Electronic Colloquium on Computational Complexity, Report No. 117 (2026)

Quantum Communication Lower Bounds for Search Problems via Matrix Discrepancy

Minbo Gao* Chenghua Liu† Guangxu Yang ‡ Tianyi Zhang §

Abstract

We study one-way quantum communication lower bounds for search problems. Unlike decision problems, search problems can have many valid outputs, which poses a fundamental barrier to standard quantum lower-bound techniques. We overcome this by developing a novel method based on matrix discrepancy, which allows us to bound the output measurements of a quantum protocol jointly.

As applications of our method, we establish the first tight quantum lower bounds for two fundamental search problems in some natural parameter regimes: collision finding and triangle finding. For collision finding, we prove a tight $\Omega(N^{1/4})$ one-way quantum communication lower bound. Previously, the best-known quantum communication lower bound for collision finding was $\Omega(N^{1/12})$ due to Göös and Jain (RANDOM 2022), and no stronger bound was known even under the one-way restriction. For triangle finding in graph streams, we prove a one-pass quantum streaming space lower bound of $\Omega\left(\sqrt{\Delta_V}\right)$ for graphs with m edges, $\Theta(m)$ triangles, and constant Δ_E, where Δ_V and Δ_E denote the maximum number of triangles sharing a common vertex and edge, respectively. This constitutes the first nontrivial quantum space lower bound in this regime, matching the classical upper bound of Jayaram and Kallaugher (RANDOM 2021) up to logarithmic factors. Notably, our method also recovers the classical lower bound of Kallaugher and Price (SODA 2017) through an entirely different argument, avoiding their Boolean-Hidden-Matching reduction that breaks down for quantum protocols.

*Institute of Software, Chinese Academy of Sciences, and University of Chinese Academy of Sciences. Email: gaomb@ios.ac.cn or gmb17@tsinghua.org.cn.

†Institute of Software, Chinese Academy of Sciences, and University of Chinese Academy of Sciences. Email: liuch.russell@gmail.com

‡University of Southern California. Email: guangxuy@usc.edu. Research supported by NSF CAREER award 2141536.

§State Key Laboratory for Novel Software Technology, Nanjing University, Email: tianyiz25@nju.edu.cn. Research supported by the Fundamental and Interdisciplinary Disciplines Breakthrough Plan of the Ministry of Education of China (No. JYB2025XDXM118) and the "111 Center" (No. B26023).

ISSN 1433-8092

1 Introduction

One-way quantum communication asks how many qubits Alice must send in a single message for Bob to solve a two-party task with bounded error. Alice, given an input x, encodes it as a quantum state and sends it to Bob; Bob, given his own input y, chooses a measurement and outputs either a value $f(x, y)$ or, for a search relation, a witness that is valid for the pair (x, y). Proving lower bounds in this model is a fundamental task with many applications, including quantum streaming lower bounds [NT17, Kal22, AD24], extension complexity [FMP+12, LRS15], the Matrix Spencer problem [HRS22], coding theory [Nay99, ANTSV02, KdW04], and quantum finite automata [Nay99, ANTSV02, Kla07b].

For total and partial Boolean functions, several powerful lower-bound techniques are available. Quantum information complexity methods are particularly useful for bounded-round quantum communication [JRS03b, BGK+18] and amortized lower bounds [JRS03a, Tou15]. Norm and rank methods [Raz03, Kla07a, LS09b, LS09a], including approximate-degree-to-approximate-rank lifting [SZ09, LZ10, She11], give lower bounds for composed Boolean functions. Fourier-analytic methods, especially matrix-valued hypercontractive inequalities, provide another approach to one-way quantum communication lower bounds [BARdW08] and have been extended to quantum streaming lower bounds [KP22, AD24]. At a high level, these techniques turn a protocol into a single object to be bounded, such as an acceptance operator, a sign matrix, or a matrix-valued Boolean function. This fits decision problems, where each input pair has one target bit and Bob's measurement can be summarized by its acceptance probability.

Search relations with many valid outputs pose a different challenge. Here Bob is not merely deciding one predicate. For each Bob input, his quantum strategy can be described as a positive operator-valued measure (POVM) over a large output space, and correctness is the total probability assigned to the subset of witnesses that are valid for the joint input. Thus, a lower bound must control how an entire family of POVM elements can correlate with a witness set determined jointly by Alice and Bob. Existing Boolean-function techniques often do not apply to this object directly, and decision-to-search reductions may lose polynomial factors. For instance, in collision finding, the previous quantum lower bound obtained through decision-to-search reductions was only $\Omega(N^{1/12})$, far below the birthday-paradox upper bound $\widetilde{O}(N^{1/4})$[1] [GJ22]. These limitations motivate the following question:

> *Can we develop direct techniques for proving one-way quantum communication lower bounds for natural search problems?*

In this paper, we answer this question affirmatively by proposing a measurement-discrepancy method. Instead of reducing the search task to a Boolean decision problem, we analyze Bob's quantum strategy directly through the positive operator-valued measures (POVMs) associated with his inputs. In our applications, the Bob-side validity condition can be transformed into packing constraints of positive semidefinite (PSD) operators. After subtracting the trivial strategy baseline, the success probability is upper bounded by a matrix-discrepancy quantity: the expected operator norm of a centered random matrix sum under PSD packing constraints. We prove the required discrepancy bounds using noncommutative Khintchine inequalities and matrix concentration estimates, yielding the desired one-way quantum lower bounds.

This viewpoint is inspired by the connection between one-way quantum communication and matrix discrepancy in [HRS22], but our use is different. Their work derives matrix-discrepancy

[1] Throughout the paper, $\widetilde{O}$ and $\widetilde{\Omega}$ suppress poly-logarithmic factors.

bounds from quantum communication protocols; here, on the contrary, discrepancy estimates are used inside the lower-bound proof to control the success probability of quantum search protocols.

We apply our method to two representative search problems with many valid outputs: *collision finding*, where Bob must output a common collision certified jointly by Alice's and Bob's inputs, and *streaming triangle finding*, where the algorithm must output an actual triangle in a graph stream. For collision finding, we obtain an $\Omega(N^{1/4})$ one-way quantum lower bound, matching the birthday-paradox upper bound in the $M = N + \Omega(N)$ regime. For triangle finding, we prove an $\Omega(m\sqrt{\Delta_V}/T)$ one-pass quantum streaming lower bound on a hard family with $T = \Theta(m)$, $\Delta_E = O(1)$, and $1 \le \Delta_V \le m^{2/3}$, recovering the classical $\sqrt{\Delta_V}$ dependence in the quantum setting where the known reduction to Boolean-Hidden-Matching route is unavailable.

1.1 Our Results

Collision finding. For integers M, N with $\sqrt{N} \in \mathbb{N}$, the bipartite collision-finding problem $\mathsf{ColFind}_{N,M}$ is defined as follows. Alice receives $x = (x_1, \ldots, x_M) \in [\sqrt{N}]^M$, Bob receives $y = (y_1, \ldots, y_M) \in [\sqrt{N}]^M$, and Bob must output a pair $i < j$ satisfying $x_i = x_j$ and $y_i = y_j$.

Theorem 1.1. *For $M > N$, every one-way quantum protocol that solves $\mathsf{ColFind}_{N,M}$ with constant success probability over independent uniform inputs must send $\Omega(N^{1/4})$ qubits.*

The main difficulty of proving the above theorem lies in the regime $M = N + \Omega(N)$. When $M = N + o(N)$, Itsykson and Riazanov [IR21] proved a tight $\Omega(\sqrt{N})$ quantum one-way lower bound via a randomized reduction from set disjointness. For $M = N + \Omega(N)$, Göös and Jain [GJ22] gave a $\widetilde{O}(N^{1/4})$ birthday-paradox protocol, but only proved an $\Omega(N^{1/12})$ quantum lower bound, even for one-way protocols. Yang and Zhang [YZ24] later obtained the matching $\widetilde{\Omega}(N^{1/4})$ lower bound classically via density increments, but their argument does not extend to quantum communication; nor does the standard quantum information-complexity approach seem to suffice [BFM18]. Our theorem closes this gap with an $\Omega(N^{1/4})$ one-way quantum lower bound, tight up to logarithmic factors in the hard regime.

Triangle finding in graph streams. For a simple undirected graph G, let T be its number of triangles, Δ_E the maximum number of triangles sharing an edge, and Δ_V the maximum number sharing a vertex. In triangle-finding streaming problem, a one-pass quantum algorithm receives an arbitrary-order insertion stream of G's edges and must output a triangle.

Theorem 1.2. *Every one-pass quantum streaming algorithm that outputs a triangle with success probability greater than $2/3$ uses $\Omega\big(\sqrt{\Delta_V}\big)$ qubits of space on a hard family of graphs with m edges, $T = \Theta(m)$, $\Delta_E = O(1)$, and $1 \le \Delta_V \le m^{2/3}$.*

In our parameter regime, it matches the general classical space bound $\widetilde{O}\left((m/T)(\Delta_E + \sqrt{\Delta_V})\right) = \widetilde{O}(\sqrt{\Delta_V})$ of Jayaram and Kallaugher [JK21], which is tight up to logarithmic factors.[2] Thus, in this regime, triangle finding admits no quantum space advantage.

