# Randomized and Quantum Lifting for One-Way Conservative NOF Model

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

**Pei Wu**
The Pennsylvania State University, State College, 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 type of restricted view has appeared in the NOF literature under the term conservative. 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 cylinder intersections. In the quantum setting, lifting follows when each preimage looks pseudorandom to generalized cylinder intersections. 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, with 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.2026.73

**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 $\mathrm{ACC}^0$ 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, who computes $f(z, v)$. In the lifted NOF problem, there are $k$ nonterminal senders $P_1, \ldots, P_k$ and a terminal player Charlie. Player $P_i$ sees $z$ and $\mathbf{x}_{-i}$ (all gadget inputs except $\mathbf{x}_i$), and messages are sent in the order $P_1 \to \cdots \to P_k \to$ Charlie. 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. For the discussion below, let $\mathbf{x}'$ denote a uniformly random gadget input. 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

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

provided the gadget-induced extra error loss is at most $\delta$. 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. For $v \in \mathcal{V}$, call $G^{-1}(v)$ a *fiber* of $G$. Informally, we show the following:

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 by

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

Our randomized lifting theorem reads

▶ **Theorem 1** (Randomized lifting via GIP (informal Theorem 16)). *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 $F = f \circ \mathrm{GIP}^{(k)}_{q,r}$ where $r \geq 2^k \log_{q/2k}\left(2^{\mathrm{R}^{\to}_{\varepsilon+\delta}(f)} q/\delta\right)$, we have $\mathrm{R}^{\to,\mathrm{cons}}_{\varepsilon}(F) \geq \mathrm{R}^{\to}_{\varepsilon+\delta}(f)$.*

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 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 full one-way NOF communication, Yang and Zhang recently established an exponential separation for a *search* problem [22], whereas our separation is for a *decision* problem.

The proof principle is terminal mixing. Fix the outer input $z$, 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 $\Delta_G$ 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 $2^{\mathrm{R}^{\to}_{\varepsilon+\delta}(f)}\Delta_G \leq \delta$. 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 outer input and the public randomness, the transcript lies in $\{0,1\}^{\leq C}$, each transcript cell is a cylinder intersection, and summing over all cells gives total-variation loss $\leq 2^C \Delta_G$. 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

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

For $G = \mathrm{GIP}^{(k)}_{q,r}$, adapting the character-sum estimate of Yang–Zhang [21, Lemma 3.2], one can show $\Delta_G \leq 4q\,(k/q)^{r/2^{k-1}}$. 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 $\delta$ 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 is as follows.

▶ **Theorem 4** (Quantum one-way lifting via GIP (informal)). *Given $k \geq 2$, 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 $r \geq 2^k \log_{q/(k-1)}\left(2^{2\mathrm{Q}^{\rightarrow}_{\varepsilon+\delta}(f)+2} q/\delta\right)$, we have*

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

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 $\sigma_{z,\mathbf{x}}$ denote the final message state on gadget input $\mathbf{x}$, let

$$\sigma_{z,v} := \mathbb{E}_{\mathbf{x}'' \sim \mathrm{Uni}_{X_v}}[\sigma_{z,\mathbf{x}''}], \qquad \sigma_z := \mathbb{E}_{\mathbf{x}' \sim \mathrm{Uni}_X}[\sigma_{z,\mathbf{x}'}].$$

The ordinary one-way simulation has Alice send the unconditional state $\sigma_z$, while Bob uses $v$ to perform Charlie's terminal measurement. The analysis therefore bounds, for the corresponding output-1 POVM element $M^{(1)}_v$,

$$\left|\mathrm{Tr}\left(M^{(1)}_v(\sigma_z - \sigma_{z,v})\right)\right|.$$

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* $\Delta_G^{\Pi}$. 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 $\Delta_G^{\Pi}$ 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*

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

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 $\mathrm{Uni}_A$ 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 $i$th 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

We use the standard bit-protocol convention: after fixing the public coins, the current transcript determines whether communication stops and, if not, who writes the next bit. A player's message is the possibly empty block of consecutive bits assigned to that player by this rule. Thus message lengths may vary, but the end of a message conveys no information beyond the bits written.

▶ **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 $\tau_i$, with $\tau_0$ 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 $\tau_{i-1}$, 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 $\eta$. 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 $i$th 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 $\Delta_G$ 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, an adaptation of the character-sum argument in the proof of Yang–Zhang's Lemma 3.2 [21] bounds this quantity by $\gamma_k(q,r)$. Fourier inversion then converts this correlation bound into a bound on the fiber discrepancy $\Delta_G$.

## 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 $\sigma_{z,\mathbf{x}}$ for the final message state received by the terminal player. We also use the average states

$$\sigma_{z,v} := \mathbb{E}_{\mathbf{x}'' \sim \mathrm{Uni}_{X_v}}[\sigma_{z,\mathbf{x}''}], \qquad \sigma_z := \mathbb{E}_{\mathbf{x}' \sim \mathrm{Uni}_X}[\sigma_{z,\mathbf{x}'}].$$

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 $\sigma_z$ on a $C$-qubit register for each $z \in Z$, and a binary POVM $\mathcal{M}_v = \{M_v^{(0)}, M_v^{(1)}\}$ for each $v \in \mathcal{V}$. Alice sends $\sigma_z$, and Bob applies $\mathcal{M}_v$.*

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 $\eta$. 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 $\eta$. 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 $\Delta_G^{\Pi}$.

## 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 $i$th 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],

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

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 $\mathsf{BHM}_n$ 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],

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

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

In the following section, we give the details of the randomized lifting theorem for the GIP gadget. The quantum lifting theorem and the remaining proofs appear in subsequent sections.

# 4 Randomized lifting

Our randomized lifting theorem works by composing a two-party function $f$ and a $k$-party function $g$ to obtain a $(k+1)$-party function $f \circ g$ as the following definition.

▶ **Definition 15** (lifted function). *Fix integer $k \ge 2$ and prime $q$. Let $N$ be an arbitrary finite set. For any Boolean function $f : \mathbb{F}_q \times \mathbb{F}_q \to \{0,1\}$ and a function $g : N^k \to \mathbb{F}_q$, we define the lifted function $f \circ g$ as*

$$(f \circ g) \colon N^k \times \mathbb{F}_q \to \{0,1\}, \qquad (f \circ g)(\mathbf{x}_1, \dots, \mathbf{x}_k, \mathbf{z}) := f\big(g(\mathbf{x}_1, \dots, \mathbf{x}_k), \mathbf{z}\big).$$

*We call $f$ the outer function and $g$ the gadget function.*

By choosing the generalized inner product function as the gadget function, the randomized lifting theorem transfers the communication lower bound of the outer function to that of the lifted function as follows.

▶ **Theorem 16.** *Let $0 \le \varepsilon \le 1$ and $0 < \delta \le 1 - \varepsilon$ be constants. Let the gadget be $\mathrm{GIP}^k_{q,r} : (\mathbb{F}_q^r)^k \to \mathbb{F}_q$, where $k \ge 2$ and $q$ is the smallest prime in $[4k, 8k]$ [1]. If $r \ge 2^k \log\left(q^2/\delta\right)$, for any outer function $f : \mathbb{F}_q \times \mathbb{F}_q \to \{0,1\}$, we have*

$$\mathrm{R}^{\to,\mathrm{cons}}_{\varepsilon}(f \circ \mathrm{GIP}^k_{q,r}) \ge \mathrm{R}^{\to}_{\varepsilon+\delta}(f).$$

▶ Remark 17. It suffices to take $r = \lceil 2^k \log(q^2/\delta) \rceil$. Thus the input length of the gadget function is

$$|\mathbf{x}_i| = \lceil r \log q \rceil = \Theta\left(2^k \log^2 q\right), \forall i \in [k].$$

Theorem 16 builds on the following key lifting lemma, which shows a $(k+1)$-party conservative one-way protocol for the lifed function $f \circ g$ can be simulated by a two-party one-way protocol for the outer function $f$. The additive loss in the error is controlled by the fiber discrepancy of the gadget function.

▶ **Lemma 18** (Key lifting lemma)**.** *Let $g : N^k \to \mathbb{F}_q$ be a surjective gadget function with fiber discrepancy $\Delta_g$. For any outer function $f : \mathbb{F}_q \times \mathbb{F}_q \to \{0,1\}$, if $f \circ g$ has a $(k+1)$-party conservative one-way protocol with cost $\le C$ and error $\le \varepsilon$, then $f$ has a two-party one-way protocol with cost $\le C$ and error $\le \varepsilon + 2^C \cdot \Delta_g$.*

The proof of Lemma 18 is postponed to Section 4.1. To control the fiber discrepancy $\Delta_g$, Lemma 19 bounds fiber discrepancy in terms of Fourier correlation, and Lemma 20 bounds the Fourier correlation of $\mathrm{GIP}^k_{q,r}$.

▶ **Lemma 19.** *Given a surjective gadget function $g : N^k \to \mathbb{F}_q$, if $\mathrm{FCorr}(g) \le \gamma$ and $q\gamma < 1/2$, the fiber discrepancy $\Delta_g \le 4q\gamma$.*

The proof of Lemma 19 is postponed to Section 4.2.

▶ **Lemma 20.** *The Fourier correlation of $\mathrm{GIP}^k_{q,r}$ satisfies $\mathrm{FCorr}(\mathrm{GIP}^k_{q,r}) \le (k/q)^{r/2^{k-1}}$.*

The proof of Lemma 20 is adapted from Yang–Zhang's Lemma 3.2 [21]; we include the details in the appendix for completeness.

With these three lemmas in hand, we can prove Theorem 16 now.

**Proof of Theorem 16.** For any public-coin conservative one-way protocol $\Pi$ for $f \circ \mathrm{GIP}^k_{q,r}$, which has cost $C$ and worst-case error $\varepsilon$, we prove that $C \ge \mathrm{R}^{\to}_{\varepsilon+\delta}(f)$ as follows.

Let $G := \mathrm{GIP}^k_{q,r}$. For contradiction, suppose $C < \mathrm{R}^{\to}_{\varepsilon+\delta}(f)$. By Lemma 18, there exists a public-coin two-party one-way protocol $\Pi'$ for $f$ with cost $C$ and worst-case error $\varepsilon + 2^C \Delta_G$.

Let $\gamma_k(q,r) := (k/q)^{r/2^{k-1}}$. We have $q \cdot \gamma_k(q,r) \le \frac{1}{q} < 1/2$. Since $G$ is surjective, Lemma 20 and Lemma 19 imply that $\Delta_G \le 4q\,\gamma_k(q,r)$. Therefore the error of $\Pi'$ satisfies

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

The last inequality follows from $r \ge 2^k \log(q^2/\delta)$. Indeed, since $q \ge 4k$,

$$\gamma_k(q,r) \le \left(\frac{1}{4}\right)^{2\log(q^2/\delta)} = \left(\frac{\delta}{q^2}\right)^4.$$

Moreover, $\mathrm{R}^{\to}_{\varepsilon+\delta}(f) \le \lceil \log q \rceil \le \log q + 1$, and hence

$$2^{\mathrm{R}^{\to}_{\varepsilon+\delta}(f)+2} q\,\gamma_k(q,r) \le 8q^2 \left(\frac{\delta}{q^2}\right)^4 \le \delta.$$

So $\Pi'$ has worst-case error $\varepsilon + \delta$ and cost $C < \mathrm{R}^{\to}_{\varepsilon+\delta}(f)$, which is impossible. ◀

[1] By the Bertrand–Chebyshev theorem, there exists a prime in $[4k, 8k]$.

## 4.1 Proof of Key Lifting Lemma

In this section, we complete the proof of Lemma 18. At first, we need the following technical lemma which shows all transcript cells are cylinder intersections.

For each one-way conservative NOF protocol on $f \circ g$, the transcript $\tau$ is determined by the inputs $(\mathbf{x}_1, \mathbf{x}_2, \cdots, \mathbf{x}_k) \in N^k$, $\mathbf{z} \in \mathbb{F}_q$ and the public randomness $\rho$. After fixing $\mathbf{z}$ and $\rho$, the transcript map $T_{\mathbf{z},\rho} : N^k \to \{0,1\}^{\leq C}$ is a deterministic function of the inputs $(\mathbf{x}_1, \mathbf{x}_2, \cdots, \mathbf{x}_k)$, where $C$ is the cost of the protocol.

▶ **Lemma 21.** *For each one-way conservative NOF protocol of cost $C$ on $f \circ g : \mathbb{F}_q \times N^k \to \{0,1\}$, given input $\mathbf{z} \in \mathbb{F}_q$ and public randomness $\rho$, let $T_{\mathbf{z},\rho} \colon N^k \to \{0,1\}^{\leq C}$ be the transcript map. Then for every transcript $\tau$, $T^{-1}_{\mathbf{z},\rho}(\tau)$ is a cylinder intersection of $N^k$.*

**Proof.** Fix a transcript $\tau$. If $T^{-1}_{\mathbf{z},\rho}(\tau)$ is empty, the claim is immediate. Otherwise, by the bit-protocol convention, $\rho$ and $\tau$ uniquely determine the messages $m_1, \ldots, m_k$ and the intermediate transcripts $\tau_0, \tau_1, \ldots, \tau_k$, where $\tau_0 = \emptyset$, $\tau_k = \tau$, and $\tau_i = \tau_{i-1} m_i$. For each $i \in [k]$, let $M_i$ be the message map of player $P_i$ in the protocol. For each $i \in [k]$, define

$$C_i := \big\{\mathbf{x} \in N^k : M_i(\mathbf{z}, \mathbf{x}_{-i}, \rho, \tau_{i-1}) = m_i\big\}.$$

So $C_i$ is an $i$-cylinder.

