(0)}$.

3.8 Benchmark outer problems

For a prime q, the index function is

$$\mathrm{INDEX}_q : \{0,1\}^{\mathbb{F}_q} \times \mathbb{F}_q \to \{0,1\}, \qquad \mathrm{INDEX}_q(z, v) := z(v).$$

We use the standard Nayak's random-access-code lower bound: for every $0 \le \eta < 1/2$ [16],

$$\mathrm{Q}^{\rightarrow}_{\eta}(\mathrm{INDEX}_q) \ge (1 - H(\eta))q,$$

where $H(\eta) := -\eta \log_2 \eta - (1-\eta)\log_2(1-\eta)$ is the binary entropy function, with $H(0) = 0$.

We also use the standard Boolean Hidden Matching partial function BHM_n as a calibration example. Alice receives $u \in \{0,1\}^{2n}$; Bob receives a perfect matching M on $[2n]$ and a string $w \in \{0,1\}^n$, promised that either $w_e = u_i \oplus u_j$ for every edge $e = (i,j) \in M$, or $w_e = u_i \oplus u_j \oplus 1$ for every edge $e = (i,j) \in M$. The desired output is the corresponding case bit. We use the known bounds [2, 8],

$$\mathrm{Q}^{\rightarrow}_{1/3}(\mathsf{BHM}_n) = O(\log n), \qquad \mathrm{R}^{\rightarrow}_{1/3}(\mathsf{BHM}_n) = \Omega(\sqrt{n}),$$

with constant changes in the error parameter absorbed by standard amplification.

In the following section, we provide the details of the randomized lifting theorem on the GIP gadget. The proofs of the remaining theorems can be found in the full version.

4 Randomized lifting

Our randomized lifting theorem reads as follows.

▶ **Theorem 15** (Randomized lifting via GIP). *Given $k \ge 2$, let $q > 2k$ be prime. Let Z be an arbitrary finite set. For any $f\colon Z \times \mathbb{F}_q \to \{0,1\}$, define*

$$F\colon Z \times (\mathbb{F}_q^r)^k \to \{0,1\}, \qquad F(z, \mathbf{x}_1, \dots, \mathbf{x}_k) := f\big(z, \mathrm{GIP}^{(k)}_{q,r}(\mathbf{x}_1, \dots, \mathbf{x}_k)\big).$$

Let $0 \le \varepsilon \le 1$ and $0 < \delta \le 1 - \varepsilon$ be constants. If $r \ge 2^k \log_{q/2k}\left(\frac{2^{\mathrm{R}^{\rightarrow}_{\varepsilon+\delta}(f)} q}{\delta}\right)$, we have

$$\mathrm{R}^{\rightarrow,\mathrm{cons}}_{\varepsilon}(F) \ge \mathrm{R}^{\rightarrow}_{\varepsilon+\delta}(f).$$

Moreover, since $\mathrm{R}^{\rightarrow}_{\varepsilon+\delta}(f) \lesssim \log|Z|$, it suffices to take $r = \left\lceil 2^k \frac{\log|Z| + \log(q/\delta)}{\log q/2k} \right\rceil$. The input length $|z| = \lceil \log|Z| \rceil$ and $|\mathbf{x}_i| = \lceil r \log q \rceil = \Theta_\delta\left(2^k \frac{\log q}{\log q/2k}(\log|Z| + \log q)\right)$, $\forall i \in [k]$.

Before we prove the above theorem, we collect the following three technical lemmas.

▶ **Lemma 16** (Key lifting lemma). *Suppose the gadget function $G\colon X \to \mathcal{V}$ has fiber discrepancy Δ_G. Let $f\colon Z \times \mathcal{V} \to \{0,1\}$. For any $z \in Z$ and $\mathbf{x} \in X$, define $F(z,\mathbf{x}) := f\big(z, G(\mathbf{x})\big)$. If F has a public-coin conservative one-way protocol with cost C bits and worst-case error $\le \varepsilon$, then f has a public-coin two-party one-way protocol with cost C bits and worst-case error $\le \varepsilon + 2^C\Delta_G$.*

▶ **Lemma 17** (GIP cylinder-correlation bound). *Let $G = \mathrm{GIP}^{(k)}_{q,r}\colon (\mathbb{F}_q^r)^k \to \mathbb{F}_q$. Denote $\gamma_k(q,r) := \left(\frac{k}{q}\right)^{r/2^{k-1}}$. We have $\mathrm{FCorr}(G) \le \gamma_k(q,r)$.*

▶ **Lemma 18** (Fourier correlation implies fiber discrepancy). *Let $G\colon X \to \mathbb{F}_q$ be surjective. If $\mathrm{FCorr}(G) \le \gamma$ and $q\gamma < 1/2$, then $\Delta_G \le 4q\gamma$.*

With these three lemmas at our disposal, we prove the main Theorem 15.