On the lower-bound side, the quantum lower bound that follows from the reduction to INDEX is only $\Omega(m\Delta_E/T)$[ANTSV02, BOV13, Kal22], which is merely a constant in our parameter setting $T = \Theta(m)$ and $\Delta_E = O(1)$. Under this choice of graph parameters, there has been an $\Omega(\sqrt{\Delta_V})$ classical lower bound [KP17] via reduction to Boolean Hidden Matching, but it does not hold in the quantum setting because Boolean Hidden Matching admits exponentially efficient one-way quantum protocols [GKK+07, BYJK08].

[2] They give this upper bound for triangle counting, which is related but distinct from triangle finding. However, their sampling procedure can be extended to triangle finding with the same asymptotic space bound.

1.2 Technical Overview

The common idea: from search protocols to matrix discrepancy. The starting point of our proofs is to treat Bob's whole output *measurement* as the object to be bounded. Consider a one-way quantum protocol for a search relation $R \subseteq \mathcal{A} \times \mathcal{B} \times \mathcal{Z}$. On Alice's input $a \in \mathcal{A}$, Alice sends a d-dimensional quantum state ρ_a; on Bob's input $b \in \mathcal{B}$, Bob applies a POVM $\{M_z^{(b)}\}_{z \in \mathcal{Z}}$. For a fixed Alice input a, define the averaged success operator

$$H_a := \mathbb{E}_b \sum_{z \in \mathcal{Z}} \mathbf{1}[(a, b, z) \in R]\, M_z^{(b)}.$$

The success probability conditioned on a is $\mathrm{Tr}(\rho_a H_a)$, and therefore

$$p_{\mathrm{succ}} \leq \mathbb{E}_a \|H_a\|.$$

Thus, rather than reducing the search problem to a Boolean decision problem, we directly upper bound the largest eigenvalue of the operator collecting all successful outputs.

The main structural step is to separate the Alice-side and Bob-side parts of the validity condition before bounding the protocol. For each possible output $z \in \mathcal{Z}$, we introduce a finite set Ω_z of refined witnesses associated with z. We take these sets to be disjoint and write

$$\Omega := \bigsqcup_{z \in \mathcal{Z}} \Omega_z.$$

In our applications, the validity indicator factors as

$$\mathbf{1}[(a, b, z) \in R] = \sum_{\omega \in \Omega_z} X_\omega(a) Y_\omega(b),$$

where $X_\omega(a)$ depends only on Alice's input and $Y_\omega(b)$ depends only on Bob's input. Thus $\omega \in \Omega_z$ should be read as a refined way in which the output z can be certified as valid. In the refinements used below, the Bob-side factors are nonnegative and satisfy $\sum_{\omega \in \Omega_z} Y_\omega(b) \leq 1$ for every fixed b and z.

We absorb the Bob-side factor into Bob's POVM: for every $z \in \mathcal{Z}$ and $\omega \in \Omega_z$, define

$$P_\omega := \mathbb{E}_b \left[Y_\omega(b) M_z^{(b)} \right].$$

Then

$$H_a = \sum_{z \in \mathcal{Z}} \sum_{\omega \in \Omega_z} X_\omega(a) P_\omega = \sum_{\omega \in \Omega} X_\omega(a) P_\omega.$$

The operators P_ω are positive semidefinite and satisfy packing constraints from POVM normalization:

$$P_\omega \succeq 0, \qquad \sum_{\omega \in \Omega} P_\omega = \mathbb{E}_b \sum_{z \in \mathcal{Z}} \sum_{\omega \in \Omega_z} Y_\omega(b) M_z^{(b)} \preceq I.$$

In our applications, each P_ω also has an upper bound $P_\omega \preceq \beta I$: in collision finding, $\beta = 1/\sqrt{N}$; in triangle finding, $\beta = 1/s$. The global packing constraint prevents Bob's POVM from placing large total mass on many possible witnesses, while the pointwise bound prevents a single Bob-valid measurement operator from dominating after the Bob-side randomness has been averaged out.

We observe that, the contribution of $\mathbb{E}X_\omega$ is the trivial guessing baseline. After subtracting this baseline, the remaining advantage is captured by the centered operator

$$G_a = \sum_{\omega \in \Omega} \big(X_\omega(a) - \mathbb{E}X_\omega\big) P_\omega.$$

The lower-bound task is therefore to prove that $\mathbb{E}_a \|G_a\|$ is small for every PSD packing that could be produced by Bob's POVM. Although Bob's measurement is completely arbitrary and protocol-dependent, the proof uses only the packing constraints forced by POVM normalization and the Bob-side validity condition.

This is where matrix discrepancy enters. The centered variables $X_\omega(a) - \mathbb{E}X_\omega$ play the role of random signs or centered random coefficients, while the operators P_ω form a packed family of matrices. We bound the resulting random matrix sum using a noncommutative Khintchine inequality, which reduces the problem to controlling the largest grouped operator norm in the packing. This final control is obtained by a matrix concentration argument tailored to the combinatorics of the problem. In collision finding, the grouping comes from buckets of equal labels after a decoupling step; in triangle finding, it comes from the hidden block structure induced by random bijections. Thus both lower bounds follow the same route: convert the search measurement into a PSD packing, subtract the baseline success, and bound the centered advantage by a matrix-discrepancy estimate.

Collision finding: decoupling collision indicators into buckets. We first illustrate the method on collision finding. Alice and Bob receive independent strings $x, y \in [\sqrt{N}]^M$, and Bob must output a pair $i < j$ such that $x_i = x_j$ and $y_i = y_j$. For Bob's POVM $\{M_{i,j}^{(y)}\}_{i<j}$, we absorb the Bob-side collision condition into the measurement by defining

$$P_{i,j} := \mathbb{E}_y\big[\mathbf{1}[y_i = y_j] M_{i,j}^{(y)}\big].$$

The POVM normalization and $\mathbb{E}[\mathbf{1}[y_i = y_j]] = \frac{1}{\sqrt{N}}$ immediately imply

$$P_{i,j} \succeq 0, \qquad P_{i,j} \preceq \frac{1}{\sqrt{N}} I, \qquad \sum_{i<j} P_{i,j} \preceq I.$$

For a fixed Alice input x, the success operator is given by

$$H_x = \sum_{i<j} \mathbf{1}[x_i = x_j] P_{i,j}.$$

Centering the Alice-side collision indicators gives

$$H_x = \frac{1}{\sqrt{N}} \sum_{i<j} P_{i,j} + \sum_{i<j} \left(\mathbf{1}[x_i = x_j] - \frac{1}{\sqrt{N}}\right) P_{i,j}.$$

The first term is bounded by $I/\sqrt{N}$, which is the trivial guessing contribution. Hence, it remains to bound the operator norm of the centered discrepancy

$$G_x := \sum_{i<j} \left(\mathbf{1}[x_i = x_j] - \frac{1}{\sqrt{N}}\right) P_{i,j}.$$

The indicators $\mathbf{1}[x_i = x_j]$ are highly dependent because different pairs may share common coordinates. To expose independent randomness, we randomly bipartition the index set into $(L \cup R)$ and keep only the cross pairs. It suffices, up to a constant factor, to bound the cross term

$$S_{L,R}(x) := \sum_{i \in L} \sum_{j \in R} \left(\mathbf{1}[x_i = x_j] - \frac{1}{\sqrt{N}} \right) P_{i,j}.$$

After conditioning on the labels on the right side, define the bucket operators

$$B_{i,c} := \sum_{j \in R : x_j = c} P_{i,j}, \qquad B_i := \frac{1}{\sqrt{N}} \sum_{c \in [\sqrt{N}]} B_{i,c}.$$

Then the cross term becomes

$$S_{L,R}(x) = \sum_{i \in L} \big(B_{i,x_i} - B_i \big),$$

where the remaining randomness comes from the independent labels $(x_i)_{i \in L}$. A matrix Khintchine inequality bounds this centered sum in terms of the largest bucket norm

$$Z := \max_{i \in L,\ c \in [\sqrt{N}]} \|B_{i,c}\|.$$

The packing condition implies $\sum_{i,c} B_{i,c} \preceq I$, while a matrix Chernoff argument over the right-side labels gives

$$\mathbb{E} Z \lesssim \frac{\log d + \log N}{\sqrt{N}}.$$

Consequently,

$$\mathbb{E}_x \|G_x\| \lesssim \sqrt{\frac{\log d (\log d + \log N)}{\sqrt{N}}}.$$

Combining this with the baseline term yields

$$p_{\text{succ}} \leq \frac{1}{\sqrt{N}} + O\left(\sqrt{\frac{\log d (\log d + \log N)}{\sqrt{N}}} \right).$$

Since $d = 2^k$, any protocol with constant success probability must satisfy $k = \Omega(N^{1/4})$, giving the desired one-way quantum lower bound for collision finding.