We prove $T^{-1}_{\mathbf{z},\rho}(\tau) = C_1 \cap \cdots \cap C_k$ as follows. On the one hand, if $\mathbf{x} \in T^{-1}_{\mathbf{z},\rho}(\tau)$, then the protocol is deterministic once the input $(\mathbf{z}, \mathbf{x})$ and randomness $\rho$ are fixed, and it produces the messages $m_1, \ldots, m_k$ and the transcripts $\tau_1, \ldots, \tau_k$. Therefore $\mathbf{x} \in C_i$ for each $i \in [k]$.

On the other hand, if $\mathbf{x} \in C_1 \cap \cdots \cap C_k$, we prove by induction that the protocol on input $(\mathbf{z}, \mathbf{x})$ and randomness $\rho$ produces $m_1, \ldots, m_i$ and $\tau_1, \ldots, \tau_i$ 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 $\tau_{i-1}$. Because $\mathbf{x} \in C_i$, the next message must be $m_i$ by definition. Hence the next transcript is $\tau_i = \tau_{i-1} m_i$. This completes the induction. Taking $i = k$ gives $\tau_k = \tau$, so $\mathbf{x} \in T^{-1}_{\mathbf{z},\rho}(\tau)$. ◀

Now we prove the key lifting lemma.

**Proof of Lemma 18.** Fix a conservative one-way NOF protocol $\Pi$ on $f \circ g : N^k \times \mathbb{F}_q \to \{0,1\}$ with cost $C$ and error $\varepsilon$. We construct a two-party one-way protocol $\Pi'$ on $f : \mathbb{F}_q \times \mathbb{F}_q \to \{0,1\}$ by simulating $\Pi$; it has cost $C$ and error $\varepsilon + 2^C \Delta_g$. Let $\mathcal{T} := \{0,1\}^{\leq C}$.

Let $\rho$ denote the public randomness. All probabilities and expectations over $\rho$ below are taken with respect to its distribution. Let $\mathcal{R}$ be the space of public randomness. Given input $\mathbf{z} \in \mathbb{F}_q$ and $\rho \in \mathcal{R}$, let $T_{\mathbf{z},\rho} \colon N^k \to \mathcal{T}$ be the transcript map of $\Pi$.

**Protocol:** In the two-party one-way model, Alice receives $\mathbf{z} \in \mathbb{F}_q$ and Bob receives $\mathbf{v} \in \mathbb{F}_q$. Alice sends a message to Bob, who outputs $f(\mathbf{v}, \mathbf{z})$. First, sample $\rho$ according to the distribution of public randomness of $\Pi$. Using additional independent public randomness, Alice samples $\mathbf{x}' \sim \mathrm{Uni}[N^k]$ and computes the transcript $\tau := T_{\mathbf{z},\rho}(\mathbf{x}')$ according to $\Pi$. Then Alice sends $\tau$ to Bob. On input $\mathbf{v}$, Bob outputs $\mathsf{DEC}(\mathbf{v}, \rho, \tau)$ using the decoder of $\Pi$.

**Analysis:** It is clear that the cost of $\Pi'$ is $|\tau| \leq C$. We bound the error probability of $\Pi'$ as follows. Given $(\mathbf{z}, \mathbf{v}) \in \mathbb{F}_q \times \mathbb{F}_q$, let $\mu_{\mathbf{z},\mathbf{v}}$ be the distribution of $(\rho, T_{\mathbf{z},\rho}(\mathbf{x}''))$ for $\mathbf{x}'' \sim \mathrm{Uni}[N^k|_{\mathbf{v}}]$, and let $\nu_{\mathbf{z}}$ be the distribution of $(\rho, T_{\mathbf{z},\rho}(\mathbf{x}'))$ for $\mathbf{x}' \sim \mathrm{Uni}[N^k]$. In both cases, the gadget input is independent of $\rho$. Define the error event

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

**Step 1:** We show that $\mu_{\mathbf{z},\mathbf{v}}(E_{\mathbf{z},\mathbf{v}})$ equals the error of $\Pi$ averaged over the fiber set $N^k|_{\mathbf{v}}$. Recall that $N^k|_{\mathbf{v}} = \{\mathbf{x} \in N^k : g(\mathbf{x}) = \mathbf{v}\}$. For any $\mathbf{x} \in N^k|_{\mathbf{v}}$, $(f \circ g)(\mathbf{x}, \mathbf{z}) = f(\mathbf{v}, \mathbf{z})$.

Given $(\mathbf{x}, \rho) \in N^k|_{\mathbf{v}} \times \mathcal{R}$, the protocol $\Pi$ produces the transcript $T_{\mathbf{z},\rho}(\mathbf{x})$ and outputs $\mathsf{DEC}\big(\mathbf{v}, \rho, T_{\mathbf{z},\rho}(\mathbf{x})\big)$. Therefore $\Pi$ errs on $(\mathbf{x}, \mathbf{z}, \rho)$ if and only if $(\rho, T_{\mathbf{z},\rho}(\mathbf{x})) \in E_{\mathbf{z},\mathbf{v}}$.

Because $\Pi$ has worst-case error $\varepsilon$, for any $(\mathbf{x}, \mathbf{z}) \in N^k|_{\mathbf{v}} \times \mathbb{F}_q$,

$$\Pr_{\rho}[\Pi \text{ errs on } (\mathbf{x}, \mathbf{z})] \le \varepsilon.$$

Thus by averaging over $\mathbf{x}'' \sim \mathrm{Uni}[N^k|_{\mathbf{v}}]$, we have

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

**Step 2:** Under $\Pi'$, $\nu_{\mathbf{z}}(E_{\mathbf{z},\mathbf{v}})$ equals the error probability on input $(\mathbf{z}, \mathbf{v})$. On public randomness $(\rho, \mathbf{x}')$, Alice sends $T_{\mathbf{z},\rho}(\mathbf{x}')$ to Bob, and Bob outputs $\mathsf{DEC}(\mathbf{v}, \rho, T_{\mathbf{z},\rho}(\mathbf{x}'))$. Hence $\Pi'$ errs if and only if $(\rho, T_{\mathbf{z},\rho}(\mathbf{x}')) \in E_{\mathbf{z},\mathbf{v}}$. Therefore $\nu_{\mathbf{z}}(E_{\mathbf{z},\mathbf{v}}) = \Pr_{\rho,\mathbf{x}'}\big[\Pi' \text{ errs on } (\mathbf{z}, \mathbf{v})\big]$.

**Step 3:** We now bound the total variation distance between $\mu_{\mathbf{z},\mathbf{v}}$ and $\nu_{\mathbf{z}}$. By Lemma 21, $T^{-1}_{\mathbf{z},\rho}(\tau)$ is a cylinder intersection in $N^k$. Thus by the definition of fiber discrepancy (Definition 9), we have for any $(\rho, \tau) \in \mathcal{R} \times \mathcal{T}$,

$$\left| \Pr_{\mathbf{x}'' \sim \mathrm{Uni}[N^k|_{\mathbf{v}}]}\big[T_{\mathbf{z},\rho}(\mathbf{x}'') = \tau\big] - \Pr_{\mathbf{x}' \sim \mathrm{Uni}[N^k]}\big[T_{\mathbf{z},\rho}(\mathbf{x}') = \tau\big] \right| \le \Delta_g.$$

Therefore the total variation distance between $\mu_{\mathbf{z},\mathbf{v}}$ and $\nu_{\mathbf{z}}$ satisfies:

$$\begin{aligned}
\mathrm{TV}(\mu_{\mathbf{z},\mathbf{v}}, \nu_{\mathbf{z}}) &= \frac{1}{2}\mathbb{E}_{\rho}\left[\sum_{\tau \in \mathcal{T}} \left| \Pr_{\mathbf{x}'' \sim \mathrm{Uni}[N^k|_{\mathbf{v}}]}\big[T_{\mathbf{z},\rho}(\mathbf{x}'') = \tau\big] - \Pr_{\mathbf{x}' \sim \mathrm{Uni}[N^k]}\big[T_{\mathbf{z},\rho}(\mathbf{x}') = \tau\big] \right| \right] \\
&\le \frac{1}{2}|\mathcal{T}|\Delta_g \\
&\le 2^C \Delta_g.
\end{aligned}$$

Consequently,

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

It holds for arbitrary $(\mathbf{z}, \mathbf{v}) \in \mathbb{F}_q \times \mathbb{F}_q$, so $\Pi'$ has worst-case error at most $\varepsilon + 2^C \cdot \Delta_g$. ◀

## 4.2 From Fourier correlation to fiber discrepancy

In this section, we prove Lemma 19, which relates the fiber discrepancy to the Fourier correlation.

**Proof of Lemma 19.** Fix $\mathbf{v} \in \mathbb{F}_q$ and a cylinder intersection $S \in \mathrm{CI}[N^k]$. Let $\mathbf{x}' \sim \mathrm{Uni}[N^k]$, set $\mathbf{v}' := g(\mathbf{x}')$, and let

$$p_{\mathbf{v}} := \Pr[\mathbf{v}' = \mathbf{v}].$$

By taking the cylinder intersection $N^k \in \mathrm{CI}[N^k]$ and the definition of $\mathrm{FCorr}(g)$, we have

$$\big|\mathbb{E}[\chi(\alpha \mathbf{v}')]\big| \le \gamma$$

for every $\alpha \in \mathbb{F}_q^{\times}$.

By character orthogonality,

$$\mathbf{1}[\mathbf{v}' = \mathbf{v}] = \frac{1}{q} \sum_{\alpha \in \mathbb{F}_q} \chi\big(\alpha(\mathbf{v}' - \mathbf{v})\big).$$

After taking expectations on both sides, we obtain

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

Therefore

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

and $p_{\mathbf{v}} \ge \frac{1}{q} - \gamma > 0$.

Again by character orthogonality,

$$\begin{aligned} \Pr[\mathbf{x}' \in S, \mathbf{v}' = \mathbf{v}] &= \mathbb{E}\big[\mathbf{1}[\mathbf{x}' \in S]\, \mathbf{1}[\mathbf{v}' = \mathbf{v}]\big] \\ &= \frac{\Pr[\mathbf{x}' \in S]}{q} + \frac{1}{q} \sum_{\alpha \in \mathbb{F}_q^\times} \chi(-\alpha \mathbf{v}) \mathbb{E}\big[\mathbf{1}[\mathbf{x}' \in S]\, \chi(\alpha \mathbf{v}')\big]. \end{aligned}$$

Multiplying the expression for $p_{\mathbf{v}}$ above by $\Pr[\mathbf{x}' \in S]$ gives

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

Subtracting the preceding two displays gives

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

Since $|\chi(-\alpha \mathbf{v})| = 1$ for every $\alpha \in \mathbb{F}_q^\times$, the triangle inequality gives

$$\Big| \Pr[\mathbf{x}' \in S, \mathbf{v}' = \mathbf{v}] - \Pr[\mathbf{x}' \in S] \cdot p_{\mathbf{v}} \Big| \le \frac{1}{q} \sum_{\alpha \in \mathbb{F}_q^\times} \Big| \mathbb{E}\big[\mathbf{1}[\mathbf{x}' \in S]\, \chi(\alpha \mathbf{v}')\big] - \Pr[\mathbf{x}' \in S]\, \mathbb{E}[\chi(\alpha \mathbf{v}')] \Big|.$$

For every $\alpha \in \mathbb{F}_q^\times$, applying the definition of $\mathrm{FCorr}(g)$ to the fixed cylinder intersection $S$ gives

$$\big| \mathbb{E}\big[\mathbf{1}[\mathbf{x}' \in S]\, \chi(\alpha \mathbf{v}')\big] \big| \le \gamma.$$

Moreover, since $0 \le \Pr[\mathbf{x}' \in S] \le 1$, the estimate $\big|\mathbb{E}[\chi(\alpha \mathbf{v}')]\big| \le \gamma$ established above gives

$$|\Pr[\mathbf{x}' \in S]\, \mathbb{E}[\chi(\alpha \mathbf{v}')]| \le \Pr[\mathbf{x}' \in S] \gamma \le \gamma.$$

Thus, by the triangle inequality, for every $\alpha \in \mathbb{F}_q^\times$,

$$\big| \mathbb{E}\big[\mathbf{1}[\mathbf{x}' \in S]\, \chi(\alpha \mathbf{v}')\big] - \Pr[\mathbf{x}' \in S]\, \mathbb{E}[\chi(\alpha \mathbf{v}')] \big| \le 2\gamma.$$

Since $\mathbb{F}_q^\times$ contains $q-1$ elements, substituting this bound into the preceding display gives

$$\Big| \Pr[\mathbf{x}' \in S, \mathbf{v}' = \mathbf{v}] - \Pr[\mathbf{x}' \in S] \cdot p_{\mathbf{v}} \Big| \le \frac{q-1}{q} \cdot 2\gamma \le 2\gamma.$$

Hence

$$\begin{aligned} \left| \Pr_{\mathbf{x}'' \sim \mathrm{Uni}[N^k|_{\mathbf{v}}]}[\mathbf{x}'' \in S] - \Pr_{\mathbf{x}' \sim \mathrm{Uni}[N^k]}[\mathbf{x}' \in S] \right| &= |\Pr[\mathbf{x}' \in S \mid \mathbf{v}' = \mathbf{v}] - \Pr[\mathbf{x}' \in S]| \\ &= \frac{\Big| \Pr[\mathbf{x}' \in S, \mathbf{v}' = \mathbf{v}] - \Pr[\mathbf{x}' \in S] \cdot p_{\mathbf{v}} \Big|}{p_{\mathbf{v}}} \\ &\le \frac{2q\gamma}{1 - q\gamma}. \end{aligned}$$

Since $q\gamma < \frac{1}{2}$, we have $\frac{2q\gamma}{1-q\gamma} \le 4q\gamma$. Taking the supremum over $\mathbf{v} \in \mathbb{F}_q$ and $S \in \mathrm{CI}[N^k]$ proves the claim. ◀

## 5 Quantum lifting

In this section, we prove our quantum lifting theorem as follows.