Proof of Theorem 15. Consider any public-coin conservative one-way blackboard protocol for F with cost C and worst-case error at most ε. We prove that necessarily $C \ge \mathrm{R}^{\rightarrow}_{\varepsilon+\delta}(f)$ as follows

Indeed, for contradiction, suppose $C < \mathrm{R}^{\rightarrow}_{\varepsilon+\delta}(f)$ By Lemma 16, there is a public-coin two-party one-way protocol for f with cost C and worst-case error at most $\varepsilon + 2^C\Delta_G$.

Let $G := \mathrm{GIP}^{(k)}_{q,r}$. Recall that $\gamma_k(q,r) = (k/q)^{r/2^{k-1}}$. By hypothesis

$$r \ge 2^k \log_{q/2k}\left(\frac{2^{R^{\rightarrow}_{\varepsilon+\delta}(f)}q}{\delta}\right),$$

we have $q\,\gamma_k(q,r) \le \frac{1}{q} < 1/2$. So by Lemmas 18 and 17, $\Delta_G \le 4q\,\gamma_k(q,r)$. Therefore

$$\varepsilon + 2^C\Delta_G \le \varepsilon + 2^C \cdot 4q\,\gamma_k(q,r) < \varepsilon + 2^{\mathrm{R}^{\rightarrow}_{\varepsilon+\delta}(f)+2}q\,\gamma_k(q,r) \le \varepsilon + \delta.$$

The last inequality follows by rearranging $r \ge 2^k \log_{q/2k}\left(\frac{2^{R_{\varepsilon+\delta}(f)}q}{\delta}\right)$ to get $\gamma_k(q,r) \le \delta/(2^{\mathrm{R}^{\rightarrow}_{\varepsilon+\delta}(f)+2}q)$.

So a public-coin two-party one-way protocol for f with worst-case error $\varepsilon+\delta$ and cost $C < \mathrm{R}^{\rightarrow}_{\varepsilon+\delta}(f)$ would exist, which is impossible ◀

4.1 Proof of the lemmas

In this subsection, we complete the proof by proving Lemmas 16-18. We first show that the transcript cells are cylinder intersections.

▶ **Lemma 19.** *Fix input $z \in Z$ and randomness $\rho \in \mathcal{R}$. Given a conservative one-way blackboard protocol of cost C, let $T_{z,\rho}\colon X \to \{0,1\}^{\le C}$ be the transcript map, where $\{0,1\}^{\le C} := \bigcup_{c=0}^{C}\{0,1\}^c$. Then, for every transcript τ, $T^{-1}_{z,\rho}(\tau)$ is a cylinder intersection of X.*

Proof. Fix a transcript τ. It uniquely determines the messages $m_1,\dots,m_k$ and the intermediate blackboard strings $\tau_0,\tau_1,\dots,\tau_k$, where $\tau_0 = \emptyset$, $\tau_k = \tau$, and $\tau_i = \tau_{i-1}m_i$. For each $i \in [k]$, define $C_i := \big\{\mathbf{x} \in X : M_i(z,\mathbf{x}_{-i},\rho,\tau_{i-1}) = m_i\big\}$. The defining condition depends on $\mathbf{x}$ only through $\mathbf{x}_{-i}$, so C_i is an i-cylinder.