Triangle finding: hidden blocks and concentration over bijections. The second application, triangle finding, uses the same proof method after a streaming-to-communication reduction. The communication problem arising from our hard distribution is denoted by $\mathsf{TripTri}(r, s)$. Alice holds random bijections $F_i : X \to Z_i$ for $i \in [s]$ and a random matrix $A : X \times Y \to \{0, 1\}$, while Bob holds a random bijection $C : [s] \to Y$. Bob must output a triple (x, i, z) satisfying

$$z = F_i(x) \qquad \text{and} \qquad A_{x,C(i)} = 1.$$

In the streaming reduction, Alice inserts the XZ- and XY-edges and sends the memory state of the streaming algorithm to Bob; Bob then inserts the YZ-edges. Any triangle output by the streaming algorithm gives exactly such a witness.

The quantum lower bound for $\mathsf{TripTri}(r, s)$ mirrors the collision argument. For Bob's POVM $M^C_{x,i,z}$, define the averaged success operator

$$H_{F,A} := \mathbb{E}_C \sum_{x\in X} \sum_{i=1}^{s} A_{x,C(i)} M^C_{x,i,F_i(x)}.$$

Writing $A_{x,y} = 1/2 + \eta_{x,y}$ separates the trivial baseline from the advantage. The constant part contributes at most $I/2$, and the centered part is

$$G_{F,A} := \mathbb{E}_C \sum_{x\in X} \sum_{i=1}^{s} \eta_{x,C(i)} M^C_{x,i,F_i(x)}.$$

As before, the goal is to bound $\mathbb{E}_{F,A}\|G_{F,A}\|$. To expose the matrix-discrepancy structure, define

$$P_{x,i,z,y} := \mathbb{E}_C \left[\mathbf{1}_{C(i)=y} M^C_{x,i,z}\right].$$

These matrices form a PSD packing: each $P_{x,i,z,y}$ is positive semidefinite and the total mass is bounded by the identity. With

$$Q_{x,y}(F) := \sum_{i=1}^{s} P_{x,i,F_i(x),y},$$

the centered operator becomes

$$G_{F,A} = \sum_{x\in X} \sum_{y\in Y} \eta_{x,y} Q_{x,y}(F).$$

It remains to control the block norms $\max_{x,y} \|Q_{x,y}(F)\|$. This is where the random bijections $F_1, \ldots, F_s$ are used: they spread the packed measurement mass across the r vertices inside each block, and a matrix concentration bound shows that no block $Q_{x,y}(F)$ is too large on average. Combined with the matrix Khintchine bound for the centered signs $\eta_{x,y}$, this gives the desired upper bound on $\mathbb{E}_{F,A}\|G_{F,A}\|$.

1.3 Related Work

1.3.1 Communication Lower Bounds for Collision Finding.

Collision finding is a basic search problem at the interface of communication complexity [GJ22], cryptography [BFM18], proof complexity [IR21], and quantum algorithms [BHT98]. In the query model, the problem has a well-understood quantum complexity: the Brassard–Høyer–Tapp algorithm [BHT98] finds a collision in an r-to-one function using $O((N/r)^{1/3})$ queries, and this bound was shown to be optimal by Shi [Shi02], improving Aaronson's earlier lower bound [Aar02].

Communication versions of collision finding have emerged more recently from several independent motivations. Bauer, Farshim, and Mazaheri introduced related communication tasks in their study of backdoored random oracles, where communication lower bounds imply security of hash combiners [BFM18]. Itsykson and Riazanov studied collision-type search problems arising from the bit-pigeonhole principle and used communication lower bounds to derive proof-complexity lower bounds[IR21]. Göös and Jain [GJ22] subsequently introduced a natural two-party bipartite collision problem, in which Alice and Bob hold complementary parts of the binary encoding of each item, and proved the first polynomial lower bound, $\Omega(N^{1/12})$, even for quantum communication protocols. They also observed an $O(N^{1/4} \log N)$ birthday-paradox protocol and conjectured it to

be essentially optimal. For classical randomized communication, this conjecture was resolved by Yang and Zhang, who proved a tight $\widetilde{\Omega}(N^{1/4})$ lower bound via density-increment arguments [YZ24]. Recent work of Beame and Whitmeyer further extended collision-finding lower bounds to multi-party number-in-hand communication, with applications to cutting-plane lower bounds for concise pigeonhole principles [BW25].

1.3.2 Streaming Lower Bounds for Triangle Finding

Triangle finding is a canonical subgraph problem that appears far beyond streaming algorithms, serving as a structural primitive in graph algorithms [IR78, AYZ97], fine-grained complexity [RVW11, VWW18], database theory [NPRR12], quantum algorithms [MSS07, LMS13, LG14], property testing [AKKR08], distributed computing [ILG17, CPZ19, ILGM20], and network analysis [MSOI+02, SW05, Lat08, SV11]. These connections make triangle finding a natural problem for understanding the power and limitations of quantum streaming algorithms.

Triangle counting and detection in graph streams. Most of the streaming literature on triangles has focused on numerical or Boolean versions of the problem: estimating the number of triangles, or distinguishing triangle-free graphs from graphs containing many triangles. Bar-Yossef, Kumar, and Sivakumar initiated the use of communication reductions for triangle counting in streams [BYKS02]. Subsequent work refined both the algorithms and the parameterized lower bounds for this problem [BOV13, CJ17, BC17]. A convenient parameterization, now standard in this line of work, uses the number of triangles T, the maximum number Δ_E of triangles sharing an edge, and the maximum number Δ_V of triangles sharing a vertex. Braverman, Ostrovsky, and Vilenchik proved an $\Omega(m\Delta_E/T)$ lower bound [BOV13]. Kallaugher and Price gave the complementary $\Omega(m\sqrt{\Delta_V}/T)$ lower bound and a hybrid sampling algorithm [KP17]. Jayaram and Kallaugher later obtained the optimal one-pass insertion-stream algorithm, with space $\widetilde{O}\left(\frac{m}{T}(\Delta_E + \sqrt{\Delta_V})\right)$, matching these lower bounds up to logarithmic factors [JK21]. Related linear-sketching and hypergraph-counting variants were studied by Kallaugher, Kapralov, and Price [KKP18].

Quantum streaming algorithms for triangle counting. The problem in the quantum setting is quite different. The $\Omega(m\Delta_E/T)$ lower bound continues to hold in the quantum streaming model, because it is based on the INDEX problem, or equivalently on quantum random-access-code lower bounds [ANTSV02, BOV13]. In contrast, the classical $\Omega(m\sqrt{\Delta_V}/T)$ lower bound of Kallaugher and Price [KP17] goes through Boolean Hidden Matching, which has exponentially more efficient one-way quantum protocols [BYJK08, GKK+07]. The missing $\sqrt{\Delta_V}$ quantum lower bound for triangle counting is not merely a limitation of existing proof techniques: a quantum lower bound matching the classical $\Omega(m\sqrt{\Delta_V}/T)$ term cannot hold in general, since Kallaugher gave a one-pass quantum streaming algorithm for triangle counting using

$$\widetilde{O}\left(\frac{m^{8/5}\Delta_E^{4/5}}{T^{6/5}}\right)$$

space, which is polynomially smaller than the optimal classical bound in some parameter regimes [Kal22]. For example, when $\Delta_E = O(1)$ and $\Delta_V = \Omega(T) = \Omega(m)$, this gives $\widetilde{O}(m^{2/5})$ space, whereas the classical lower bound is $\widetilde{\Omega}(m^{1/2})$. More recent work abstracts the design of such quantum streaming algorithms and gives a more modular way to derive quantum streaming upper bounds [KPV25]. Together, these results show that triangle problems in quantum streams exhibit a subtly different parameter dependence from their classical counterparts.

1.4 Open Problems

Our results naturally suggest several directions for future work.

- First, it remains open to obtain a *complete* parameterized lower bound for quantum triangle finding. We prove an $\Omega(\sqrt{\Delta_V})$ one-pass lower bound in the regime $T = \Theta(m)$, $\Delta_E = O(1)$, and $1 \le \Delta_V \le m^{2/3}$. A natural goal is to understand whether the optimal one-pass quantum space complexity matches the classical bound

$$\widetilde{\Theta}\Big(\frac{m}{T}(\Delta_E + \sqrt{\Delta_V})\Big)$$

  throughout all parameter regimes.

- Second, it would be interesting to understand the multi-pass quantum triangle finding. Our reduction is one-pass and yields a one-way quantum communication problem; a p-pass algorithm would correspond to a p-round communication protocol, which is not covered by our current matrix-discrepancy argument. Classically, triangle counting admits strong multi-pass lower bounds, for example

$$\Omega\Big(\min\{m^{3/2}/T,\, m/\sqrt{T}\}\Big)$$

  up to pass-dependent factors [BC17]. This raises the question of whether similar multi-pass quantum lower bounds hold for triangle finding or triangle counting, or whether quantum multi-pass streaming algorithms can achieve a space advantage in some parameter regime.