▶ **Theorem 22.** *Let $0 \le \varepsilon \le 1$ and $0 < \delta \le 1 - \varepsilon$ be constants. Let the gadget be $\mathrm{GIP}^k_{q,r} : (\mathbb{F}_q^r)^k \to \mathbb{F}_q$, where $k \ge 2$ and $q$ is the smallest prime in $[4k, 8k]$. If $r \ge 2^k \log(q^2/\delta)$, for any outer function $f : \mathbb{F}_q \times \mathbb{F}_q \to \{0,1\}$, we have*

$$\mathrm{Q}^{\to,\mathrm{cons}}_{\varepsilon}(f \circ \mathrm{GIP}^k_{q,r}) \ge \mathrm{Q}^{\to}_{\varepsilon+\delta}(f).$$

▶ Remark 23. It suffices to take $r = \lceil 2^k \log(q^2/\delta) \rceil$. Thus the input length of the gadget function is

$$|\mathbf{x}_i| = \lceil r \log q \rceil = \Theta\left(2^k \log^2 q\right), \forall i \in [k].$$

Before proving Theorem 22, we need the following key lifting lemma that translates $(k+1)$-party quantum one-way conservative NOF protocol into two-party quantum one-way protocol, and charges the extra error by the fiber discrepancy of gadget function.

▶ **Lemma 24** (Key lifting lemma)**.** *Let $g : N^k \to \mathbb{F}_q$ be a surjective gadget function with fiber discrepancy $\Delta^{\Pi}_g$. For any outer function $f : \mathbb{F}_q \times \mathbb{F}_q \to \{0,1\}$, if $f \circ g$ has a $(k+1)$-party quantum one-way conservative protocol with message lengths $c_1, \ldots, c_k$ and error $\le \varepsilon$, $f$ has a two-party quantum one-way protocol with cost $\le c_k$ and error $\le \varepsilon + 4^{c_1+\cdots+c_{k-1}} \cdot \Delta^{\Pi}_g$.*

The main idea behind Lemma 24 is to decompose the terminal acceptance probability into bounded product tests, which can be controlled by $\Delta^{\Pi}_g$. The proof is deferred to Section 5.1.

It remains to bound the fiber discrepancy $\Delta^{\Pi}_g$. The next two lemmas do so by relating it to product Fourier correlation and then bounding this correlation on $\mathrm{GIP}^k_{q,r}$.

▶ **Lemma 25.** *Given a surjective gadget function $g : N^k \to \mathbb{F}_q$, if the product Fourier correlation $\mathrm{PCorr}(g) \le \gamma$ and $q\gamma < 1/2$, the fiber discrepancy satisfies $\Delta^{\Pi}_g \le 4q\gamma$.*

▶ **Lemma 26.** *The product Fourier correlation of $\mathrm{GIP}^k_{q,r}$ satisfies $\mathrm{PCorr}(\mathrm{GIP}^k_{q,r}) \le (k/q)^{r/2^{k-1}}$.*

Lemmas 25 and 26 are analogous to Lemmas 19 and 20 in the randomized lifting argument. Fourier inversion is identical, while the GIP estimate replaces indicator tests by bounded product tests. The proofs are deferred to the appendix.

**Proof of Theorem 22.** Let $G := \mathrm{GIP}^k_{q,r}$. Consider any one-way conservative quantum protocol $\Pi$ for $f \circ G$ with cost $C$ and worst-case error at most $\varepsilon$. We prove that $C \ge \mathrm{Q}^{\to}_{\varepsilon+\delta}(f)$.

Suppose, for contradiction, that $C < \mathrm{Q}^{\to}_{\varepsilon+\delta}(f)$. Let $c_1, \ldots, c_k$ be the message lengths of $\Pi$ and $\sum_{i=1}^k c_i = C$. Let $\gamma_k(q,r) := (k/q)^{r/2^{k-1}}$. Since $q \ge 4k$ and $r \ge 2^k \log(q^2/\delta)$, we have $q\gamma_k(q,r) \le 1/q < 1/2$. Because $\mathrm{GIP}^k_{q,r}$ is surjective, by Lemma 25 and Lemma 26, we have $\Delta^{\Pi}_G \le 4q\gamma_k(q,r)$.

By Lemma 24, $\Pi$ yields a two-party one-way quantum protocol $\Pi'$ for $f$ with cost at most $c_k$ and error at most

$$\varepsilon + 4^{c_1+\cdots+c_{k-1}}\Delta^{\Pi}_G \le \varepsilon + 4^{c_1+\cdots+c_{k-1}} \cdot 4q\gamma_k(q,r) < \varepsilon + 2^{2\mathrm{Q}^{\to}_{\varepsilon+\delta}(f)+2} q\gamma_k(q,r) \le \varepsilon + \delta.$$

The last inequality follows from $r \ge 2^k \log(q^2/\delta)$ and $q \ge 4k$, which give

$$\gamma_k(q,r) \le \left(\frac{1}{4}\right)^{2\log(q^2/\delta)} = \left(\frac{\delta}{q^2}\right)^4.$$

Since $\mathrm{Q}^{\rightarrow}_{\varepsilon+\delta}(f) \le \lceil \log q \rceil$, we have

$$2^{2\mathrm{Q}^{\rightarrow}_{\varepsilon+\delta}(f)+2} q\gamma_k(q,r) \le 16q^3 \left(\frac{\delta}{q^2}\right)^4 \le \delta.$$

Thus $\Pi'$ has cost at most $c_k < \mathrm{Q}^{\rightarrow}_{\varepsilon+\delta}(f)$ and error at most $\varepsilon+\delta$, contradicting the definition of $\mathrm{Q}^{\rightarrow}_{\varepsilon+\delta}(f)$. ◀

## 5.1 Proof of Key Lifting Lemma

In this section, we prove Lemma 24. At first, we expand each completely positive trace-preserving (CPTP) map in the matrix-unit bases of its input and output spaces, denoted by $E^{\mathrm{in}}_{ab}$ and $E^{\mathrm{out}}_{cd}$, respectively. The following lemma shows that every coefficient in this expansion has magnitude at most 1.

▶ **Lemma 27.** *Let $\Lambda\colon \mathbb{C}^{t\times t} \to \mathbb{C}^{t'\times t'}$ be CPTP. For each $a,b \in [t]$, write $\Lambda(E^{\mathrm{in}}_{ab}) = \sum_{c=1}^{t'}\sum_{d=1}^{t'} \lambda_{cd,ab} E^{\mathrm{out}}_{cd}$. Then $|\lambda_{cd,ab}| \le 1$ for every $a,b \in [t]$ and $c,d \in [t']$.*

Fix a one-way conservative quantum protocol with message lengths $c_1,\dots,c_k$. Let $\mathcal{H}_k$ be the register sent by $P_k$ to Charlie, and let $\sigma_{\mathbf{x},\mathbf{z}}$ be its state on input $(\mathbf{x},\mathbf{z})$. Using Lemma 27, the next lemma expresses the terminal acceptance probability as a sum of bounded product tests, which can be controlled by $\Delta^{\Pi}_g$.

▶ **Lemma 28.** *For every input $\mathbf{z} \in \mathbb{F}_q$ and operator $0 \preceq M \preceq I_{\mathcal{H}_k}$, there exist an integer $L \le 4^{c_1+\cdots+c_{k-1}}$ and functions $\phi_{i,j}\colon N^{k-1} \to \mathbb{C}$ such that for every input $\mathbf{x} \in N^k$,*

$$\mathrm{Tr}(M\sigma_{\mathbf{x},\mathbf{z}}) = \sum_{j=1}^{L}\prod_{i=1}^{k} \phi_{i,j}(\mathbf{x}_{-i}),$$

*where $|\phi_{i,j}| \le 1$ for every $i \in [k], j \in [L]$.*

With these two lemmas in hand, we can finish the proof of Lemma 24. The proof of Lemma 27 and Lemma 28 are put into the rest of this section.

**Proof of Lemma 24.** Fix a one-way conservative quantum protocol $\Pi$ for $f \circ g$ with message lengths $c_1,\dots,c_k$ and worst-case error at most $\varepsilon$. For each $(\mathbf{x},\mathbf{z}) \in N^k \times \mathbb{F}_q$, let $\sigma_{\mathbf{x},\mathbf{z}}$ denote the final message state received by the terminal player Charlie.

Construct a two-party one-way quantum protocol $\Pi'$ for $f$ as follows. On input $\mathbf{z} \in \mathbb{F}_q$, Alice samples $\mathbf{x}' \sim \mathrm{Uni}[N^k]$, simulates $\Pi$ on $(\mathbf{x}',\mathbf{z})$, and sends Bob the final message state $\sigma_{\mathbf{x}',\mathbf{z}}$. Equivalently, Alice sends the mixed state $\mathbb{E}_{\mathbf{x}'\sim\mathrm{Uni}[N^k]}[\sigma_{\mathbf{x}',\mathbf{z}}]$. On input $\mathbf{v} \in \mathbb{F}_q$, Bob applies the same binary measurement that Charlie would use in $\Pi$ on gadget value $\mathbf{v}$. The message sent by Alice is the last message register of $\Pi$, so the cost of $\Pi'$ is at most $c_k$.

Next, we analyze the error probability of $\Pi'$. Fix $(\mathbf{v},\mathbf{z}) \in \mathbb{F}_q \times \mathbb{F}_q$. Let $\mathcal{M}_{\mathbf{v}} = \{M^{(0)}_{\mathbf{v}}, M^{(1)}_{\mathbf{v}}\}$ be Bob's binary POVM. Recall that $N^k|_{\mathbf{v}} := \{\mathbf{x} \in N^k : g(\mathbf{x}) = \mathbf{v}\}$. Define the averaged states

$$\sigma_{\mathbf{v},\mathbf{z}} := \mathbb{E}_{\mathbf{x}''\sim\mathrm{Uni}[N^k|_{\mathbf{v}}]}[\sigma_{\mathbf{x}'',\mathbf{z}}], \qquad \sigma_{\mathbf{z}} := \mathbb{E}_{\mathbf{x}'\sim\mathrm{Uni}[N^k]}[\sigma_{\mathbf{x}',\mathbf{z}}].$$

For every $\mathbf{x} \in N^k|_{\mathbf{v}}$, we have $(f\circ g)(\mathbf{x},\mathbf{z}) = f(\mathbf{v},\mathbf{z})$. By the worst-case error guarantee, the original protocol $\Pi$ has average error at most $\varepsilon$ on the fiber $N^k|_{\mathbf{v}}$. Therefore:

1. if $f(\mathbf{v},\mathbf{z}) = 1$, $\mathrm{Tr}(M^{(1)}_{\mathbf{v}}\sigma_{\mathbf{v},\mathbf{z}}) \ge 1-\varepsilon$;
2. if $f(\mathbf{v},\mathbf{z}) = 0$, $\mathrm{Tr}(M^{(1)}_{\mathbf{v}}\sigma_{\mathbf{v},\mathbf{z}}) \le \varepsilon$.

We now compare the error of $\Pi'$ on $(\mathbf{z}, \mathbf{v})$ with the corresponding quantity for $\sigma_{\mathbf{v},\mathbf{z}}$.

If $f(\mathbf{v}, \mathbf{z}) = 1$, then the error of $\Pi'$ on $(\mathbf{z}, \mathbf{v})$ is $1 - \mathrm{Tr}(M_{\mathbf{v}}^{(1)}\sigma_{\mathbf{z}})$. So we obtain

$$\begin{aligned} 1 - \mathrm{Tr}(M_{\mathbf{v}}^{(1)}\sigma_{\mathbf{z}}) &= 1 - \mathrm{Tr}(M_{\mathbf{v}}^{(1)}\sigma_{\mathbf{v},\mathbf{z}}) + \mathrm{Tr}\big(M_{\mathbf{v}}^{(1)}(\sigma_{\mathbf{v},\mathbf{z}} - \sigma_{\mathbf{z}})\big) \\ &\le \varepsilon + \Big|\mathrm{Tr}\big(M_{\mathbf{v}}^{(1)}(\sigma_{\mathbf{v},\mathbf{z}} - \sigma_{\mathbf{z}})\big)\Big|. \end{aligned}$$

If $f(\mathbf{v}, \mathbf{z}) = 0$, the error of $\Pi'$ on $(\mathbf{z}, \mathbf{v})$ is $\mathrm{Tr}(M_{\mathbf{v}}^{(1)}\sigma_{\mathbf{z}})$, and similarly,

$$\begin{aligned} \mathrm{Tr}(M_{\mathbf{v}}^{(1)}\sigma_{\mathbf{z}}) &= \mathrm{Tr}(M_{\mathbf{v}}^{(1)}\sigma_{\mathbf{v},\mathbf{z}}) + \mathrm{Tr}\big(M_{\mathbf{v}}^{(1)}(\sigma_{\mathbf{z}} - \sigma_{\mathbf{v},\mathbf{z}})\big) \\ &\le \varepsilon + \Big|\mathrm{Tr}\big(M_{\mathbf{v}}^{(1)}(\sigma_{\mathbf{v},\mathbf{z}} - \sigma_{\mathbf{z}})\big)\Big|. \end{aligned}$$

So in both cases, it remains to bound $\Big|\mathrm{Tr}\big(M_{\mathbf{v}}^{(1)}(\sigma_{\mathbf{v},\mathbf{z}} - \sigma_{\mathbf{z}})\big)\Big|$.