We prove that the transcript cell is a cylinder intersection: $T^{-1}_{z,\rho}(\tau) = C_1 \cap \cdots \cap C_k$ as follows. On the one hand, if $\mathbf{x} \in T^{-1}_{z,\rho}(\tau)$, then the deterministic protocol on input $(z,\mathbf{x})$ and coins ρ produces the messages $m_1,\dots,m_k$, and the blackboard strings $\tau_1,\dots,\tau_k$. Therefore $\mathbf{x} \in C_i$ for every $i \in [k]$; On the other hand, if $\mathbf{x} \in C_1 \cap \cdots \cap C_k$, we prove by induction on i that the protocol on input $(z,\mathbf{x})$ and coins ρ produces the $m_1,\dots,m_i$, and $\tau_1,\dots,\tau_i$, during the first i rounds. The case $i = 1$ is immediate from the definition of C_1. Assume the claim

holds up to round $i-1$. Then player P_i sees the current transcript τ_{i-1}, and because $\mathbf{x} \in C_i$, the next message is exactly m_i. Hence the next blackboard string is $\tau_i = \tau_{i-1}m_i$. Therefore the final transcript is τ, so $\mathbf{x} \in T_{z,\rho}^{-1}(\tau)$. ◀

Then we could prove the key lifting lemma, which translates the conservative protocol to ordinary two-party one-way protocol and control the error by fiber discrepancy.

Proof of Lemma 16. Fix a cost C public-coin conservative one-way blackboard protocol Π for F with worst-case error $\leq \varepsilon$. Let $\mathcal{T} := \{0,1\}^{\leq C}$, $\{0,1\}^{\leq C} := \bigcup_{c=0}^{C}\{0,1\}^c$, and let ω denote the distribution of the public coins. For each $z \in Z$ and $\rho \in \mathcal{R}$, let $T_{z,\rho}\colon X \to \mathcal{T}$ be the final transcript map.

Construct a public-coin two-party one-way protocol Π' for f as follows. Sample the public coins ρ according to ω. On input z, Alice samples $\mathbf{Y} \sim \mathrm{Uni}_X$ and computes transcript $\tau := T_{z,\rho}(\mathbf{Y}) \in \mathcal{T}$ according to Π. Alice sends τ to Bob. On input v, Bob applies the decoder DEC from Π to output $\mathsf{DEC}(v,\rho,\tau)$. Since $|\tau| \leq C$, the cost of Π' is $\leq C$.

Next, we analyze the error probability of Π'. Fix $(z,v) \in Z \times \mathcal{V}$. Define two distributions $\mu_{z,v}$ and ν_z on $\mathcal{R} \times \mathcal{T}$ by

$$\mu_{z,v}(\rho,\tau) := \omega(\rho) \Pr_{\mathbf{X}\sim\mathrm{Uni}_{X_v}}\big[T_{z,\rho}(\mathbf{X}) = \tau\big], \qquad \nu_z(\rho,\tau) := \omega(\rho) \Pr_{\mathbf{Y}\sim\mathrm{Uni}_X}\big[T_{z,\rho}(\mathbf{Y}) = \tau\big].$$

Since $(z,\mathbf{X},\rho)$ can determine τ, $\mu_{z,v}$ could be determined by ω and Uni_{X_v}. ν_z is similar. Notice that ρ, $\mathbf{X}$ and $\mathbf{Y}$ are independent.

Define the error set as s

$$E_{z,v} := \big\{(\rho,\tau) \in \mathcal{R} \times \mathcal{T} : \mathsf{DEC}(v,\rho,\tau) \neq f(z,v)\big\}.$$

First, we show that $\mu_{z,v}(E_{z,v})$ equals the error of Π averaged over the fiber X_v as follows. For any $\mathbf{x} \in X_v$, $G(\mathbf{x}) = v$ and $f(z,v) = F(z,\mathbf{x})$. For every fixed pair $(\rho,\mathbf{x}) \in \mathcal{R} \times X_v$, the protocol Π produces the final transcript $T_{z,\rho}(\mathbf{x})$ and then outputs $\mathsf{DEC}\big(v,\rho,T_{z,\rho}(\mathbf{x})\big)$. Therefore Π errs on $(z,\mathbf{x},\rho)$ if and only if $(\rho,T_{z,\rho}(\mathbf{x})) \in E_{z,v}$.

Because Π has worst-case error $\leq \varepsilon$, we have $\forall (z,\mathbf{x}) \in Z \times X_v$, $\Pr_\rho[\Pi \text{ errs on } (z,\mathbf{x})] \leq \varepsilon$. Then taking probability over $\mathbf{X} \sim \mathrm{Uni}_{X_v}$ gives

$$\mu_{z,v}(E_{z,v}) = \Pr_{\rho,\mathbf{X}}\big[\Pi \text{ errs on } (z,\mathbf{X})\big] \leq \varepsilon.$$

Secondly, we show that $\nu_z(E_{z,v})$ equals the error probability of Π' on input (z,v). Under Π', Alice sends $T_{z,\rho}(\mathbf{Y})$, and Bob outputs $\mathsf{DEC}(v,\rho,T_{z,\rho}(\mathbf{Y}))$. Hence Π' errs on (z,v,ρ) if and only if $(\rho,T_{z,\rho}(\mathbf{Y})) \in E_{z,v}$. Therefore $\nu_z(E_{z,v}) = \Pr_\rho\big[\Pi' \text{ errs on } (z,v)\big]$.