- In addition, another direction is to see if the measurement-discrepancy method can be extended to multiparty communication models. A natural setting is the k-party number-in-hand version of collision finding studied by Beame and Whitmeyer [BW25]: player r receives $x^{(r)} \in [q]^M$, and the players must output a pair $i \neq j$ such that

$$x_i^{(r)} = x_j^{(r)} \qquad \text{for every } r \in [k].$$

  Their work gives nearly tight randomized communication lower bounds for this problem. Can one prove analogous lower bounds for quantum multiparty protocols?

2 Preliminaries

We write $[n] := \{1, \dots, n\}$ and denote by S_n the symmetric group on $[n]$. All logarithms are natural unless stated otherwise. We say $A \succeq 0$ if A is positive semidefinite. For Hermitian matrices A and B of the same dimension, we write $A \preceq B$ if $B - A$ is positive semidefinite. The norm $\|A\|$ denotes the spectral norm, and I denotes the identity operator on the underlying Hilbert space. A density matrix is a positive semidefinite operator with trace one. All Hilbert spaces appearing in our proofs are finite-dimensional.

We shall use the following two standard estimates repeatedly. The first is the contraction principle for Rademacher sums in Banach spaces.

Lemma 2.1 ([LT91, Theorem 4.4])**.** *Let B be a Banach space, let $x_a \in B$, and let ε_a be independent Rademacher signs. If $\alpha_a \in \mathbb{R}$ satisfy $|\alpha_a| \le L$, then*

$$\mathbb{E}_\varepsilon \Big\| \sum_a \varepsilon_a \alpha_a x_a \Big\|_B \le L\, \mathbb{E}_\varepsilon \Big\| \sum_a \varepsilon_a x_a \Big\|_B .$$

The second estimate is the self-adjoint matrix Khintchine inequality, which controls the spectral norm of a random signed sum of fixed self-adjoint matrices.

Lemma 2.2 (See [Tro15, Section 4.7.2], see also [Ver18, Theorem 5.4.14]). *Let A_a be fixed self-adjoint operators on a d-dimensional Hilbert space, and let ε_a be independent Rademacher signs. Then, for some sufficiently large constant K, we have:*

$$\mathbb{E}_\varepsilon \left\| \sum_a \varepsilon_a A_a \right\| \le K \sqrt{\log(2d)} \left\| \left(\sum_a A_a^2 \right)^{1/2} \right\|.$$

We use the following standard scalar Chernoff bound.

Lemma 2.3. *Let $X_1, \dots, X_n$ be independent random variables taking values in $[0,1]$, and let $X = \sum_{i=1}^n X_i$ and $\mathbb{E}[X] = \mu$. Then, for every $\delta \in (0,1)$,*

$$\Pr\left[|X - \mu| \ge \delta\mu\right] \le 2\exp(-\delta^2\mu/3).$$

Graph notations Let $G = (V, E)$ be a finite, simple, and undirected graph, where $V(G)$ and $E(G)$ denote the vertex set and edge set, respectively. We denote the set of all triangles in G by $\mathrm{Tri}(G)$, and write the number of triangles in G as

$$T(G) := |\mathrm{Tri}(G)|.$$

We define the maximum edge-triangle degree of G as

$$\Delta_E(G) := \max_{e \in E(G)} |\{\tau \in \mathrm{Tri}(G) : e \subseteq \tau\}|.$$

and the maximum vertex-triangle degree of G as

$$\Delta_V(G) := \max_{v \in V(G)} |\{\tau \in \mathrm{Tri}(G) : v \in \tau\}|.$$

For simplicity, whenever the underlying graph G is unambiguous from the context, we suppress the explicit dependence and simply write T, Δ_E, and Δ_V.

Definition 2.4 (Collision finding). *Assume that $\sqrt{N}$ is an integer, and there is an integer $M > N$. Alice receives $x = (x_1, \dots, x_M) \in [\sqrt{N}]^M$ and Bob receives $y = (y_1, \dots, y_M) \in [\sqrt{N}]^M$. Alice sends a single quantum message to Bob. Bob must output a pair $i < j$ such that $x_i = x_j$ and $y_i = y_j$.*

Definition 2.5 (Triangle finding). *In the one-pass insertion-only graph-stream version of triangle finding, the input is an arbitrary-order stream of the edges of a finite simple graph $G = ([n], E)$. After processing the stream, the algorithm outputs either a triple of vertices $\tau = \{u, v, w\} \subseteq [n]$ or a failure symbol $\perp$. The output is valid if and only if $\tau \in \mathrm{Tri}(G)$, equivalently all three edges $\{u,v\}, \{u,w\}, \{v,w\}$ belong to E. In parameterized statements, we restrict the input graph by its number of edges $m = |E|$, number of triangles $T(G)$, maximum edge-triangle degree $\Delta_E(G)$, and maximum vertex-triangle degree $\Delta_V(G)$.*

2.1 Quantum Computing

In this paper, we only consider finite-dimensional Hilbert space. A qubit is a quantum system described by a two-dimensional complex Hilbert space $\mathbb{C}^2$, with computational basis written in Dirac notation as $|0\rangle$ and $|1\rangle$; a pure qubit state is a unit vector $\alpha|0\rangle + \beta|1\rangle \in \mathbb{C}^2$, where $|\alpha|^2 + |\beta|^2 = 1$. Moreover, a k-qubit system has state space $(\mathbb{C}^2)^{\otimes k} \cong \mathbb{C}^{2^k}$, with computational basis $\{|x\rangle : x \in \{0,1\}^k\}$. A pure state is a unit vector $|\psi\rangle$ and is identified with the rank-one density operator $|\psi\rangle\langle\psi|$. More generally, a mixed state on a Hilbert space $\mathcal{H}$ is a density operator which is positive semidefinite and has trace one, and we write the set of all density operators on $\mathbb{H}$ as

$$\mathsf{D}(\mathcal{H}) := \{\rho \succeq 0 : \mathrm{Tr}(\rho) = 1\}.$$

A quantum channel is a completely positive trace-preserving linear map between operator spaces. Measurements in this paper are described by POVMs, recalled next.

Definition 2.6 (Positive Operator-Valued Measure)**.** *Let $\mathcal{H}$ be a d-dimensional Hilbert space representing the state space of k qubits, where $d = 2^k$. Let Ω be a finite set of measurement outcomes. A* Positive Operator-Valued Measure (POVM) *on Ω is a collection of positive semidefinite operators $\{M_\omega\}_{\omega\in\Omega}$ acting on $\mathcal{H}$ that satisfies:*

$$M_\omega \succeq 0 \quad \forall \omega \in \Omega, \tag{1}$$

and the completeness relation:

$$\sum_{\omega\in\Omega} M_\omega = I. \tag{2}$$

If a POVM $\{M_\omega\}_{\omega\in\Omega}$ is measured on a state ρ, then the probability of outcome ω is $\mathrm{Tr}(M_\omega\rho)$.

Quantum one-way protocols for search relations Let $\mathcal{A}$ and $\mathcal{B}$ be Alice's and Bob's input spaces, $\mathcal{Z}$ be the output space, and $R \subseteq \mathcal{A}\times\mathcal{B}\times\mathcal{Z}$ be a relation. An output $z \in \mathcal{Z}$ is valid on input (a,b) if and only if $(a,b,z) \in R$.

Definition 2.7 (Quantum one-way communication complexity)**.** *Let $R \subseteq \mathcal{A}\times\mathcal{B}\times\mathcal{Z}$ be a relation, and let $\varepsilon \in [0,1]$. We assume that Alice and Bob share no prior entanglement.*

A quantum one-way protocol Π of message dimension d consists of the following parts:

1. *For each input $a \in \mathcal{A}$, Alice prepares a density operator*

$$\rho_a \in \mathsf{D}(\mathbb{C}^d)$$

and sends it to Bob.

2. *For each input $b \in \mathcal{B}$, Bob performs a POVM*

$$M^{(b)} = \{M_z^{(b)}\}_{z\in\mathcal{Z}}$$

on $\mathbb{C}^d$, where $M_z^{(b)} \succeq 0$ and $\sum_{z\in\mathcal{Z}} M_z^{(b)} = I_d$. On inputs (a,b), the protocol outputs $z \in \mathcal{Z}$ with probability

$$\Pr[z \mid a,b] = \mathrm{Tr}\left(M_z^{(b)}\rho_a\right).$$

The quantum one-way communication cost of Π is $\log_2 d$.