By Lemma 28, the map $\mathbf{x} \mapsto \mathrm{Tr}(M_{\mathbf{v}}^{(1)}\sigma_{\mathbf{x},\mathbf{z}})$ admits a decomposition

$$\mathrm{Tr}(M_{\mathbf{v}}^{(1)}\sigma_{\mathbf{x},\mathbf{z}}) = \sum_{j=1}^{L}\prod_{i=1}^{k}\phi_{i,j}(\mathbf{x}_{-i}),$$

where $L \le 4^{c_1+\cdots+c_{k-1}}$ and $|\phi_{i,j}| \le 1$. For every $j \in [L]$, Definition 13 gives

$$\left|\mathbb{E}_{\mathbf{x}''\sim\mathrm{Uni}[N^k|_{\mathbf{v}}]}\left[\prod_{i=1}^{k}\phi_{i,j}(\mathbf{x}''_{-i})\right] - \mathbb{E}_{\mathbf{x}'\sim\mathrm{Uni}[N^k]}\left[\prod_{i=1}^{k}\phi_{i,j}(\mathbf{x}'_{-i})\right]\right| \le \Delta_g^{\Pi}.$$

Therefore, by the definitions of the averaged states and the triangle inequality,

$$\Big|\mathrm{Tr}\big(M_{\mathbf{v}}^{(1)}(\sigma_{\mathbf{v},\mathbf{z}} - \sigma_{\mathbf{z}})\big)\Big| \le L\Delta_g^{\Pi} \le 4^{c_1+\cdots+c_{k-1}}\Delta_g^{\Pi}.$$

Thus the derived two-party protocol $\Pi'$ has worst-case error at most

$$\varepsilon + 4^{c_1+\cdots+c_{k-1}}\Delta_g^{\Pi}.$$

◀

Now we finish the proof of Lemma 27 and Lemma 28.

**Proof of Lemma 27.** Fix $a, b \in [t]$. The output matrix units form a basis, so the expansion is unique and, for every $c, d \in [t']$, $\lambda_{cd,ab} = \big(\Lambda(E_{ab}^{\mathrm{in}})\big)_{cd}$. Choose a Kraus representation $\Lambda(T) = \sum_s K_s T K_s^*$ satisfying $\sum_s K_s^* K_s = I_t$. Since $E_{ab}^{\mathrm{in}} = e_a e_b^*$, we have $\lambda_{cd,ab} = \sum_s (K_s)_{c,a}\overline{(K_s)_{d,b}}$. Thus, by Cauchy–Schwarz,

$$|\lambda_{cd,ab}| \le \left(\sum_s |(K_s)_{c,a}|^2\right)^{1/2}\left(\sum_s |(K_s)_{d,b}|^2\right)^{1/2}.$$

Moreover,

$$\sum_s |(K_s)_{c,a}|^2 \le \sum_{u=1}^{t'}\sum_s |(K_s)_{u,a}|^2 = \left\langle e_a, \left(\sum_s K_s^* K_s\right) e_a\right\rangle = 1,$$

and the same argument gives $\sum_s |(K_s)_{d,b}|^2 \le 1$. Hence $|\lambda_{cd,ab}| \le 1$. ◀

**Proof of Lemma 28.** Fix the input $\mathbf{z} \in \mathbb{F}_q$ and an operator $0 \preceq M \preceq I$. Set $d_0 := 1$ and $d_i := 2^{c_i}$ for every $i \in [k]$. For each $i \in [k]$ and local view $(\mathbf{z}, \mathbf{x}_{-i})$, let

$$\Lambda_i^{(\mathbf{z},\mathbf{x}_{-i})} : \mathbb{C}^{d_{i-1}\times d_{i-1}} \to \mathbb{C}^{d_i \times d_i}$$

be the channel applied by $P_i$.

Let $(\Lambda_k^{(\mathbf{z},\mathbf{x}_{-k})})^*$ denote the Hilbert–Schmidt adjoint. Pull $M$ back through the last sender: $A_M(\mathbf{z}, \mathbf{x}_{-k}) := \big(\Lambda_k^{(\mathbf{z},\mathbf{x}_{-k})}\big)^*(M)$.

Since $\Lambda_k^{(\mathbf{z},\mathbf{x}_{-k})}$ is completely positive and trace preserving, its adjoint is unital and positive. Hence

$$0 \preceq A_M(\mathbf{z}, \mathbf{x}_{-k}) \preceq I_{d_{k-1}}, \qquad \|A_M(\mathbf{z}, \mathbf{x}_{-k})\|_{\mathrm{op}} \le 1.$$

The operator $A_M(\mathbf{z}, \mathbf{x}_{-k})$ acts on the $(k-1)$st message register and depends on the input only through $\mathbf{x}_{-k}$.

Using the matrix units, expand for each $i \in [k-1]$:

$$\Lambda_i^{(\mathbf{z},\mathbf{x}_{-i})}\big(E_{ab}^{(i-1)}\big) = \sum_{c=1}^{d_i}\sum_{d=1}^{d_i} \lambda_{cd,ab}^{(i)}(\mathbf{z}, \mathbf{x}_{-i}) E_{cd}^{(i)}.$$

By Lemma 27, $\big|\lambda_{cd,ab}^{(i)}(\mathbf{z}, \mathbf{x}_{-i})\big| \le 1$.

Let $\sigma_{\mathbf{x},\mathbf{z}}^{<}$ be the state after the first $k-1$ senders. Iterating the above matrix-unit expansions gives

$$\sigma_{\mathbf{x},\mathbf{z}}^{<} = \sum_{a_1,b_1,\ldots,a_{k-1},b_{k-1}} \left(\prod_{i=1}^{k-1} \lambda_{a_i b_i, a_{i-1} b_{i-1}}^{(i)}(\mathbf{z}, \mathbf{x}_{-i})\right) E_{a_{k-1}b_{k-1}}^{(k-1)},$$

where $(a_0, b_0) = (1, 1)$.

Write

$$A_M(\mathbf{z}, \mathbf{x}_{-k}) = \sum_{u=1}^{d_{k-1}}\sum_{v=1}^{d_{k-1}} a_{uv}(\mathbf{z}, \mathbf{x}_{-k}) E_{uv}^{(k-1)}.$$

Since $\|A_M(\mathbf{z}, \mathbf{x}_{-k})\|_{\mathrm{op}} \le 1$, each entry satisfies

$$|a_{uv}(\mathbf{z}, \mathbf{x}_{-k})| = |\langle e_u^{(k-1)}, A_M(\mathbf{z}, \mathbf{x}_{-k}) e_v^{(k-1)}\rangle| \le 1.$$

Since

$$\sigma_{\mathbf{x},\mathbf{z}} = \Lambda_k^{(\mathbf{z},\mathbf{x}_{-k})}\big(\sigma_{\mathbf{x},\mathbf{z}}^{<}\big),$$

the definition of the adjoint gives

$$\mathrm{Tr}(M\sigma_{\mathbf{x},\mathbf{z}}) = \mathrm{Tr}\big(A_M(\mathbf{z}, \mathbf{x}_{-k})\sigma_{\mathbf{x},\mathbf{z}}^{<}\big).$$

Substituting the two expansions and using

$$\mathrm{Tr}\Big(E_{uv}^{(k-1)} E_{ab}^{(k-1)}\Big) = \delta_{v,a}\delta_{u,b},$$

we get

$$\mathrm{Tr}(M\sigma_{\mathbf{x},\mathbf{z}}) = \sum_{a_1,b_1,\ldots,a_{k-1},b_{k-1}} \left(\prod_{i=1}^{k-1} \lambda_{a_i b_i, a_{i-1} b_{i-1}}^{(i)}(\mathbf{z}, \mathbf{x}_{-i})\right) a_{b_{k-1}a_{k-1}}(\mathbf{z}, \mathbf{x}_{-k}).$$

Since $\mathbf{z}$ is fixed, each summand is a product of $k$ functions: for $i \in [k-1]$, the $i$th factor depends only on $\mathbf{x}_{-i}$, and the last factor depends only on $\mathbf{x}_{-k}$. All factors have magnitude at most 1. The number of index choices is

$$L := \prod_{i=1}^{k-1} d_i^2 = 4^{c_1+\cdots+c_{k-1}}.$$

Index these summands by $j \in [L]$ and take their corresponding matrix entries as the functions $\phi_{i,j}$. This gives the desired representation. ◀

## 6 Applications

In this section, we present two applications of our lifting theorems to two benchmark outer functions: the Boolean hidden matching function and the index function.

▶ **Theorem 29** (Lifted Boolean Hidden Matching). *Let* BHM *be the outer function $f$. For every sufficiently large total input length $n$ and every $k \geq 2$ in the ranges below, there are partial $(k+1)$-party functions $F := \mathsf{BHM} \circ G$ on $n$ input bits such that*

$$\mathrm{Q}^{\rightarrow,\mathrm{cons}}_{1/3}(F) = O(\log n).$$

*Using the $G :=$ GIP gadget, one obtains $\mathrm{R}^{\rightarrow,\mathrm{cons}}_{1/3}(F_{\mathrm{GIP}}) \geq \widetilde{\Omega}\big(\sqrt{\frac{n}{k2^k}}\big)$, whereas using $G$ as a random gadget gives, with high probability, $\mathrm{R}^{\rightarrow,\mathrm{cons}}_{1/3}(F_{\mathrm{rand}}) \geq \widetilde{\Omega}\big(\sqrt{\frac{n}{k}}\big)$.*

*Consequently, this application gives a polynomial-versus-logarithmic, hence exponential, separation in the GIP construction only when $k = O(\log n)$. For the random gadget, the same separation holds throughout the polynomial sender regime $k \leq n^{1-\Omega(1)}$.*

**Proof.** Let $\mathsf{BHM}_N$ be Boolean Hidden Matching with Alice's input $z \in \{0,1\}^N$. We use the standard one-way bounds, valid for constant error $2/5$,

$$\mathrm{R}^{\rightarrow}(\mathsf{BHM}_N) = \Omega(\sqrt{N}), \qquad \mathrm{Q}^{\rightarrow}(\mathsf{BHM}_N) = O(\log N);$$

see, e.g., [2, 8].

The number of possible Bob inputs in $\mathsf{BHM}_N$ is $2^{\Theta(N \log N)}$. Choose a prime $q$ large enough to encode Bob's input alphabet into $\mathbb{F}_q$ and also satisfying $q \geq (2k)^2$. Thus

$$\log q = \Theta(N \log N + \log k).$$

We write $\mathsf{BHM}_N$ also for the resulting encoded promise function $\{0,1\}^N \times \mathbb{F}_q \to \{0,1\}$. The composed function is defined on the inverse image of the BHM promise. We use Theorems 16 and 32 in this promise form, which is obtained by restricting the usual lifting simulation to the promised outer inputs.

First consider the GIP gadget. Take the GIP parameters as in Theorem 16, with constant error slack. Since $q \geq (2k)^2$, the factor $\log q / \log(q/2k)$ is constant, and the per-sender gadget block length is $\widetilde{O}(2^k N)$.

Theorem 16 gives

$$\mathrm{R}^{\rightarrow,\mathrm{cons}}_{1/3}(\mathsf{BHM}_N \circ \mathrm{GIP}) \geq \mathrm{R}^{\rightarrow}_{2/5}(\mathsf{BHM}_N) = \Omega(\sqrt{N}).$$

Choosing the largest even $N$ for which the total input length $N + k \cdot \widetilde{O}(2^k N)$ is at most $n$ gives $N = \widetilde{\Theta}\big(\frac{n}{k2^k}\big)$, as long as $k2^k \leq n/\operatorname{polylog} n$. Hence

$$\mathrm{R}^{\rightarrow,\mathrm{cons}}_{1/3}(\mathsf{BHM} \circ \mathrm{GIP}) \geq \widetilde{\Omega}\left(\sqrt{\frac{n}{k2^k}}\right).$$

Now consider the random gadget. Apply Theorem 32 with failure probability, say, $n^{-10}$. Since $\mathrm{R}^{\rightarrow}_{2/5}(\mathsf{BHM}_N) \le N$, the required random-gadget alphabet can be chosen so that each sender has input length $\widetilde{O}(N)$. Therefore, with probability at least $1 - n^{-10}$ over the choice of the random gadget $G$,

$$\mathrm{R}^{\rightarrow,\mathrm{cons}}_{1/3}(\mathsf{BHM}_N \circ G) \ge \mathrm{R}^{\rightarrow}_{2/5}(\mathsf{BHM}_N) = \Omega(\sqrt{N}).$$

Choosing the largest even $N$ for which $N + k \cdot \widetilde{O}(N) \le n$ gives $N = \widetilde{\Theta}\left(\frac{n}{k}\right)$, provided $k \le n/\operatorname{polylog} n$. Thus, with high probability,

$$\mathrm{R}^{\rightarrow,\mathrm{cons}}_{1/3}(\mathsf{BHM} \circ G) \ge \widetilde{\Omega}\left(\sqrt{\frac{n}{k}}\right).$$

It remains to note the quantum upper bound. In the lifted conservative protocol, the terminal player sees the gadget output and hence can compute the encoded Bob input of $\mathsf{BHM}_N$. Any nonterminal sender sees Alice's input $z$ and sends the $O(\log N)$-qubit message from the standard quantum BHM protocol. The terminal player then completes Bob's measurement. Hence, for both gadgets,

$$\mathrm{Q}^{\rightarrow,\mathrm{cons}}_{1/3}(\mathsf{BHM} \circ G) \le O(\log N) \le O(\log n).$$

Finally, the displayed lower bounds are polynomial in $n$ precisely in the corresponding parameter ranges. For the GIP gadget this requires $k2^k \le n^{1-\Omega(1)}$, which in particular forces $k = O(\log n)$. For the random gadget it only requires $k \le n^{1-\Omega(1)}$. Since the quantum cost is $O(\log n)$, these regimes give the claimed polynomial-versus-logarithmic, hence exponential, separations. ◀

▶ **Theorem 30** (Lifted INDEX). *For sufficiently large $n$ and $k \ge 2$, there are $(k+1)$-party total functions $F$ with total input length $n$ obtained by composing the* INDEX *function with a gadget $G$.*

**(i)** *Using the gadget* GIP*, namely*

$$F_{\mathrm{GIP}}(z, x_1, \ldots, x_k) := \mathrm{INDEX}\big(z, \mathrm{GIP}^{(k)}_{q,r}(x_1, \ldots, x_k)\big),$$

*one obtains* $\mathrm{R}^{\rightarrow,\mathrm{cons}}_{1/3}(F_{\mathrm{GIP}}) \ge \widetilde{\Omega}\left(\frac{n}{k2^k}\right)$.