Now we compare $\mu_{z,v}$ and ν_z. By Lemma 19, $T_{z,\rho}^{-1}(\tau)$ belongs to $\mathrm{CI}(X)$. Hence, by the definition of fiber discrepancy (Definition 9), for every $(\rho,\tau) \in \mathcal{R} \times \mathcal{T}$,

$$\left|\Pr_{\mathbf{X}\sim\mathrm{Uni}_{X_v}}\big[T_{z,\rho}(\mathbf{X}) = \tau\big] - \Pr_{\mathbf{Y}\sim\mathrm{Uni}_X}\big[T_{z,\rho}(\mathbf{Y}) = \tau\big]\right| \leq \Delta_G.$$

Therefore

$$\begin{aligned}
\mathrm{TV}(\mu_{z,v},\nu_z) &= \frac{1}{2}\sum_{(\rho,\tau)\in\mathcal{R}\times\mathcal{T}} \big|\mu_{z,v}(\rho,\tau) - \nu_z(\rho,\tau)\big| \\
&= \frac{1}{2}\sum_{(\rho,\tau)\in\mathcal{R}\times\mathcal{T}} \omega(\rho)\left|\Pr_{\mathbf{X}\sim\mathrm{Uni}_{X_v}}\big[T_{z,\rho}(\mathbf{X}) = \tau\big] - \Pr_{\mathbf{Y}\sim\mathrm{Uni}_X}\big[T_{z,\rho}(\mathbf{Y}) = \tau\big]\right| \\
&\leq \frac{1}{2}\sum_{(\rho,\tau)\in\mathcal{R}\times\mathcal{T}} \omega(\rho)\Delta_G \\
&\leq \frac{1}{2}|\mathcal{T}|\Delta_G \\
&< 2^C\Delta_G.
\end{aligned}$$

Consequently,

$$\Pr\big[\Pi' \text{ errs on } (z,v)\big] = \nu_z(E_{z,v}) \le \mu_{z,v}(E_{z,v}) + \mathrm{TV}(\mu_{z,v},\nu_z) < \varepsilon + 2^C\Delta_G.$$

This holds for every $(z,v) \in Z \times \mathcal{V}$, so Π' has cost at most C and worst-case error at most $\varepsilon + 2^C\Delta_G$. ◀

We prove Lemma 17 and Lemma 18 as follows.

Proof of Lemma 17. This result has been proved by Yang and Zhang [21, Lemma 3.2]. We put the proof here for completeness. Fix $S \in \mathrm{CI}((\mathbb{F}_q^r)^k)$ and $\alpha \in \mathbb{F}_q^\times$. Choose i-cylinders $S_1,\dots,S_k$ such that $S = S_1 \cap \cdots \cap S_k$. Define

$$\Gamma_\alpha(S) := \mathbb{E}_{\mathbf{x}_1,\dots,\mathbf{x}_k}\left[\prod_{i=1}^k \mathbf{1}_{S_i}(\mathbf{x}_1,\dots,\mathbf{x}_k)\chi\left(\alpha\sum_{t=1}^r\prod_{i=1}^k x_{i,t}\right)\right].$$

Since $\mathbf{1}[\mathbf{x}\in S] = \prod_{i=1}^k \mathbf{1}_{S_i}(\mathbf{x})$, it is enough to prove $|\Gamma_\alpha(S)| \le \gamma_k(q,r)$.