We consider distributional one-way quantum communication protocols for search relations. Let μ be an input distribution on $\mathcal{A}\times\mathcal{B}$. The success probability of the protocol under μ is

$$p_{\mathrm{succ}} = \mathbb{E}_{(a,b)\sim\mu} \sum_{z\in\mathcal{Z}} \mathbf{1}\{(a,b,z) \in R\}\, \mathrm{Tr}\left(M_z^{(b)}\rho_a\right).$$

Quantum streaming algorithms A quantum streaming algorithm for a graph problem has sequential access to an edge stream

$$e_1, e_2, \ldots, e_m,$$

where each e_i is an edge of an input graph $G = ([n], E)$. The algorithm processes the edges from left to right using a limited quantum workspace. The edges may arrive in an arbitrary, possibly adversarial, order.

First, the algorithm receives the number of vertices n and the number of edges m. It then initializes a quantum work register W, consisting of $s(n)$ qubits, to a fixed state ρ_0, typically

$$\rho_0 = |0^{s(n)}\rangle \langle 0^{s(n)}| .$$

For each possible edge $e \in \binom{[n]}{2}$, the algorithm has a corresponding quantum channel $\mathcal{A}_e$ acting on W. As the edge stream is processed, the state of the work register evolves as

$$\rho_i = \mathcal{A}_{e_i}(\rho_{i-1}), \qquad i = 1, 2, \ldots, m.$$

After the last edge is processed, the algorithm measures the work register W. Based on the measurement outcome, it outputs a value Z, which may be a decision, an estimate, or another quantity determined by the graph problem.

Throughout this framework, the space complexity of the algorithm is the number of qubits $s(n)$ stored in the work register between two consecutive edge arrivals. We place no restriction on the running time or computational complexity of the quantum update channels. We also allow the algorithm read-only access to public random bits; these random bits are not stored in the work register and are not charged to the streaming space.

3 Quantum Communication Lower Bound for Collision Finding

In this section, we prove a one-way quantum communication lower bound for the collision-finding problem. We begin by establishing the matrix discrepancy estimate and the matrix Chernoff bound that will be used in the proof.

3.1 Matrix Discrepancy and Matrix Chernoff Bound

Lemma 3.1. *Let $\mathcal{A}$ and $\mathcal{C}$ be finite sets. Let $\{R_{a,c} : a \in \mathcal{A},\ c \in \mathcal{C}\}$ be positive semidefinite operators on a d-dimensional Hilbert space such that*

$$\sum_{a \in \mathcal{A}} \sum_{c \in \mathcal{C}} R_{a,c} \preceq I.$$

For each $a \in \mathcal{A}$, set $\overline{R}_a := \frac{1}{|\mathcal{C}|} \sum_{c \in \mathcal{C}} R_{a,c}$ and $Z := \max_{a \in \mathcal{A},\ c \in \mathcal{C}} \|R_{a,c}\|$. Let $u = (u_a)_{a \in \mathcal{A}}$, where the u_a's are independent and uniformly distributed on $\mathcal{C}$. Then

$$\mathbb{E}_u \left\| \sum_{a \in \mathcal{A}} (R_{a,u_a} - \overline{R}_a) \right\| \leq C \sqrt{\log(2d)} \sqrt{Z},$$

where $C > 0$ is a universal constant.

Proof. Let $u' = (u'_a)_{a\in\mathcal{A}}$ be an independent copy of u. Since $\mathbb{E}_{u'_a}[R_{a,u'_a}] = \overline{R}_a$, by Jensen's inequality, we have

$$\mathbb{E}_u \left\| \sum_{a\in\mathcal{A}} (R_{a,u_a} - \overline{R}_a) \right\| = \mathbb{E}_u \left\| \mathbb{E}_{u'} \sum_{a\in\mathcal{A}} (R_{a,u_a} - R_{a,u'_a}) \right\| \le \mathbb{E}_{u,u'} \left\| \sum_{a\in\mathcal{A}} (R_{a,u_a} - R_{a,u'_a}) \right\|.$$

Let $(\varepsilon_a)_{a\in\mathcal{A}}$ be independent Rademacher signs. Specifically, they are independent of u, u'. By symmetry,

$$\mathbb{E}_{u,u'} \left\| \sum_{a\in\mathcal{A}} (R_{a,u_a} - R_{a,u'_a}) \right\| = \mathbb{E}_{u,u',\varepsilon} \left\| \sum_{a\in\mathcal{A}} \varepsilon_a (R_{a,u_a} - R_{a,u'_a}) \right\| \le 2\mathbb{E}_{u,\varepsilon} \left\| \sum_{a\in\mathcal{A}} \varepsilon_a R_{a,u_a} \right\|.$$

Conditioning on u, Lemma 2.2 applied with $A_a = R_{a,u_a}$ gives

$$\mathbb{E}_\varepsilon \left\| \sum_{a\in\mathcal{A}} \varepsilon_a R_{a,u_a} \right\| \le C_0 \sqrt{\log(2d)} \left\| \left(\sum_{a\in\mathcal{A}} R_{a,u_a}^2 \right)^{1/2} \right\|.$$

Since $0 \preceq R_{a,u_a} \preceq ZI$, we have $R_{a,u_a}^2 \preceq ZR_{a,u_a}$. Moreover, $\sum_{a\in\mathcal{A}} R_{a,u_a} \preceq \sum_{a\in\mathcal{A}} \sum_{c\in\mathcal{C}} R_{a,c} \preceq I$. Therefore

$$\sum_{a\in\mathcal{A}} R_{a,u_a}^2 \preceq ZI, \text{ and } \left\| \left(\sum_{a\in\mathcal{A}} R_{a,u_a}^2 \right)^{1/2} \right\| \le \sqrt{Z}.$$

Combining the estimates and absorbing the numerical factor into C proves the claim. □

To analyze the quantum protocol, we use a matrix Chernoff bound.

Lemma 3.2. *Let $\mathcal{A}, \mathcal{B}, \mathcal{C}$ be finite sets. For every $a \in \mathcal{A}$ and $b \in \mathcal{B}$, let $P_{a,b} \succeq 0$ be an operator on a d-dimensional Hilbert space. Suppose*

$$P_{a,b} \preceq \frac{1}{|\mathcal{C}|} I \qquad \text{for all } a, b, \text{ and } \sum_{a\in\mathcal{A}} \sum_{b\in\mathcal{B}} P_{a,b} \preceq I.$$

Let $v = (v_b)_{b\in\mathcal{B}}$, where v_b's are independent and uniformly distributed on $\mathcal{C}$. Define $R_{a,c}(v) := \sum_{b\in\mathcal{B}:\, v_b = c} P_{a,b}$ for $a \in \mathcal{A}$, $c \in \mathcal{C}$. Then

$$\mathbb{E}_v \max_{a\in\mathcal{A},\ c\in\mathcal{C}} \|R_{a,c}(v)\| \le C \frac{\log(2d) + \log(2|\mathcal{C}|)}{|\mathcal{C}|},$$

where $C > 0$ is a universal constant.

Proof. For each $a \in \mathcal{A}$ define the row sum $A_a := \sum_{b\in\mathcal{B}} P_{a,b}$. Then $A_a \succeq 0$, $A_a \preceq I$, and

$$\sum_{a\in\mathcal{A}} A_a = \sum_{a\in\mathcal{A}} \sum_{b\in\mathcal{B}} P_{a,b} \preceq I.$$

In particular, $\sum_{a\in\mathcal{A}} \operatorname{Tr}(A_a) \le d$. Let $L := \log(2d) + \log(2|\mathcal{C}|)$ and $\tau := \frac{L}{|\mathcal{C}|}$. For every row with $\|A_a\| \le \tau$, we have

$$\max_{c\in\mathcal{C}} \|R_{a,c}(v)\| \le \|A_a\| \le \tau$$

deterministically. It remains to control the rows with $\|A_a\| > \tau$. Let $\mathcal{A}_{\text{big}} := \{a \in \mathcal{A} : \|A_a\| > \tau\}$. Since $A_a \succeq 0$, $\mathrm{Tr}(A_a) \geq \|A_a\|$, and hence

$$|\mathcal{A}_{\text{big}}|\,\tau < \sum_{a \in \mathcal{A}_{\text{big}}} \mathrm{Tr}(A_a) \leq d.$$

Thus, $|\mathcal{A}_{\text{big}}| \leq d/\tau$. If $\mathcal{A}_{\text{big}}$ is empty, the maximum over big rows is zero, and only the deterministic small-row bound remains. Hence, we assume below that $\mathcal{A}_{\text{big}}$ is nonempty.