**(ii)** *Using a uniformly random gadget $G := G_m$, namely*

$$F_{\mathrm{rand}}(z, x_1, \ldots, x_k) := \mathrm{INDEX}\big(z, G_m(x_1, \ldots, x_k)\big),$$

*one obtains, with high probability over the choice of $G_m$,* $\mathrm{R}^{\rightarrow,\mathrm{cons}}_{1/3}(F_{\mathrm{rand}}) \ge \widetilde{\Omega}\left(\frac{n}{k}\right)$.

*Consequently, this* INDEX *application gives polynomial randomized lower bounds in the* GIP *construction only when $k = O(\log n)$. For the random gadget, polynomial randomized lower bounds hold throughout the polynomial sender regime $k \le n^{1-\Omega(1)}$. Here $\widetilde{\Omega}$ hides polylogarithmic factors in $n$.*

**Proof.** Let $\mathrm{IND}_N : \{0,1\}^N \times [N] \to \{0,1\}$ be the one-way INDEX function, $\mathrm{IND}_N(z, i) = z_i$. We use the standard bound $\mathrm{R}^{\rightarrow}_{1/3}(\mathrm{IND}_N) = \Omega(N)$ for public-coin one-way randomized protocols; see, e.g., [14]. We will choose $N$ as a function of the final input length $n$.

First consider the GIP gadget. Choose a prime $q = \Theta(\max\{N, k^2\})$, and fix a map $\pi : \mathbb{F}_q \to [N]$ whose restriction to some subset of $\mathbb{F}_q$ is a bijection onto $[N]$. Define the encoded total outer function

$$f_N(z, a) := z_{\pi(a)}, \qquad z \in \{0,1\}^N,\ a \in \mathbb{F}_q.$$

Since $\mathrm{IND}_N$ is a restriction of $f_N$, we have $\mathrm{R}^{\to}_{1/3}(f_N) = \Omega(N)$. Applying Theorem 16 with constant error slack gives

$$\mathrm{R}^{\to,\mathrm{cons}}_{1/3}(f_N \circ \mathrm{GIP}) \geq \Omega(N).$$

Moreover, because $q \geq k^2$, the GIP block length per sender is $|\mathbf{x}_i| = \widetilde{O}(2^k N)$, where the $\widetilde{O}$ hides polylogarithmic factors in $n$. Thus the total lifted input length is $N + k \cdot \widetilde{O}(2^k N)$. Choosing the largest $N$ for which this quantity is at most $n$, and then padding by dummy bits if necessary, gives $N = \widetilde{\Theta}\big(\frac{n}{k2^k}\big)$ in the nontrivial GIP regime $k2^k \leq n/\operatorname{polylog} n$. Consequently,

$$\mathrm{R}^{\to,\mathrm{cons}}_{1/3}(F_{\mathrm{GIP}}) \geq \widetilde{\Omega}\Big(\frac{n}{k2^k}\Big).$$

Now consider the random gadget. Choose a prime $q = \Theta(N)$ and define the same encoded total outer function $f_N : \{0,1\}^N \times \mathbb{F}_q \to \{0,1\}$. Apply Theorem 32 with constant error slack and failure probability, say, $n^{-10}$. Since $\mathrm{R}^{\to}_{1/3}(f_N) = \Omega(N)$ and $\mathrm{R}^{\to}_{1/3}(f_N) \leq N$, the random gadget can be chosen so that each sender has block length $|\mathbf{x}_i| = \widetilde{O}(N)$. Hence, with probability at least $1 - n^{-10}$ over the choice of $G_m$,

$$\mathrm{R}^{\to,\mathrm{cons}}_{1/3}(f_N \circ G_m) \geq \Omega(N).$$

The total input length is now $N + k \cdot \widetilde{O}(N)$. Choosing the largest $N$ for which this is at most $n$, and padding by dummy bits if necessary, gives $N = \widetilde{\Theta}\big(\frac{n}{k}\big)$ in the nontrivial random-gadget regime $k \leq n/\operatorname{polylog} n$. Therefore, with high probability,

$$\mathrm{R}^{\to,\mathrm{cons}}_{1/3}(F_{\mathrm{rand}}) \geq \widetilde{\Omega}\Big(\frac{n}{k}\Big).$$

Finally, the GIP lower bound is polynomial in $n$ only when $k2^k \leq n^{1-\Omega(1)}$, which forces $k = O(\log n)$. In contrast, the random-gadget lower bound is polynomial throughout the regime $k \leq n^{1-\Omega(1)}$. The functions are total because the encoded INDEX function is defined on all of $\mathbb{F}_q$, and both gadgets are total. ◀

## 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. arXiv:1904.13056, 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.

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. arXiv:quant-ph/9904093, 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. arXiv:0906.4291, 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. URL: https://arxiv.org/abs/2506.12420, arXiv:2506.12420, 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. URL: https://arxiv.org/abs/2603.22795, arXiv:2603.22795, doi:10.48550/arXiv.2603.22795.

## A Fourier correlation of the GIP gadget

**Proof of Lemma 20.** Throughout the proof, $\mathbf{x}_1, \dots, \mathbf{x}_k$ are independent and uniformly distributed over $\mathbb{F}_q^r$, and each $\mathbf{y}_i$ is an independent copy of $\mathbf{x}_i$. Fix a cylinder intersection $S \in \mathrm{CI}[(\mathbb{F}_q^r)^k]$ and an element $\alpha \in \mathbb{F}_q^\times$. Write $S = S_1 \cap \cdots \cap S_k$, where each $S_i$ is an $i$-cylinder. Define

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

Since

$$\mathbf{1}[(\mathbf{x}_1,\dots,\mathbf{x}_k) \in S] = \prod_{i=1}^{k} \mathbf{1}[(\mathbf{x}_1,\dots,\mathbf{x}_k) \in S_i],$$

it is enough to prove that $|\Gamma_\alpha(S)| \le (k/q)^{r/2^{k-1}}$ for every $\alpha \in \mathbb{F}_q^\times$ and every $S \in \mathrm{CI}[(\mathbb{F}_q^r)^k]$.

First, we square $\Gamma_\alpha(S)$ and expand with respect to $\mathbf{x}_k$. Because $S_k$ is a $k$-cylinder, the indicator $\mathbf{1}[(\mathbf{x}_1,\dots,\mathbf{x}_k) \in S_k]$ is independent of $\mathbf{x}_k$. Hence

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

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

$$\chi\left(\alpha \sum_{t=1}^{r}(\mathbf{x}_{k,t} - \mathbf{y}_{k,t})\prod_{i=1}^{k-1} \mathbf{x}_{i,t}\right).$$

In 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

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

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

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

For a fixed $t \in [r]$, the event $\prod_{i=2}^{k}(\mathbf{x}_{i,t} - \mathbf{y}_{i,t}) = 0$ means that $\mathbf{x}_{i,t} = \mathbf{y}_{i,t}$ for at least one $i \in \{2,\dots,k\}$. By the union bound,

$$\Pr\left[\prod_{i=2}^{k}(\mathbf{x}_{i,t} - \mathbf{y}_{i,t}) = 0\right] \le \frac{k}{q}.$$

Because the variables corresponding to different coordinates $t \in [r]$ are independent, $|\Gamma_\alpha(S)|^{2^{k-1}} \le (k/q)^r$. Since $S$ and $\alpha$ are arbitrary, taking the supremum proves the lemma. ◀

## B Product Fourier correlation of the GIP gadget

**Proof of Lemma 25.** Fix $\mathbf{v} \in \mathbb{F}_q$ and functions $\phi_i \colon N^{k-1} \to \mathbb{C}$ with $|\phi_i| \le 1$ for every $i \in [k]$. Define

$$\Phi(\mathbf{x}) := \prod_{i=1}^{k} \phi_i(\mathbf{x}_{-i}).$$

Then $|\Phi| \le 1$. Let $\mathbf{x}' \sim \mathrm{Uni}[N^k]$ and $\mathbf{v}' := g(\mathbf{x}')$. Write $p_{\mathbf{v}} := \Pr[\mathbf{v}' = \mathbf{v}]$. Taking all $\phi_i \equiv 1$ in the definition of $\mathrm{PCorr}(g)$ gives $\left|\mathbb{E}[\chi(\alpha\mathbf{v}')]\right| \le \gamma$ for every $\alpha \in \mathbb{F}_q^\times$.

By Fourier inversion, $\mathbf{1}[\mathbf{v}' = \mathbf{v}] = \frac{1}{q}\sum_{\alpha\in\mathbb{F}_q} \chi\big(\alpha(\mathbf{v}' - \mathbf{v})\big)$. Taking expectations gives

$$p_{\mathbf{v}} = \frac{1}{q} + \frac{1}{q}\sum_{\alpha\in\mathbb{F}_q^\times} \chi(-\alpha\mathbf{v})\mathbb{E}[\chi(\alpha\mathbf{v}')].$$

Therefore

$$\left|p_{\mathbf{v}} - \frac{1}{q}\right| \le \frac{1}{q}\sum_{\alpha\in\mathbb{F}_q^\times} \left|\mathbb{E}[\chi(\alpha\mathbf{v}')]\right| \le \frac{q-1}{q}\gamma \le \gamma.$$

In particular,

$$p_{\mathbf{v}} \ge \frac{1}{q} - \gamma = \frac{1 - q\gamma}{q} > 0.$$

Again by Fourier inversion,

$$\mathbb{E}\big[\Phi(\mathbf{x}')\mathbf{1}[\mathbf{v}' = \mathbf{v}]\big] = \frac{\mathbb{E}[\Phi(\mathbf{x}')]}{q} + \frac{1}{q}\sum_{\alpha\in\mathbb{F}_q^\times} \chi(-\alpha\mathbf{v})\mathbb{E}\big[\Phi(\mathbf{x}')\chi(\alpha\mathbf{v}')\big].$$

Also,

$$\mathbb{E}[\Phi(\mathbf{x}')]p_{\mathbf{v}} = \frac{\mathbb{E}[\Phi(\mathbf{x}')]}{q} + \frac{1}{q}\sum_{\alpha\in\mathbb{F}_q^\times} \chi(-\alpha\mathbf{v})\mathbb{E}[\Phi(\mathbf{x}')]\mathbb{E}[\chi(\alpha\mathbf{v}')].$$

Subtracting the two displays yields

$$\mathbb{E}\big[\Phi(\mathbf{x}')\mathbf{1}[\mathbf{v}' = \mathbf{v}]\big] - \mathbb{E}[\Phi(\mathbf{x}')]p_{\mathbf{v}} = \frac{1}{q}\sum_{\alpha\in\mathbb{F}_q^\times} \chi(-\alpha\mathbf{v})\left(\mathbb{E}\big[\Phi(\mathbf{x}')\chi(\alpha\mathbf{v}')\big] - \mathbb{E}[\Phi(\mathbf{x}')]\mathbb{E}[\chi(\alpha\mathbf{v}')]\right).$$

For every $\alpha \in \mathbb{F}_q^\times$, the definition of $\mathrm{PCorr}(g)$ gives

$$\left|\mathbb{E}\big[\Phi(\mathbf{x}')\chi(\alpha\mathbf{v}')\big]\right| \le \gamma.$$

Moreover,

$$\left|\mathbb{E}[\Phi(\mathbf{x}')]\right| \le \mathbb{E}[|\Phi(\mathbf{x}')|] \le 1,$$

and hence

$$|\mathbb{E}[\Phi(\mathbf{x}')]\mathbb{E}[\chi(\alpha\mathbf{v}')]| \le \gamma.$$

Since $|\chi(-\alpha\mathbf{v})| = 1$, the triangle inequality gives

$$\left|\mathbb{E}\big[\Phi(\mathbf{x}')\mathbf{1}[\mathbf{v}' = \mathbf{v}]\big] - \mathbb{E}[\Phi(\mathbf{x}')]p_{\mathbf{v}}\right| \le \frac{1}{q}\sum_{\alpha\in\mathbb{F}_q^\times} 2\gamma = \frac{q-1}{q}\cdot 2\gamma \le 2\gamma.$$