Because S_k is a k-cylinder, the factor $\mathbf{1}_{S_k}(\mathbf{x}_1,\dots,\mathbf{x}_k)$ is independent of $\mathbf{x}_k$. Hence

$$|\Gamma_\alpha(S)|^2 \le \mathbb{E}_{\mathbf{x}_1,\dots,\mathbf{x}_{k-1}}\left|\mathbb{E}_{\mathbf{x}_k}\left[\prod_{i=1}^{k-1}\mathbf{1}_{S_i}(\mathbf{x}_1,\dots,\mathbf{x}_k)\chi\left(\alpha\sum_{t=1}^r x_{k,t}\prod_{i=1}^{k-1}x_{i,t}\right)\right]\right|^2.$$

Expanding the square introduces an independent copy $\mathbf{y}_k$ of $\mathbf{x}_k$; the new phase is

$$\chi\left(\alpha\sum_{t=1}^r(x_{k,t}-y_{k,t})\prod_{i=1}^{k-1}x_{i,t}\right).$$

At the next step, the factor coming from S_{k-1} is independent of $\mathbf{x}_{k-1}$, so the same argument can be applied to $\mathbf{x}_{k-1}$. Repeating this computation for $\mathbf{x}_k,\mathbf{x}_{k-1},\dots,\mathbf{x}_2$ introduces independent copies $\mathbf{y}_k,\mathbf{y}_{k-1},\dots,\mathbf{y}_2$ and yields

$$|\Gamma_\alpha(S)|^{2^{k-1}} \le \mathbb{E}_{\mathbf{x}_2,\dots,\mathbf{x}_k,\mathbf{y}_2,\dots,\mathbf{y}_k}\left|\mathbb{E}_{\mathbf{x}_1}\chi\left(\alpha\sum_{t=1}^r x_{1,t}\prod_{i=2}^k(x_{i,t}-y_{i,t})\right)\right|.$$

Fix the outer variables. If there exists $t\in[r]$ such that $\prod_{i=2}^k(x_{i,t}-y_{i,t}) \neq 0$, then the inner expectation over $x_{1,t}\in\mathbb{F}_q$ vanishes by character orthogonality. Therefore the inner expectation can be nonzero only if $\prod_{i=2}^k(x_{i,t}-y_{i,t}) = 0$ for every $t\in[r]$. Hence

$$|\Gamma_\alpha(S)|^{2^{k-1}} \le \Pr\left[\forall t\in[r],\ \prod_{i=2}^k(x_{i,t}-y_{i,t}) = 0\right].$$

For a fixed coordinate t, the event $\prod_{i=2}^k(x_{i,t}-y_{i,t})=0$ means that $x_{i,t}=y_{i,t}$ for at least one $i\in\{2,\dots,k\}$. By the union bound,

$$\Pr\left[\prod_{i=2}^k(x_{i,t}-y_{i,t})=0\right] \le \frac{k-1}{q} \le \frac{k}{q}.$$

The coordinates $t=1,\dots,r$ are independent, so $|\Gamma_\alpha(S)|^{2^{k-1}} \le \left(\frac{k}{q}\right)^r$. Therefore $|\Gamma_\alpha(S)| \le (k/q)^{r/2^{k-1}} = \gamma_k(q,r)$. Since S and α are arbitrary, taking the supremum proves the lemma. ◀

Proof of Lemma 18. Fix $v \in \mathbb{F}_q$ and $S \in \mathrm{CI}(X)$. Let $\mathbf{X} \sim \mathrm{Uni}_X$, $\mathbf{V} := G(\mathbf{X})$ and $p_v := \Pr[\mathbf{V} = v]$. Because $X \in \mathrm{CI}(X)$, the definition of $\mathrm{FCorr}(G)$ gives $\left|\mathbb{E}[\chi(\alpha V)]\right| \le \gamma$ for every $\alpha \in \mathbb{F}_q^\times$.

By character orthogonality, $\mathbf{1}[V = v] = \frac{1}{q}\sum_{\alpha\in\mathbb{F}_q} \chi\big(\alpha(V - v)\big)$. Taking expectations, we obtain $p_v = \frac{1}{q} + \frac{1}{q}\sum_{\alpha\in\mathbb{F}_q^\times} \chi(-\alpha v)\,\mathbb{E}[\chi(\alpha V)]$. Therefore

$$\left|p_v - \frac{1}{q}\right| \le \frac{1}{q}\sum_{\alpha\in\mathbb{F}_q^\times} \left|\mathbb{E}[\chi(\alpha V)]\right| \le \frac{q-1}{q}\gamma \le \gamma,$$

and $p_v \ge \frac{1}{q} - \gamma > 0$. Next, we have

$$\Pr[\mathbf{X} \in S, V = v] = \mathbb{E}\big[\mathbf{1}[\mathbf{X} \in S]\,\mathbf{1}[V = v]\big] = \frac{\Pr[\mathbf{X} \in S]}{q} + \frac{1}{q}\sum_{\alpha\in\mathbb{F}_q^\times} \chi(-\alpha v)\mathbb{E}\big[\mathbf{1}[\mathbf{X} \in S]\,\chi(\alpha V)\big].$$