For fixed $a \in \mathcal{A}$ and $c \in \mathcal{C}$, the operators $\mathbf{1}_{\{v_b = c\}} P_{a,b}$ indexed by $b \in \mathcal{B}$ are independent and positive semidefinite. Since $\sum_{b \in \mathcal{B}} P_{a,b} \preceq I$, we have

$$\mathbb{E}_v[R_{a,c}(v)] = \frac{1}{|\mathcal{C}|} \sum_{b \in \mathcal{B}} P_{a,b} \preceq \frac{1}{|\mathcal{C}|} I.$$

Moreover, $0 \preceq \mathbf{1}_{\{v_b = c\}} P_{a,b} \preceq \frac{1}{|\mathcal{C}|} I$. By the matrix Chernoff bound, for every $u \geq 0$,

$$\Pr\left[\|R_{a,c}(v)\| \geq C_0 \frac{u + \log(2d) + 1}{|\mathcal{C}|}\right] \leq e^{-u},$$

where $C_0 > 0$ is a universal constant. Taking a union bound over the $|\mathcal{A}_{\text{big}}|\,|\mathcal{C}|$ choices of (a, c) with $a \in \mathcal{A}_{\text{big}}$ gives

$$\Pr\left[\max_{a \in \mathcal{A}_{\text{big}},\ c \in \mathcal{C}} \|R_{a,c}(v)\| \geq C_0 \frac{u + \log(2d) + \log(|\mathcal{A}_{\text{big}}|\,|\mathcal{C}|) + 1}{|\mathcal{C}|}\right] \leq e^{-u}.$$

Since $\tau = L/|\mathcal{C}|$ and $L \geq 1$,

$$\log(|\mathcal{A}_{\text{big}}|\,|\mathcal{C}|) \leq \log(d|\mathcal{C}|/\tau) = \log d + \log|\mathcal{C}| + \log(|\mathcal{C}|/L) \leq \log d + 2\log|\mathcal{C}|.$$

Integrating this tail bound over $u \geq 0$ yields

$$\mathbb{E}_v \max_{a \in \mathcal{A}_{\text{big}},\ c \in \mathcal{C}} \|R_{a,c}(v)\| \leq C \cdot \frac{\log(2d) + \log(2|\mathcal{C}|)}{|\mathcal{C}|},$$

after absorbing the additive constant into the universal constant C. Combining the deterministic bound on the small rows with the last inequality and absorbing $\tau = L/|\mathcal{C}|$ into the constant proves the claim. □

3.2 Proof of Theorem 1.1

Proof of Theorem 1.1. Let $\mathcal{I} = [M]$ and $\mathcal{C} = [\sqrt{N}]$. Alice and Bob receive independent uniform strings $x, y \in \mathcal{C}^{\mathcal{I}}$, and Bob must output a pair $i < j$ such that $x_i = x_j$ and $y_i = y_j$.

Fix a k-qubit one-way quantum protocol and put $d = 2^k$. On Alice's input x, Alice sends a density matrix ρ_x on $\mathbb{C}^d$. On Bob's input y, Bob performs a POVM

$$\mathcal{M}^{(y)} = \left\{M^{(y)}_{\{i,j\}} : \{i,j\} \in \tbinom{\mathcal{I}}{2}\right\}$$

where $M^{(y)}_{\{i,j\}} \succeq 0$ and $\sum_{\{i,j\} \in \binom{\mathcal{I}}{2}} M^{(y)}_{\{i,j\}} = I$. For fixed Alice input x, define the averaged success operator

$$H_x := \mathbb{E}_y \sum_{\{i,j\} \in \binom{\mathcal{I}}{2}} \mathbf{1}_{\{x_i = x_j\}} \mathbf{1}_{\{y_i = y_j\}} M^{(y)}_{\{i,j\}}.$$

The success probability conditioned on x is $\mathrm{Tr}(\rho_x H_x)$. Since ρ_x is a density matrix, $\mathrm{Tr}(\rho_x H_x) \leq \|H_x\|$. Therefore

$$p_{\mathrm{succ}} \leq \mathbb{E}_x \|H_x\|. \tag{3}$$

For each output pair $\{i,j\} \in \binom{\mathcal{I}}{2}$, define $P_{\{i,j\}} := \mathbb{E}_y \left[\mathbf{1}_{\{y_i=y_j\}} M^{(y)}_{\{i,j\}}\right]$. These operators are positive semidefinite. Moreover, because each POVM element satisfies $M^{(y)}_{\{i,j\}} \preceq I$ and $\Pr_y[y_i = y_j] = 1/|\mathcal{C}|$, we have

$$P_{\{i,j\}} \preceq \frac{1}{|\mathcal{C}|} I.$$

The POVM normalization also gives

$$\sum_{\{i,j\}\in\binom{\mathcal{I}}{2}} P_{\{i,j\}} = \mathbb{E}_y \sum_{\{i,j\}\in\binom{\mathcal{I}}{2}} \mathbf{1}_{\{y_i=y_j\}} M^{(y)}_{\{i,j\}} \preceq \mathbb{E}_y \sum_{\{i,j\}\in\binom{\mathcal{I}}{2}} M^{(y)}_{\{i,j\}} \preceq I.$$

Thus, the protocol induces a PSD packing

$$P_{\{i,j\}} \succeq 0, \qquad P_{\{i,j\}} \preceq \frac{1}{|\mathcal{C}|} I, \qquad \sum_{\{i,j\}\in\binom{\mathcal{I}}{2}} P_{\{i,j\}} \preceq I.$$

The success operator becomes

$$H_x = \sum_{\{i,j\}\in\binom{\mathcal{I}}{2}} \mathbf{1}_{\{x_i=x_j\}} P_{\{i,j\}}.$$

For every pair $\{i,j\}$, we have

$$\mathbf{1}_{\{x_i=x_j\}} = \frac{1}{|\mathcal{C}|} + \left(\mathbf{1}_{\{x_i=x_j\}} - \frac{1}{|\mathcal{C}|}\right).$$

The constant part contributes an operator bounded by $\frac{1}{|\mathcal{C}|}\sum_{\{i,j\}\in\binom{\mathcal{I}}{2}} P_{\{i,j\}} \preceq \frac{1}{|\mathcal{C}|} I$.

Hence, by (3),

$$p_{\mathrm{succ}} \leq \frac{1}{|\mathcal{C}|} + \mathbb{E}_x \|G_x\|, \tag{4}$$

where the centered discrepancy operator is $G_x := \sum_{\{i,j\}\in\binom{\mathcal{I}}{2}} \left(\mathbf{1}_{\{x_i=x_j\}} - \frac{1}{|\mathcal{C}|}\right) P_{\{i,j\}}$.

We first decouple the pairs by a random bipartition. Let $(\delta_i)_{i\in\mathcal{I}}$ be independent uniform bits, independent of x, and define

$$\mathrm{Cross}_\delta(i,j) := \mathbf{1}_{\{\delta_i\neq\delta_j\}}.$$

Since $\mathbb{E}_\delta \mathrm{Cross}_\delta(i,j) = 1/2$,

$$G_x = 2\,\mathbb{E}_\delta \sum_{\{i,j\}\in\binom{\mathcal{I}}{2}} \mathrm{Cross}_\delta(i,j) \left(\mathbf{1}_{\{x_i=x_j\}} - \frac{1}{|\mathcal{C}|}\right) P_{\{i,j\}}.$$

By Jensen's inequality, we have

$$\mathbb{E}_x \|G_x\| \leq 2\mathbb{E}_{\delta,x} \left\| \sum_{\{i,j\}\in\binom{\mathcal{I}}{2}} \mathrm{Cross}_\delta(i,j) \left(\mathbf{1}_{\{x_i=x_j\}} - \frac{1}{|\mathcal{C}|}\right) P_{\{i,j\}} \right\|. \tag{5}$$

Fix the partition

$$\mathcal{L} := \{i \in \mathcal{I} : \delta_i = 0\}, \qquad \mathcal{R} := \{i \in \mathcal{I} : \delta_i = 1\}.$$

For $a \in \mathcal{L}$ and $b \in \mathcal{R}$, write $P_{a,b} := P_{\{a,b\}}$. Then

$$P_{a,b} \preceq \frac{1}{|\mathcal{C}|} I, \qquad \sum_{a\in\mathcal{L}} \sum_{b\in\mathcal{R}} P_{a,b} \preceq I.$$

The cross contribution is

$$S_{\mathcal{L},\mathcal{R}}(x) := \sum_{a\in\mathcal{L}} \sum_{b\in\mathcal{R}} \left(\mathbf{1}_{\{x_a = x_b\}} - \frac{1}{|\mathcal{C}|} \right) P_{a,b}.$$

It remains to bound this quantity uniformly over the fixed partition. The following argument will condition on the x_b's for $b \in \mathcal{R}$. To explicitly emphasize the difference of left and right, we write $u_a := x_a$ for $a \in \mathcal{L}$ and $v_b := x_b$ for $b \in \mathcal{R}$. For $a \in \mathcal{L}$ and $c \in \mathcal{C}$, define

$$B_{a,c}(v) := \sum_{b\in\mathcal{R}:\, v_b = c} P_{a,b}, \qquad \overline{B}_a(v) := \frac{1}{|\mathcal{C}|} \sum_{c\in\mathcal{C}} B_{a,c}(v).$$