Hence

$$\begin{aligned}\left|\mathbb{E}_{\mathbf{x}''\sim\mathrm{Uni}[N^k|_{\mathbf{v}}]}[\Phi(\mathbf{x}'')] - \mathbb{E}_{\mathbf{x}'\sim\mathrm{Uni}[N^k]}[\Phi(\mathbf{x}')]\right| &= \left|\mathbb{E}[\Phi(\mathbf{x}') \mid \mathbf{v}' = \mathbf{v}] - \mathbb{E}[\Phi(\mathbf{x}')]\right| \\ &= \frac{\left|\mathbb{E}\big[\Phi(\mathbf{x}')\mathbf{1}[\mathbf{v}' = \mathbf{v}]\big] - \mathbb{E}[\Phi(\mathbf{x}')]p_{\mathbf{v}}\right|}{p_{\mathbf{v}}} \\ &\le \frac{2q\gamma}{1-q\gamma}.\end{aligned}$$

Since $q\gamma < 1/2$,

$$\frac{2q\gamma}{1-q\gamma} \le 4q\gamma.$$

Taking the supremum over $\mathbf{v} \in \mathbb{F}_q$ and all functions $\phi_i \colon N^{k-1} \to \mathbb{C}$ with $|\phi_i| \le 1$ proves the lemma. ◀

**Proof of Lemma 26.** Fix $\alpha \in \mathbb{F}_q^\times$ and functions $\phi_i \colon (\mathbb{F}_q^r)^{k-1} \to \mathbb{C}$ with $|\phi_i| \le 1$ for every $i \in [k]$. Throughout the proof, $\mathbf{x}_1, \dots, \mathbf{x}_k$ are independent and uniformly distributed over $\mathbb{F}_q^r$. Set $\ell := k-1$, and write $\mathbf{x}_i = (x_{i,1}, \dots, x_{i,r})$. Let

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

For every $i \in [\ell]$, let $\mathbf{x}_i^{(0)}$ and $\mathbf{x}_i^{(1)}$ be independent copies of $\mathbf{x}_i$. For $\omega \in \{0,1\}^\ell$, write

$$\mathbf{x}_{-k}^{(\omega)} := \big(\mathbf{x}_1^{(\omega_1)}, \dots, \mathbf{x}_\ell^{(\omega_\ell)}\big).$$

Define

$$\Theta := \prod_{\substack{\omega\in\{0,1\}^\ell \\ |\omega| \text{ even}}} \phi_k\big(\mathbf{x}_{-k}^{(\omega)}\big) \prod_{\substack{\omega\in\{0,1\}^\ell \\ |\omega| \text{ odd}}} \overline{\phi_k\big(\mathbf{x}_{-k}^{(\omega)}\big)}.$$

Then $\Theta$ is independent of $\mathbf{x}_k$ and $|\Theta| \le 1$.
For every $t \in [r]$, define

$$A_t := \sum_{\omega\in\{0,1\}^\ell} (-1)^{|\omega|}\prod_{i=1}^{\ell} x_{i,t}^{(\omega_i)} = \prod_{i=1}^{\ell}\big(x_{i,t}^{(0)} - x_{i,t}^{(1)}\big).$$

Since $\overline{\chi(u)} = \chi(-u)$,

$$\prod_{\substack{\omega\in\{0,1\}^\ell \\ |\omega| \text{ even}}} \chi\left(\alpha\sum_{t=1}^{r} x_{k,t}\prod_{i=1}^{\ell} x_{i,t}^{(\omega_i)}\right) \cdot \prod_{\substack{\omega\in\{0,1\}^\ell \\ |\omega| \text{ odd}}} \overline{\chi\left(\alpha\sum_{t=1}^{r} x_{k,t}\prod_{i=1}^{\ell} x_{i,t}^{(\omega_i)}\right)} = \chi\left(\alpha\sum_{t=1}^{r} x_{k,t}A_t\right).$$

At the $i$th step, write the current expression using the product $R_i(\mathbf{u})$ of the copies and conjugates of $\phi_i$, and let $B_i$ denote the remaining integrand. Here $\mathbf{u}$ denotes the remaining outer variables. Since $R_i$ is independent of $\mathbf{x}_i$ and $|R_i| \le 1$, Cauchy–Schwarz gives

$$\left|\mathbb{E}_{\mathbf{u}}\left[R_i(\mathbf{u})\mathbb{E}_{\mathbf{x}_i}B_i(\mathbf{u},\mathbf{x}_i)\right]\right|^2 \le \mathbb{E}_{\mathbf{u}}\left[|R_i(\mathbf{u})|^2\right]\cdot\mathbb{E}_{\mathbf{u}}\left[\left|\mathbb{E}_{\mathbf{x}_i}B_i(\mathbf{u},\mathbf{x}_i)\right|^2\right] \le \mathbb{E}_{\mathbf{u}}\left[\left|\mathbb{E}_{\mathbf{x}_i}B_i(\mathbf{u},\mathbf{x}_i)\right|^2\right].$$

Because $|\Theta| \le 1$, applying this inequality successively for $i = 1, \dots, \ell$ gives

$$|D|^{2^\ell} \le \left|\mathbb{E}_{\mathbf{x}_1^{(0)},\mathbf{x}_1^{(1)},\dots,\mathbf{x}_\ell^{(0)},\mathbf{x}_\ell^{(1)}}\left[\Theta\cdot\mathbb{E}_{\mathbf{x}_k}\chi\left(\alpha\sum_{t=1}^{r}x_{k,t}A_t\right)\right]\right| \le \mathbb{E}_{\mathbf{x}_1^{(0)},\mathbf{x}_1^{(1)},\dots,\mathbf{x}_\ell^{(0)},\mathbf{x}_\ell^{(1)}}\left|\mathbb{E}_{\mathbf{x}_k}\chi\left(\alpha\sum_{t=1}^{r}x_{k,t}A_t\right)\right|.$$

For fixed copies $\mathbf{x}_i^{(0)}, \mathbf{x}_i^{(1)}$, character orthogonality gives

$$\mathbb{E}_{\mathbf{x}_k}\chi\left(\alpha\sum_{t=1}^{r} x_{k,t}A_t\right) = \prod_{t=1}^{r}\mathbb{E}_{x_{k,t}}\left[\chi(\alpha x_{k,t}A_t)\right] = \prod_{t=1}^{r}\mathbf{1}[A_t = 0].$$

For fixed $t \in [r]$, the differences $x_{i,t}^{(0)} - x_{i,t}^{(1)}$ are independent and uniform over $\mathbb{F}_q$. Therefore

$$\Pr[A_t = 0] = 1 - \left(1 - \frac{1}{q}\right)^{\ell}.$$

The events $A_t = 0$ are independent over $t \in [r]$. Hence

$$|D|^{2^\ell} \le \left(1 - \left(1 - \frac{1}{q}\right)^{\ell}\right)^{r}.$$

Finally, $1 - \left(1 - \frac{1}{q}\right)^{\ell} \le \frac{\ell}{q} \le \frac{k}{q}$. Taking the $2^\ell$th root and recalling that $\ell = k - 1$, we obtain

$$|D| \le \left(\frac{k}{q}\right)^{r/2^{k-1}}.$$

Since $\alpha$ and the functions $\phi_i$ were arbitrary, taking the supremum proves the lemma. ◀

## C Randomized and quantum lifting with random gadgets

In this section, we replace the explicit gadget $\mathrm{GIP}_{q,r}^{(k)}$ by a random gadget. Now take $X_1 = \cdots = X_k = [m]$ and $X = [m]^k$, so that each input point is written as $\mathbf{x} = (\mathbf{x}_1, \ldots, \mathbf{x}_k) \in X$ and $\mathbf{x}_{-i} \in X_{-i} = \prod_{j\neq i} X_j$, $\forall i \in [k]$. Each player now receives $\lceil \log m \rceil$ bits of gadget input.

A random gadget is a function $G_m \colon [m]^k \to \mathbb{F}_q$ chosen by assigning the values $G_m(\mathbf{x})$ independently and uniformly in $\mathbb{F}_q$ for all $\mathbf{x} \in [m]^k$.

The following theorem shows that a random gadget has small fiber discrepancy against cylinder intersections and generalized cylinder intersections.

▶ **Theorem 31.** *Given $k \ge 2$, let $q \ge 2$ be prime, and let $0 < \zeta < 1$ be constant. Choose $G_m \colon [m]^k \to \mathbb{F}_q$ uniformly at random. Then the following estimates on fiber discrepancy*

1. ***Fiber discrepancy against cylinder intersections.*** *Define*

$$\beta_{k,q,m} := \left(\frac{10q}{3m^k}\left(km^{k-1}\ln 2 + \ln\frac{4q}{\zeta}\right)\right)^{1/2}.$$

*If*

$$m^k \ge 8q\ln\frac{2q}{\zeta} \qquad \text{and} \qquad \beta_{k,q,m} \le 1,$$

*with probability at least $1-\zeta$, every fiber of $G_m$ is nonempty and $\Delta_{G_m} \le \beta_{k,q,m}$. Moreover, when $m \ge q$, this gives a simpler estimate*

$$\Delta_{G_m} = O_\zeta\left(\sqrt{\frac{qk}{m}}\right).$$

2. ***Fiber discrepancy against generalized cylinder intersections.*** *Let $0 < \theta \le 1$. If $m$ satisfies*

$$m^k \ge 12q\ln\frac{4q}{\zeta}, \qquad \frac{m^k\theta^2}{1024q} \ge 2km^{k-1}\ln\frac{256k}{\theta} + \ln\frac{8q}{\zeta},$$

*with probability at least* $1-\zeta$*, every fiber of* $G_m$ *is nonempty and* $\Delta^{\Pi}_{G_m} \le \theta$*. Moreover, for a sufficiently large universal constant* $K_0 > 0$*, the hypothesis on* $m$ *could be simplified as*

$$m \ge K_0 \, \frac{q}{\theta^2} \left( k \ln \frac{k}{\theta} + \ln \frac{q}{\zeta} \right).$$

The proof of Theorem 31 is postponed to Section C.3. In Sections C.1 and C.2, we apply the random gadget to randomized and quantum lifting and obtain sharper gadget-size bounds than those for GIP.

## C.1 Randomized lifting with a random gadget

In this section, we prove the following randomized lifting theorem using a random gadget.

▶ **Theorem 32** (Random-gadget randomized lifting)**.** *Given* $k \ge 2$*, let* $q \ge 2$ *be prime, let* $Z$ *be an arbitrary finite set. Let* $0 < \zeta < 1$*. Let* $0 \le \varepsilon \le 1$ *and* $0 < \delta \le 1 - \varepsilon$ *be constants. Let* $f \colon Z \times \mathbb{F}_q \to \{0,1\}$*. Choose* $G_m \colon [m]^k \to \mathbb{F}_q$ *uniformly at random, and define* $F \colon Z \times [m]^k \to \{0,1\}$ *by* $F(z, \mathbf{x}) := f\big(z, G_m(\mathbf{x})\big)$*. There exists a universal constant* $K > 0$ *such that if*

$$m \ge K \, q \, 2^{2\mathrm{R}^{\rightarrow}_{\varepsilon+\delta}(f)} \delta^{-2} \left( k + \ln \frac{q}{\zeta} \right),$$

*with probability at least* $1-\zeta$ *over the choice of* $G_m$*,*

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

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

**Remark: comparison with** GIP **gadget.** Theorem 32 has exactly the same lifting interface as the GIP-based theorem, namely Theorem 16; only the gadget is changed. The tradeoff is that $G_m$ is non-explicit: its truth table consists of $m^k$ independent uniformly random entries in $\mathbb{F}_q$. The gain is that the per-player gadget size is now

$$\lceil \log m \rceil = \Theta_{\delta,\zeta}\big( \log |Z| + \log q + \log(k + \log q) \big).$$

By contrast, the GIP-gadget lifting uses gadget size

$$\lceil r \log q \rceil = \Theta_{\delta} \left( 2^k \frac{\log q}{\log(q/2k)} \left( \log |Z| + \log q \right) \right).$$

So the random gadget removes the exponential dependence on $k$ from the gadget size.

We prove the randomized lifting theorem using a random gadget as follows.

**Proof of Theorem 32.** We prove the theorem with any universal constant $K \ge 8$. Assume

$$m \ge K \, q \, 2^{2\mathrm{R}^{\rightarrow}_{\varepsilon+\delta}(f)} \delta^{-2} \left( k + \ln \frac{q}{\zeta} \right).$$

Since $K \ge 8$, $\delta \le 1$, and $\mathrm{R}^{\rightarrow}_{\varepsilon+\delta}(f) \ge 0$, this implies $m \ge 8q \left( k + \ln \frac{q}{\zeta} \right)$. In particular $m \ge q$. We first verify the two hypotheses of the part (1) in Theorem 31.

The first condition follows immediately:

$$m^k \geq m \geq 8q\left(k + \ln\frac{q}{\zeta}\right) \geq 8q \ln\frac{2q}{\zeta},$$

where the last inequality uses $k \geq 2 \geq \ln 2$.