Also, let $a := \Pr[\mathbf{X} \in S]$,

$$\Pr[\mathbf{X} \in S] \cdot p_v = \frac{\Pr[\mathbf{X} \in S]}{q} + \frac{1}{q}\sum_{\alpha\in\mathbb{F}_q^\times} \chi(-\alpha v)\,a\,\mathbb{E}[\chi(\alpha V)].$$

Subtracting the last two displays gives

$$\Pr[\mathbf{X} \in S, V = v] - \Pr[\mathbf{X} \in S] \cdot p_v = \frac{1}{q}\sum_{\alpha\in\mathbb{F}_q^\times} \chi(-\alpha v)\Big(\mathbb{E}\big[\mathbf{1}[\mathbf{X} \in S]\,\chi(\alpha V)\big] - a\,\mathbb{E}[\chi(\alpha V)]\Big).$$

Hence

$$\left|\Pr[\mathbf{X} \in S, V = v] - \Pr[\mathbf{X} \in S] \cdot p_v\right| \le \frac{1}{q}\sum_{\alpha\in\mathbb{F}_q^\times} \left|\mathbb{E}\big[\mathbf{1}[\mathbf{X} \in S]\,\chi(\alpha V)\big] - a\,\mathbb{E}[\chi(\alpha V)]\right|.$$

For each nonzero α, the first term has magnitude at most γ by the definition of $\mathrm{FCorr}(G)$, and the second term has magnitude at most $a\gamma \le \gamma$. Therefore every summand is at most 2γ, so

$$\left|\Pr[\mathbf{X} \in S, V = v] - \Pr[\mathbf{X} \in S] \cdot p_v\right| \le \frac{q-1}{q} \cdot 2\gamma \le 2\gamma.$$

Now divide by p_v:

$$\begin{aligned}\left|\Pr_{\mathbf{X}\sim\mathrm{Uni}_{X_v}}[\mathbf{X} \in S] - \Pr_{\mathbf{X}\sim\mathrm{Uni}_X}[\mathbf{X} \in S]\right| &= \left|\Pr[\mathbf{X} \in S \mid V = v] - \Pr[\mathbf{X} \in S]\right| \\ &= \frac{\left|\Pr[\mathbf{X} \in S, V = v] - \Pr[\mathbf{X} \in S] \cdot p_v\right|}{p_v} \\ &\le \frac{2q\gamma}{1 - q\gamma}.\end{aligned}$$

Notice that when $q\gamma \le \frac{1}{2}$, $\frac{2q\gamma}{1-q\gamma} \le 4q\gamma$. Then taking the supremum over $v \in \mathbb{F}_q$ and $S \in \mathrm{CI}(X)$ proves the claim. ◀

References

1 László Babai, Noam Nisan, and Mário Szegedy. Multiparty protocols and Logspace-hard pseudorandom sequences. In *Proceedings of the Twenty-First Annual ACM Symposium on Theory of Computing (STOC 1989)*, pages 1–11, New York, NY, USA, 1989. Association for Computing Machinery. doi:10.1145/73007.73008.

2 Ziv Bar-Yossef, Thathachar S Jayram, and Iordanis Kerenidis. Exponential separation of quantum and classical one-way communication complexity. In *Proceedings of the thirty-sixth annual ACM symposium on Theory of computing*, pages 128–137, 2004.

3 Joshua Brody, Stefan Dziembowski, Sebastian Faust, and Krzysztof Pietrzak. Position-based cryptography and multiparty communication complexity. In *Theory of Cryptography – 15th International Conference, TCC 2017, Baltimore, MD, USA, November 12–15, 2017, Proceedings, Part I*, volume 10677 of *Lecture Notes in Computer Science*, pages 56–81. Springer International Publishing, 2017. doi:10.1007/978-3-319-70500-2_3.

4 Amit Chakrabarti. Lower bounds for multi-player pointer jumping. In *22nd Annual IEEE Conference on Computational Complexity (CCC 2007)*, pages 33–45. IEEE Computer Society, 2007. doi:10.1109/CCC.2007.14.