Equivalently,

$$\overline{B}_a(v) = \frac{1}{|\mathcal{C}|} \sum_{b\in\mathcal{R}} P_{a,b}.$$

Conditioned on v, the variables $(u_a)_{a\in\mathcal{L}}$ are independent and uniformly distributed on $\mathcal{C}$, and

$$S_{\mathcal{L},\mathcal{R}}(x) = \sum_{a\in\mathcal{L}} \big(B_{a,u_a}(v) - \overline{B}_a(v) \big).$$

Moreover,

$$\sum_{a\in\mathcal{L}} \sum_{c\in\mathcal{C}} B_{a,c}(v) = \sum_{a\in\mathcal{L}} \sum_{b\in\mathcal{R}} P_{a,b} \preceq I.$$

Therefore Lemma 3.1, applied to the family $\{B_{a,c}(v) : a \in \mathcal{L},\ c \in \mathcal{C}\}$, gives

$$\mathbb{E}_u \big[\|S_{\mathcal{L},\mathcal{R}}(u,v)\| \mid v \big] \le C\sqrt{\log(2d)}\sqrt{Z_v},$$

where $Z_v := \max_{a\in\mathcal{L},\ c\in\mathcal{C}} \|B_{a,c}(v)\|$. Taking expectation in v and using Jensen's inequality for the square root,

$$\mathbb{E}_{u,v} \|S_{\mathcal{L},\mathcal{R}}(u,v)\| \le C\sqrt{\log(2d)}\sqrt{\mathbb{E}_v Z_v}.$$

If $\mathcal{L} = \emptyset$ or $\mathcal{R} = \emptyset$, then the last expectation is zero. Otherwise, Lemma 3.2 applies with $\mathcal{A} = \mathcal{L}$,$\mathcal{B} = \mathcal{R}$ and color set$\mathcal{C}$ yields

$$\mathbb{E}_v Z_v \le C \cdot \frac{\log(2d) + \log(2|\mathcal{C}|)}{|\mathcal{C}|}.$$

Consequently, uniformly over the fixed partition,

$$\mathbb{E}_{u,v} \|S_{\mathcal{L},\mathcal{R}}(u,v)\| \le C\sqrt{\frac{\log(2d)\big(\log(2d) + \log(2|\mathcal{C}|)\big)}{|\mathcal{C}|}}. \tag{6}$$

Averaging (6) over δ and using (5), absorbing the factor 2 into the constant, gives

$$\mathbb{E}_x\|G_x\| \le C\sqrt{\frac{\log(2d)\big(\log(2d)+\log(2|\mathcal{C}|)\big)}{|\mathcal{C}|}}.$$

Combining with (4), and using $|\mathcal{C}| = \sqrt{N}$ and $d = 2^k$, we get

$$p_{\text{succ}} \le \frac{1}{\sqrt{N}} + C\sqrt{\frac{(k+1)\big(k+1+\log N\big)}{\sqrt{N}}}. \tag{7}$$

Finally assume $M > N$ and $p_{\text{succ}} \ge \delta$ for a fixed constant $\delta > 0$. Since $1/\sqrt{N} = o(1)$, (7) implies

$$(k+1)\big(k+1+C\log N\big) = \Omega_\delta(\sqrt{N}).$$

Equivalently, there is a constant $c_0 = c_0(\delta) > 0$ such that, for all sufficiently large N,

$$(k+1)\big(k+1+C\log N\big) \ge c_0\sqrt{N}.$$

Choose $\alpha > 0$ so that $2\alpha^2 < c_0$. Since $\log N = o(N^{1/4})$, for all sufficiently large N we have $C\log N \le \alpha N^{1/4}$. If $k+1 \le \alpha N^{1/4}$, then

$$(k+1)\big(k+1+C\log N\big) \le 2\alpha^2\sqrt{N} < c_0\sqrt{N},$$

contradicting the preceding lower bound. Hence, $k = \Omega_\delta(N^{1/4})$. This completes the proof. □

4 Quantum Streaming Lower Bound for Triangle Finding

In this section, we prove the quantum streaming lower bound for the triangle-finding problem. We begin by establishing the hard input distribution and the communication game for reduction.

4.1 Hard Input Distribution

Definition 4.1. *Let $r, s \in \mathbb{N}$. We define a random graph $G = (V, E)$ as follows. Let $V = X \cup Y \cup Z$ be a partition of the vertex set with $|X| = r$ and $|Y| = s$. The set Z is partitioned into s blocks $Z = Z_1 \cup \cdots \cup Z_s$ and $|Z_i| = r$.*

- *Sample uniformly random bijections $F_i : X \to Z_i$ for all $i \in [s]$, and define*

$$E_{XZ} = \big\{(x, F_i(x)) : x \in X,\ i \in [s]\big\};$$

- *Sample a uniformly random function $A : X \times Y \to \{0,1\}$, and define*

$$E_{XY} = \big\{(x, y) : A(x, y) = 1\big\};$$

- *Sample a uniformly random bijection $C : [s] \to Y$, and define*

$$E_{YZ} = \big\{(C(i), z) : i \in [s],\ z \in Z_i\big\}.$$

Finally, set $E = E_{XZ} \cup E_{XY} \cup E_{YZ}$. Check Figure 1 for an illustration.

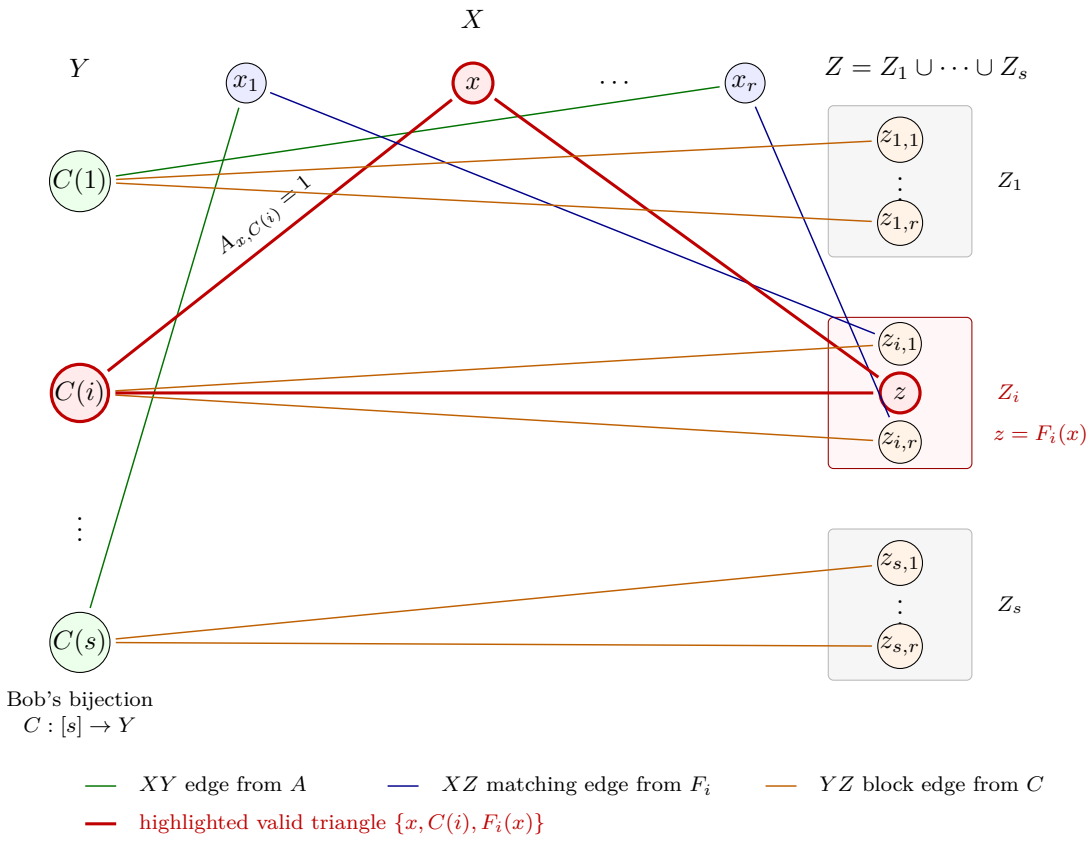

Figure 1: Visualization of the hard distribution in Definition 4.1. The set Z is partitioned into blocks Z_i of size r. Each F_i is a bijection from X to Z_i, and Bob's bijection C makes the vertex $C(i)$ adjacent to the whole block Z_i. A valid output is a triangle $\{x, C(i), F_i(x)\}$ for which the corresponding XY edge is present, i.e. $A_{x,C(i)} = 1$.

Based on the hard input distribution, we can define the communication game about triangle finding.