It remains to check that $\beta_{k,q,m} \leq 1$. More precisely, we will prove the stronger bound

$$\beta_{k,q,m} \leq \delta\, 2^{-\mathrm{R}^{\rightarrow}_{\varepsilon+\delta}(f)}.$$

By the definition of $\beta_{k,q,m}$,

$$\beta^2_{k,q,m} = \frac{10q}{3}\left(\frac{k\ln 2}{m} + \frac{\ln(4q/\zeta)}{m^k}\right).$$

Using $m^k \geq m$, $k \ln 2 \leq k$, and

$$\ln\frac{4q}{\zeta} = \ln\frac{q}{\zeta} + \ln 4 \leq \ln\frac{q}{\zeta} + k,$$

we get

$$\beta^2_{k,q,m} \leq \frac{20q}{3m}\left(k + \ln\frac{q}{\zeta}\right).$$

Now applying the lower bound on $m$,

$$\beta^2_{k,q,m} \leq \frac{20}{3K}\delta^2 2^{-2\mathrm{R}^{\rightarrow}_{\varepsilon+\delta}(f)} \leq \delta^2 2^{-2\mathrm{R}^{\rightarrow}_{\varepsilon+\delta}(f)}.$$

Therefore $\beta_{k,q,m} \leq \delta\, 2^{-\mathrm{R}^{\rightarrow}_{\varepsilon+\delta}(f)} \leq 1$. Thus both hypotheses of Theorem 31 (1) are satisfied. Hence, with probability at least $1-\zeta$, every fiber of $G_m$ is nonempty and $\Delta_{G_m} \leq \beta_{k,q,m} \leq \delta\, 2^{-\mathrm{R}^{\rightarrow}_{\varepsilon+\delta}(f)}$. Fix a gadget $G_m$ satisfying this event.

Consider any public-coin one-way conservative protocol for $F$ with cost $C$ and worst-case error at most $\varepsilon$. We show that $C \geq \mathrm{R}^{\rightarrow}_{\varepsilon+\delta}(f)$ as follows.

Suppose otherwise that $C < \mathrm{R}^{\rightarrow}_{\varepsilon+\delta}(f)$. By Lemma 18, this protocol induces a public-coin two-party one-way protocol for $f$ with cost $C$ and worst-case error at most $\varepsilon + 2^C\Delta_{G_m}$. Using the bound on $\Delta_{G_m}$, we have

$$\varepsilon + 2^C\Delta_{G_m} \leq \varepsilon + 2^C\delta\, 2^{-\mathrm{R}^{\rightarrow}_{\varepsilon+\delta}(f)} < \varepsilon + \delta.$$

This gives a two-party one-way protocol for $f$ of cost $C < \mathrm{R}^{\rightarrow}_{\varepsilon+\delta}(f)$ and error at most $\varepsilon+\delta$, contradicting the definition of $\mathrm{R}^{\rightarrow}_{\varepsilon+\delta}(f)$. ◀

## C.2 Quantum lifting with a random gadget

In this section, we prove the following quantum lifting theorem using a random gadget.

▶ **Theorem 33** (Random-gadget quantum lifting). *Given $k \geq 2$, let $q \geq 2$ be prime, let $Z$ be an arbitrary finite set. Let $0 < \zeta < 1$, $0 \leq \varepsilon \leq 1$ and $0 < \delta \leq 1-\varepsilon$ be constants. Let $f\colon Z \times \mathbb{F}_q \to \{0,1\}$. Choose $G_m\colon [m]^k \to \mathbb{F}_q$ uniformly at random, and define $F\colon Z \times [m]^k \to \{0,1\}$ by $F(z,\mathbf{x}) := f\big(z, G_m(\mathbf{x})\big)$. There exists a universal constant $K > 0$ such that if*

$$m \geq K\, 2^{4\mathrm{Q}^{\rightarrow}_{\varepsilon+\delta}(f)}\, q\, \delta^{-2}\left(k\ln\frac{k 2^{2\mathrm{Q}^{\rightarrow}_{\varepsilon+\delta}(f)}}{\delta} + \ln\frac{q}{\zeta}\right),$$

*with probability at least* $1-\zeta$ *over the choice of* $G_m$, $\mathrm{Q}^{\rightarrow,\mathrm{cons}}_{\varepsilon}(F) \geq \mathrm{Q}^{\rightarrow}_{\varepsilon+\delta}(f)$. *Moreover, since* $\mathrm{Q}^{\rightarrow}_{\varepsilon+\delta}(f) \leq \lceil \log |Z| \rceil$, *it suffices to take*

$$m = \left\lceil K\, q\, 2^{4\lceil \log |Z| \rceil} \delta^{-2} \left( k \ln \frac{k 2^{2\lceil \log |Z| \rceil}}{\delta} + \ln \frac{q}{\zeta} \right) \right\rceil .$$

*The input length* $|z| = \log |Z|$ *and* $\forall i \in [k]$,

$$|\mathbf{x}_i| = \lceil \log m \rceil = \Theta_{\delta,\zeta}(\log |Z| + \log q + \log(k \ln k + k \log |Z| + \ln q)) .$$

### C.2.0.1 Comparison with GIP.

The per-player gadget input length for a random gadget is

$$\lceil \log m \rceil = \Theta_{\delta,\zeta}(\log |Z| + \log q + \log(k \ln k + k \log |Z| + \ln q)) ,$$

whereas for the GIP gadget it is

$$\lceil r \log q \rceil = \Theta_{\delta} \left( 2^k \frac{\log q}{\log(q/k)} (\log |Z| + \log(q)) \right) .$$

Thus the random gadget removes the exponential dependence on $k$ from the gadget size.

We prove the quantum lifting theorem using a random gadget as follows.

**Proof of Theorem 33.** Let $Q := \mathrm{Q}^{\rightarrow}_{\varepsilon+\delta}(f)$ and $\theta := \delta\, 2^{-2Q}$. Then $0 < \theta \leq 1$. Choose the universal constant $K$ in the theorem large enough so that the lower bound on $m$ implies the simplified sufficient condition in Theorem 31(2) with this value of $\theta$. Hence, with probability at least $1-\zeta$, every fiber of $G_m$ is nonempty and

$$\Delta^{\Pi}_{G_m} \leq \theta = \delta\, 2^{-2Q}.$$

Fix a gadget $G_m$ satisfying this event.

Consider any quantum one-way conservative protocol for $F$ with total cost $C$ and worst-case error at most $\varepsilon$. Suppose, for contradiction, that $C < Q$. Let $c_1, \ldots, c_k$ be its message lengths and set $c_{\mathrm{pre}} := c_1 + \cdots + c_{k-1}$. Since all message lengths are nonnegative, $c_k \leq C < Q$ and $c_{\mathrm{pre}} \leq C < Q$. By Lemma 24, this protocol yields a two-party one-way quantum protocol for $f$ with cost at most $c_k$ and worst-case error at most

$$\varepsilon + 2^{2c_{\mathrm{pre}}} \Delta^{\Pi}_{G_m} \leq \varepsilon + 2^{2c_{\mathrm{pre}}} \delta\, 2^{-2Q} < \varepsilon + \delta.$$

This contradicts the definition of $Q$. Therefore every quantum one-way conservative protocol for $F$ with error at most $\varepsilon$ has total cost at least $Q$, proving the theorem. ◀

## C.3 Proof of Theorem 31

The two parts of Theorem 31 are proved in Lemmas 34 and 35. The simplified bound in part (1) follows directly from the definition of $\beta_{k,q,m}$: when $m \geq q$ and $\zeta$ is fixed, the term $q \ln(4q/\zeta)/m^k$ is dominated by $O(qk/m)$. We prove the part (1) first.

▶ **Lemma 34** (Random gadgets have small fiber discrepancy). *Fix* $k \geq 2$, *let* $q \geq 2$ *be prime, let* $m \geq 2$, *and let* $0 < \zeta < 1$. *Choose* $G_m \colon [m]^k \to \mathbb{F}_q$ *uniformly at random. Assume*

$$m^k \geq 8q \ln \frac{2q}{\zeta}$$

*and define*

$$\beta_{k,q,m} := \left(\frac{10q}{3m^k}\left(km^{k-1}\ln 2 + \ln\frac{4q}{\zeta}\right)\right)^{1/2}.$$

*If $\beta_{k,q,m} \le 1$, then with probability at least $1-\zeta$, every fiber of $G_m$ is nonempty and $\Delta_{G_m} \le \beta_{k,q,m}$.*

**Proof.** We first control the fiber sizes. For each fixed $v \in \mathbb{F}_q$, the random variable $|G_m^{-1}(v)|$ has distribution $\mathrm{Bin}(m^k, 1/q)$. By the Chernoff bound,

$$\Pr\left[|G_m^{-1}(v)| < \frac{m^k}{2q}\right] \le \exp\left(-\frac{m^k}{8q}\right).$$

Taking a union bound over all $v \in \mathbb{F}_q$ and using $m^k \ge 8q\ln(2q/\zeta)$, we get $q\exp\left(-\frac{m^k}{8q}\right) \le \frac{\zeta}{2}$. Hence, with probability at least $1-\zeta/2$,

$$\Pr_{\mathbf{x}'\sim\mathrm{Uni}_{[m]^k}}[G_m(\mathbf{x}') = v] \ge \frac{1}{2q} \qquad \text{for every } v \in \mathbb{F}_q. \tag{1}$$

In particular, every fiber of $G_m$ is nonempty on this event.

Now fix a cylinder intersection $S \in \mathrm{CI}([m]^k)$ and a value $v \in \mathbb{F}_q$. Define

$$A(S,v) := \mathbb{E}_{\mathbf{x}'\sim\mathrm{Uni}_{[m]^k}}\left[\left(\mathbf{1}[\mathbf{x}' \in S] - \Pr_{\mathbf{y}'\sim\mathrm{Uni}_{[m]^k}}[\mathbf{y}' \in S]\right)\mathbf{1}[G_m(\mathbf{x}') = v]\right].$$

Since

$$\sum_{\mathbf{x}\in[m]^k}\left(\mathbf{1}[\mathbf{x} \in S] - \Pr_{\mathbf{y}'\sim\mathrm{Uni}_{[m]^k}}[\mathbf{y}' \in S]\right) = 0,$$

we may also write

$$m^k A(S,v) = \sum_{\mathbf{x}\in[m]^k}\left(\mathbf{1}[\mathbf{x} \in S] - \Pr_{\mathbf{y}'\sim\mathrm{Uni}_{[m]^k}}[\mathbf{y}' \in S]\right)\left(\mathbf{1}[G_m(\mathbf{x}) = v] - \frac{1}{q}\right).$$

The summands on the right-hand side are independent and have mean zero, because the values $G_m(\mathbf{x})$ are independent and uniform in $\mathbb{F}_q$. Moreover, each summand has absolute value at most 1.

For the variance term, we have

$$\begin{aligned}
&\sum_{\mathbf{x}\in[m]^k}\mathbb{E}\left[\left(\mathbf{1}[\mathbf{x} \in S] - \Pr_{\mathbf{y}'\sim\mathrm{Uni}_{[m]^k}}[\mathbf{y}' \in S]\right)^2\left(\mathbf{1}[G_m(\mathbf{x}) = v] - \frac{1}{q}\right)^2\right] \\
&\le \frac{1}{q}\sum_{\mathbf{x}\in[m]^k}\left(\mathbf{1}[\mathbf{x} \in S] - \Pr_{\mathbf{y}'\sim\mathrm{Uni}_{[m]^k}}[\mathbf{y}' \in S]\right)^2 \\
&= \frac{m^k}{q}\Pr_{\mathbf{x}'\sim\mathrm{Uni}_{[m]^k}}[\mathbf{x}' \in S]\left(1 - \Pr_{\mathbf{x}'\sim\mathrm{Uni}_{[m]^k}}[\mathbf{x}' \in S]\right) \\
&\le \frac{m^k}{4q}.
\end{aligned}$$

Thus Bernstein's inequality gives, for every $0 < \theta \le 1$,

$$\Pr\left[|A(S,v)| > \frac{\theta}{2q}\right] \le 2\exp\left(-\frac{(m^k\theta/(2q))^2}{2(m^k/(4q) + m^k\theta/(6q))}\right).$$

Since $\theta \le 1$,

$$2\left(\frac{m^k}{4q} + \frac{m^k\theta}{6q}\right) \le \frac{5m^k}{6q}.$$

Therefore

$$\Pr\left[|A(S,v)| > \frac{\theta}{2q}\right] \le 2\exp\left(-\frac{3m^k\theta^2}{10q}\right). \tag{2}$$

We next take a union bound over all cylinder intersections. For each $i \in [k]$, an $i$-cylinder is determined by an arbitrary subset of $[m]^{k-1}$. Hence the number of cylinder intersections in $[m]^k$ is at most $2^{km^{k-1}}$. Applying the inequality (2) with $\theta = \beta_{k,q,m}$ is allowed by the assumption $\beta_{k,q,m} \le 1$. By the definition of $\beta_{k,q,m}$,

$$\frac{3m^k\beta_{k,q,m}^2}{10q} = km^{k-1}\ln 2 + \ln\frac{4q}{\zeta}.$$

Therefore

$$2^{km^{k-1}} \cdot q \cdot 2\exp\left(-\frac{3m^k\beta_{k,q,m}^2}{10q}\right) = 2^{km^{k-1}} \cdot q \cdot 2\exp\left(-km^{k-1}\ln 2 - \ln\frac{4q}{\zeta}\right) = \frac{\zeta}{2}.$$

So, with probability at least $1 - \zeta/2$,

$$|A(S,v)| \le \frac{\beta_{k,q,m}}{2q} \qquad \text{for every } S \in \mathrm{CI}([m]^k) \text{ and every } v \in \mathbb{F}_q. \tag{3}$$

Assume now that both events (1) and (3) hold. For every $S \in \mathrm{CI}([m]^k)$ and every $v \in \mathbb{F}_q$,

$$A(S,v) = \Pr_{\mathbf{x}' \sim \mathrm{Uni}_{[m]^k}}[G_m(\mathbf{x}') = v]\left(\Pr_{\mathbf{x}'' \sim \mathrm{Uni}_{G_m^{-1}(v)}}[\mathbf{x}'' \in S] - \Pr_{\mathbf{x}' \sim \mathrm{Uni}_{[m]^k}}[\mathbf{x}' \in S]\right).$$

Hence

$$\left|\Pr_{\mathbf{x}'' \sim \mathrm{Uni}_{G_m^{-1}(v)}}[\mathbf{x}'' \in S] - \Pr_{\mathbf{x}' \sim \mathrm{Uni}_{[m]^k}}[\mathbf{x}' \in S]\right| = \frac{|A(S,v)|}{\Pr_{\mathbf{x}' \sim \mathrm{Uni}_{[m]^k}}[G_m(\mathbf{x}') = v]}$$

$$\le \frac{\beta_{k,q,m}/(2q)}{1/(2q)} = \beta_{k,q,m}.$$

Taking the maximum over all $S \in \mathrm{CI}([m]^k)$ and all $v \in \mathbb{F}_q$ gives $\Delta_{G_m} \le \beta_{k,q,m}$. The two bad events have total probability at most $\zeta$, and the proof is complete. ◀

We prove the part (2) of Theorem 31 as follows.