5 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.

6 Carsten Damm, Stasys Jukna, and Jiří Sgall. Some bounds on multiparty communication complexity of pointer jumping. *Computational Complexity*, 7(2):109–127, 1998. doi:10.1007/PL00001595.

7 Anat Ganor and Ran Raz. Space pseudorandom generators by communication complexity lower bounds. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM 2014)*, volume 28 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 692–703, Dagstuhl, Germany, 2014. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.APPROX-RANDOM.2014.692.

8 Dmitry Gavinsky, Julia Kempe, Iordanis Kerenidis, Ran Raz, and Ronald De Wolf. Exponential separations for one-way quantum communication complexity, with applications to cryptography. In *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, pages 516–525, 2007. doi:10.1145/1250790.1250866.

9 Mika Göös, Pritish Kamath, Toniann Pitassi, and Thomas Watson. Query-to-communication lifting for P^{NP}. In *32nd Computational Complexity Conference (CCC 2017)*, volume 79 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 12:1–12:16, Dagstuhl, Germany, 2017. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.CCC.2017.12.

10 Mika Göös, Shachar Lovett, Raghu Meka, Thomas Watson, and David Zuckerman. Rectangles are nonnegative juntas. *SIAM Journal on Computing*, 45(5):1835–1869, 2016. Conference version in STOC 2015. doi:10.1137/15M103145X.

11 Mika Göös, Toniann Pitassi, and Thomas Watson. Query-to-communication lifting for BPP. In *Proceedings of the 58th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2017)*, pages 132–143. IEEE Computer Society, 2017. doi:10.1109/FOCS.2017.21.

12 Johan Håstad and Mikael Goldmann. On the power of small-depth threshold circuits. In *Proceedings of the 31st Annual Symposium on Foundations of Computer Science (FOCS 1990)*, pages 610–618. IEEE Computer Society, 1990. doi:10.1109/FSCS.1990.89582.

13 John Kallaugher, Andrew McGregor, Eric Price, and Sofya Vorotnikova. The complexity of counting cycles in the adjacency list streaming model. In *Proceedings of the 38th ACM SIGMOD-SIGACT-SIGAI Symposium on Principles of Database Systems (PODS 2019)*, pages 119–133, New York, NY, USA, 2019. Association for Computing Machinery. doi:10.1145/3294052.3319706.

14 Eyal Kushilevitz and Noam Nisan. *Communication Complexity*. Cambridge University Press, 1997. doi:10.1017/CBO9780511574948.

15 Shachar Lovett, Raghu Meka, Ian Mertz, Toniann Pitassi, and Jiapeng Zhang. Lifting with sunflowers. In *13th Innovations in Theoretical Computer Science Conference (ITCS 2022)*, volume 215 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 104:1–104:24, Dagstuhl, Germany, 2022. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.ITCS.2022.104.

16 Ashwin Nayak. Optimal lower bounds for quantum automata and random access codes. In *Proceedings of the 40th Annual Symposium on Foundations of Computer Science (FOCS 1999)*, pages 369–377. IEEE Computer Society, 1999. doi:10.1109/SFFCS.1999.814608.

17 Pavel Pudlák, Vojtěch Rödl, and Jiří Sgall. Boolean circuits, tensor ranks, and communication complexity. *SIAM Journal on Computing*, 26(3):605–633, 1997. doi:10.1137/S0097539794264809.

18 Ran Raz and Pierre McKenzie. Separation of the monotone NC hierarchy. *Combinatorica*, 19(3):403–435, 1999. doi:10.1007/s004930050062.

19 Alexander A. Sherstov. The pattern matrix method. *SIAM Journal on Computing*, 40(6):1969–2000, 2011. doi:10.1137/080733644.

20 Emanuele Viola and Avi Wigderson. One-way multi-party communication lower bound for pointer jumping with applications. In *Proceedings of the 48th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2007)*, pages 427–437. IEEE Computer Society, 2007. doi:10.1109/FOCS.2007.4389513.

21 Guangxu Yang and Jiapeng Zhang. Deterministic lifting theorems for one-way Number-on-Forehead communication, 2025. doi:10.48550/arXiv.2506.12420.

22 Guangxu Yang and Jiapeng Zhang. Exponential separation of quantum and classical one-way Numbers-on-Forehead communication, 2026. doi:10.48550/arXiv.2603.22795.