▶ **Lemma 35** (Random gadgets fool the generalized cylinder intersections). *Fix $k \ge 2$, let $q \ge 2$ be prime, let $m \ge 2$, and let $0 < \zeta < 1$. Choose $G_m \colon [m]^k \to \mathbb{F}_q$ uniformly at random. Let $0 < \theta \le 1$. Assume*

$$m^k \ge 12q\ln\frac{4q}{\zeta}$$

*and*

$$\frac{m^k\theta^2}{1024q} \ge 2km^{k-1}\ln\frac{256k}{\theta} + \ln\frac{8q}{\zeta}.$$

*Then with probability at least $1 - \zeta$, every fiber of $G_m$ is nonempty and $\Delta_{G_m}^{\Pi} \le \theta$. Moreover, these two hypotheses are implied by the simpler sufficient condition*

$$m \ge K_0\frac{q}{\theta^2}\left(k\ln\frac{k}{\theta} + \ln\frac{q}{\zeta}\right)$$

*for a sufficiently large universal constant $K_0 > 0$; for instance, one may take $K_0 = 2^{15}$.*

**Proof.** For each fixed $v \in \mathbb{F}_q$, the random variable $|G_m^{-1}(v)|$ has distribution $\mathrm{Bin}(m^k, 1/q)$. By the Chernoff bound,

$$\Pr\left[\left||G_m^{-1}(v)| - \frac{m^k}{q}\right| > \frac{m^k}{2q}\right] \le 2\exp\left(-\frac{m^k}{12q}\right).$$

A union bound over $v \in \mathbb{F}_q$ and the first hypothesis give $2q\exp\left(-\frac{m^k}{12q}\right) \le \frac{\zeta}{2}$. Thus, with probability at least $1 - \zeta/2$,

$$\frac{1}{2q} \le \Pr_{\mathbf{x}' \sim \mathrm{Uni}_{[m]^k}}[G_m(\mathbf{x}') = v] \le \frac{3}{2q} \qquad \text{for every } v \in \mathbb{F}_q. \tag{4}$$

In particular, every fiber of $G_m$ is nonempty on this event.

Let $\mathcal{P}$ be the family of product-cylinder tests

$$\psi(\mathbf{x}) = \prod_{i=1}^{k} \phi_i(\mathbf{x}_{-i}), \qquad \phi_i : \prod_{j \ne i}[m] \to \mathbb{C}, \qquad |\phi_i| \le 1.$$

For $\psi \in \mathcal{P}$ and $v \in \mathbb{F}_q$, define

$$B(\psi, v) := \mathbb{E}_{\mathbf{x}' \sim \mathrm{Uni}_{[m]^k}}\left[\left(\psi(\mathbf{x}') - \mathbb{E}_{\mathbf{y}' \sim \mathrm{Uni}_{[m]^k}}\psi(\mathbf{y}')\right)\mathbf{1}[G_m(\mathbf{x}') = v]\right].$$

If $|B(\psi, v)| \le \theta/(2q)$ for every $\psi \in \mathcal{P}$ and every $v \in \mathbb{F}_q$, then on the event (4),

$$\left|\mathbb{E}_{\mathbf{x}'' \sim \mathrm{Uni}_{G_m^{-1}(v)}}\psi(\mathbf{x}'') - \mathbb{E}_{\mathbf{x}' \sim \mathrm{Uni}_{[m]^k}}\psi(\mathbf{x}')\right| = \frac{|B(\psi, v)|}{\Pr_{\mathbf{x}' \sim \mathrm{Uni}_{[m]^k}}[G_m(\mathbf{x}') = v]} \le \theta.$$

Therefore it remains to prove this uniform bound on $B(\psi, v)$.

Fix $\psi \in \mathcal{P}$ and $v \in \mathbb{F}_q$. Since

$$\sum_{\mathbf{x} \in [m]^k}\left(\psi(\mathbf{x}) - \mathbb{E}_{\mathbf{y}' \sim \mathrm{Uni}_{[m]^k}}\psi(\mathbf{y}')\right) = 0,$$

we have

$$m^k B(\psi, v) = \sum_{\mathbf{x} \in [m]^k}\left(\psi(\mathbf{x}) - \mathbb{E}_{\mathbf{y}' \sim \mathrm{Uni}_{[m]^k}}\psi(\mathbf{y}')\right)\left(\mathbf{1}[G_m(\mathbf{x}) = v] - \frac{1}{q}\right).$$

The summands on the right-hand side are independent and have mean zero. They are bounded in modulus by 2, because $|\psi(\mathbf{x})| \le 1$ and $\left|\mathbb{E}_{\mathbf{y}' \sim \mathrm{Uni}_{[m]^k}}\psi(\mathbf{y}')\right| \le 1$. Moreover, their total second moment is at most

$$\frac{1}{q}\sum_{\mathbf{x} \in [m]^k}\left|\psi(\mathbf{x}) - \mathbb{E}_{\mathbf{y}' \sim \mathrm{Uni}_{[m]^k}}\psi(\mathbf{y}')\right|^2 \le \frac{4m^k}{q}.$$

For a complex number $z$, let $z^{\mathrm{re}}$ and $z^{\mathrm{im}}$ denote its real and imaginary parts. Applying Bernstein's inequality to either $(m^k B(\psi, v))^{\mathrm{re}}$ or $(m^k B(\psi, v))^{\mathrm{im}}$, with uniform bound 2 and variance proxy $4m^k/q$, gives

$$\Pr\left[\left|(m^k B(\psi, v))^{\mathrm{re}}\right| > \frac{m^k\theta}{8q}\right] \le 2\exp\left(-\frac{(m^k\theta/(8q))^2}{2(4m^k/q + 2m^k\theta/(24q))}\right).$$

and

$$\Pr\left[\left|(m^k B(\psi, v))^{\mathrm{im}}\right| > \frac{m^k\theta}{8q}\right] \le 2\exp\left(-\frac{(m^k\theta/(8q))^2}{2(4m^k/q + 2m^k\theta/(24q))}\right).$$

Since $\theta \le 1$, the denominator is at most $9m^k/q$. Hence each of the two probabilities is at most

$$2\exp\left(-\frac{m^k\theta^2}{576q}\right) \le 2\exp\left(-\frac{m^k\theta^2}{1024q}\right).$$

If $|B(\psi,v)| > \theta/(4q)$, then either $\left|(m^k B(\psi,v))^{\mathrm{re}}\right| > \frac{m^k\theta}{8q}$ or $\left|(m^k B(\psi,v))^{\mathrm{im}}\right| > \frac{m^k\theta}{8q}$. Therefore

$$\Pr\left[|B(\psi,v)| > \frac{\theta}{4q}\right] \le 4\exp\left(-\frac{m^k\theta^2}{1024q}\right). \tag{5}$$

We next make the estimate uniform over all product-cylinder tests. The unit disk in $\mathbb{C}$ has a $\theta/(64k)$-net, contained in the unit disk, of size at most $\left(\frac{256k}{\theta}\right)^2$. Approximating every value of every factor $\phi_i$ by this scalar net produces a finite family $\mathcal{N} \subseteq \mathcal{P}$ with $|\mathcal{N}| \le \left(\frac{256k}{\theta}\right)^{2km^{k-1}}$.

For every $\psi \in \mathcal{P}$, there is some $h \in \mathcal{N}$ such that $\|\psi - h\|_\infty \le \frac{\theta}{64}$. Indeed, if the $i$th factor is changed by at most $\theta/(64k)$, while all factors remain bounded by 1 in modulus, then the product changes by at most $\theta/(64k)$ from that factor; summing over $i \in [k]$ gives the displayed bound.

By (5), the second hypothesis, and a union bound over all $h \in \mathcal{N}$ and all $v \in \mathbb{F}_q$,

$$q|\mathcal{N}| \cdot 4\exp\left(-\frac{m^k\theta^2}{1024q}\right) \le \frac{\zeta}{2}.$$

Hence, with probability at least $1 - \zeta/2$,

$$|B(h,v)| \le \frac{\theta}{4q} \qquad \text{for every } h \in \mathcal{N} \text{ and every } v \in \mathbb{F}_q. \tag{6}$$

Assume that both events (4) and (6) hold. Fix arbitrary $\psi \in \mathcal{P}$ and $v \in \mathbb{F}_q$, and choose $h \in \mathcal{N}$ such that $\|\psi - h\|_\infty \le \theta/64$. Let $\mathbf{y}'$ be uniform over $[m]^k$. Then

$$\begin{aligned} |B(\psi,v) - B(h,v)| &= \left|\mathbb{E}_{\mathbf{x}'\sim \mathrm{Uni}_{[m]^k}}\left[\big((\psi-h)(\mathbf{x}') - \mathbb{E}_{\mathbf{y}'}(\psi-h)(\mathbf{y}')\big)\mathbf{1}[G_m(\mathbf{x}') = v]\right]\right| \\ &\le 2\|\psi - h\|_\infty \Pr_{\mathbf{x}'\sim \mathrm{Uni}_{[m]^k}}[G_m(\mathbf{x}') = v] \\ &\le \frac{3\theta}{64q}, \end{aligned}$$

where the last inequality uses (4). Therefore

$$|B(\psi,v)| \le |B(h,v)| + |B(\psi,v) - B(h,v)| \le \frac{\theta}{4q} + \frac{3\theta}{64q} < \frac{\theta}{2q}.$$

As shown above, this implies $\Delta^{\Pi}_{G_m} \le \theta$. The two bad events have total probability at most $\zeta$, so the main claim follows.

It remains to verify the simplified sufficient condition on $m$. Assume

$$m \ge K_0 \frac{q}{\theta^2}\left(k\ln\frac{k}{\theta} + \ln\frac{q}{\zeta}\right)$$

with $K_0 = 2^{15}$.

First, since $\theta \le 1$,

$$m^k \ge m \ge K_0 q\left(k\ln\frac{k}{\theta} + \ln\frac{q}{\zeta}\right).$$

Also, since $q \geq 2$ and $\zeta < 1$,

$$\ln \frac{4q}{\zeta} = \ln \frac{q}{\zeta} + \ln 4 \leq 3 \ln \frac{q}{\zeta} \leq 3 \left( k \ln \frac{k}{\theta} + \ln \frac{q}{\zeta} \right).$$

Thus

$$12q \ln \frac{4q}{\zeta} \leq 36q \left( k \ln \frac{k}{\theta} + \ln \frac{q}{\zeta} \right) \leq m^k,$$

because $K_0 = 2^{15} \geq 36$. This proves the first original hypothesis.

For the second original hypothesis, it is enough to prove

$$\frac{m\theta^2}{1024q} \geq 2k \ln \frac{256k}{\theta} + \ln \frac{8q}{\zeta}.$$

Indeed, multiplying this inequality by $m^{k-1} \geq 1$ gives

$$\frac{m^k \theta^2}{1024q} \geq 2km^{k-1} \ln \frac{256k}{\theta} + m^{k-1} \ln \frac{8q}{\zeta} \geq 2km^{k-1} \ln \frac{256k}{\theta} + \ln \frac{8q}{\zeta}.$$

Now $k \geq 2$ and $\theta \leq 1$ imply $\ln(k/\theta) \geq \ln 2$, so

$$\ln \frac{256k}{\theta} = \ln \frac{k}{\theta} + \ln 256 \leq 9 \ln \frac{k}{\theta}.$$

Similarly,

$$\ln \frac{8q}{\zeta} = \ln \frac{q}{\zeta} + \ln 8 \leq 4 \ln \frac{q}{\zeta}.$$

Consequently,

$$2k \ln \frac{256k}{\theta} + \ln \frac{8q}{\zeta} \leq 18k \ln \frac{k}{\theta} + 4 \ln \frac{q}{\zeta} \leq 20 \left( k \ln \frac{k}{\theta} + \ln \frac{q}{\zeta} \right).$$

On the other hand, the simplified condition gives

$$\frac{m\theta^2}{1024q} \geq \frac{K_0}{1024} \left( k \ln \frac{k}{\theta} + \ln \frac{q}{\zeta} \right) = 32 \left( k \ln \frac{k}{\theta} + \ln \frac{q}{\zeta} \right).$$

Since $32 \geq 20$, the second original hypothesis follows. This completes the proof. ◀