Definition 4.2 (The communication problem $\mathsf{TripTri}(r, s)$)**.** *The above distribution also defines the communication problem* $\mathsf{TripTri}(r, s)$*: Alice is given* $(F_1, \ldots, F_s, A)$*, Bob is given* C*, Alice sends one quantum message, and Bob must output* (x, i, z) *with*

$$z = F_i(x) \qquad \text{and} \qquad A_{x,C(i)} = 1.$$

The lower bound will be proved in the regime $\sqrt{s} \le r \le s$, but it is useful to compare the distribution with two degenerate extremities for better understanding. Recall that in $\mathsf{TripTri}(r, s)$ Alice holds $(F_1, \ldots, F_s, A)$, Bob holds C, and a valid witness is a triple (x, i, z) satisfying $z = F_i(x)$ and $A_{x,C(i)} = 1$. When $r = 1$, write $X = \{x_\star\}$ and $Z_i = \{z_i\}$ for each $i \in [s]$. Then the maps F_i are fixed, and Alice's nontrivial input is just the string

$$a \in \{0,1\}^Y, \qquad a_y := A_{x_\star, y}.$$

Bob's bijection $C : [s] \to Y$ is equivalently a perfect matching between the block labels $[s]$ and the coordinates Y. The accepting relation becomes

$$(x_\star, i, z_i) \text{ is accepted} \qquad \Longleftrightarrow \qquad a_{C(i)} = 1.$$

Thus, this corresponds to a Boolean Hidden Matching type instance: Bob's input hides which coordinate of Alice's string is associated with each block label. This is not suitable for proving our quantum lower bound, since Boolean Hidden Matching admits efficient one-way quantum protocols [BYJK08].

At the other extreme, when $s = 1$, write $Y = \{y_\star\}$ and $Z = Z_1$. The bijection C is fixed, and the witness condition becomes $z = F_1(x)$ and $A_{x,y_\star} = 1$. If $S := \{x \in X : A_{x,y_\star} = 1\}$ and $M := \{(x, F_1(x)) : x \in X\} \subseteq X \times Z$, Then the valid witnesses are exactly the elements of $M \cap (S \times Z)$. Since S has density $1/2$ with high probability, this is a set-intersection search problem with a constant fraction of intersections, which is easy even classically.

Our hard distribution lies between these two easy extremities. The bijection C keeps the hidden-matching feature: for each block i, Bob hides the relevant column $C(i)$ of Alice's matrix A. At the same time, each block contains r possible witnesses, and the condition $A_{x,C(i)} = 1$ adds a dense set-intersection layer inside the hidden block. Thus, the construction can be viewed as an asymmetric form of Boolean Hidden Matching, strengthened by a set-intersection component. The lower bound comes from this intermediate regime, where neither the efficient quantum protocol for Boolean Hidden Matching nor the classical easiness of dense set intersection applies.

Proposition 4.3. *Assume $\sqrt{s} \le r \le s$. With probability $1 - o(1)$,*

$$|E(G)| = \Theta(rs), \qquad T(G) = \Theta(rs), \qquad \Delta_V(G) = \Theta(s).$$

Moreover, every graph in the support satisfies $\Delta_E(G) \le 1$.

Proof. The sets E_{XZ} and E_{YZ} each have exactly rs edges. The number of XY-edges is $\mathrm{Bin}(rs, 1/2)$, so $|E(G)| = \Theta(rs)$ with high probability. The triangles are exactly the pairs (x, i) with $A_{x,C(i)} = 1$. Since C is a bijection,

$$T(G) = \sum_{x \in X} \sum_{i=1}^{s} A_{x,C(i)} = \sum_{x \in X} \sum_{y \in Y} A_{x,y} \sim \mathrm{Bin}(rs, 1/2).$$

Hence $T(G) = \Theta(rs)$ with high probability.

Every edge lies in at most one triangle. An XY-edge $\{x, y\}$ determines the unique block i with $C(i) = y$ and then the unique vertex $F_i(x)$. An XZ-edge $\{x, F_i(x)\}$ can only use $C(i)$. A YZ-edge $\{C(i), z\}$ can only use the unique x with $F_i(x) = z$. Thus $\Delta_E(G) \le 1$ deterministically. Finally, for every $x \in X$,

$$\tau(x) = \sum_{i=1}^{s} A_{x,C(i)} = \sum_{y \in Y} A_{x,y} \sim \mathrm{Bin}(s, 1/2).$$

Since $r \le s$, Chernoff bounds and a union bound over X give $\tau(x) = \Theta(s)$ for all $x \in X$ with high probability. Vertices in Y are in at most $r \le s$ triangles, and vertices in Z are in at most one. Therefore, $\Delta_V(G) = \Theta(s)$ with high probability. □

4.2 Matrix Discrepancy and Matrix Concentration Bound

In this subsection, we establish the matrix discrepancy estimate and the matrix Chernoff bound that will be used in the proof, and K denotes a universal constant.

Lemma 4.4. *Let $\mathcal{A}$ be a finite index set. For each $a \in \mathcal{A}$, let $Q_a \succeq 0$ be a fixed operator on a d-dimensional Hilbert space, and let η_a be an independent real random variable with $\mathbb{E}\eta_a = 0$ and $|\eta_a| \le 1$. Then*

$$\mathbb{E}_\eta \left\| \sum_{a \in \mathcal{A}} \eta_a Q_a \right\| \le K \sqrt{\log(2d)} \left\| \left(\sum_{a \in \mathcal{A}} Q_a^2 \right)^{1/2} \right\|.$$

Proof. This can be proved by a standard symmetrization argument, followed by the Banach-space contraction principle, and the self-adjoint matrix Khintchine inequality stated in the preliminary. We describe the detail as follows:

Let $S(\eta) := \sum_a \eta_a Q_a$, and η'_a be an independent copy of η_a, independent over a and independent of η. Since $\mathbb{E}[\eta'_a] = 0$, we have

$$\mathbb{E}_{\eta'} S(\eta') = 0.$$

Hence, for every fixed value of η,

$$S(\eta) = \mathbb{E}_{\eta'}\big(S(\eta) - S(\eta')\big).$$

Applying Jensen's inequality to the convex function $A \mapsto \|A\|$ gives

$$\mathbb{E}_\eta \|S(\eta)\| = \mathbb{E}_\eta \left\|\mathbb{E}_{\eta'}\big(S(\eta) - S(\eta')\big)\right\| \quad \le \mathbb{E}_{\eta,\eta'} \left\|S(\eta) - S(\eta')\right\| = \mathbb{E}_{\eta,\eta'} \left\|\sum_a (\eta_a - \eta'_a) Q_a\right\|.$$

The random vector $(\eta_a - \eta'_a)_a$ is symmetric coordinate-by-coordinate. Indeed, changing the sign of coordinate a has the same effect in law as swapping η_a and η'_a. Therefore, if ε_a are independent Rademacher signs, independent of η, η', then

$$\mathbb{E}_{\eta,\eta'} \left\|\sum_a (\eta_a - \eta'_a) Q_a\right\| = \mathbb{E}_{\eta,\eta',\varepsilon} \left\|\sum_a \varepsilon_a (\eta_a - \eta'_a) Q_a\right\|.$$

Now condition on η, η' and apply the contraction principle in the Banach space of $d \times d$ operators equipped with the operator norm $\|\cdot\|$, using Lemma 2.1. Since

$$|\eta_a - \eta'_a| \le |\eta_a| + |\eta'_a| \le 2,$$

the contraction principle Lemma 2.1 gives

$$\mathbb{E}_\varepsilon \left\|\sum_a \varepsilon_a (\eta_a - \eta'_a) Q_a\right\| \le 2\, \mathbb{E}_\varepsilon \left\|\sum_a \varepsilon_a Q_a\right\|.$$

Combining the preceding inequalities yields the symmetrized bound

$$\mathbb{E}_\eta \left\|\sum_a \eta_a Q_a\right\| \le 2\, \mathbb{E}_\varepsilon \left\|\sum_a \varepsilon_a Q_a\right\|.$$

It remains to control the Rademacher series. Since $Q_a \succeq 0$, each Q_a is self-adjoint. Applying Lemma 2.2 with $A_a = Q_a$, we obtain

$$\mathbb{E}_\eta \left\|\sum_a \eta_a Q_a\right\| \le 2K\sqrt{\log(2d)} \left\|\left(\sum_a Q_a^2\right)^{1/2}\right\|.$$

Absorbing the factor 2 into the universal constant K gives the desired inequality. □

Remark 4.5. *The matrix Khintchine inequality can be viewed as the degree-one square-function form of the matrix hypercontractivity inequality. The standard matrix-valued Boolean hypercontractive inequality is not sufficient as a black box here: it gives a Frobenius-type variance* $\left(\mathrm{Tr} \sum_a Q_a^2\right)^{1/2}$ *rather than the operator square function* $\left\|\left(\sum_a Q_a^2\right)^{1/2}\right\|$. *This distinction matters because the Frobenius bound can lose a factor* $\sqrt{d}$, *where* $d = 2^k$, *which would destroy the desired communication lower bound.*

Lemma 4.6. *For $x \in X$, $i \in [s]$, $z \in Z_i$, and $y \in Y$, let $P_{x,i,z,y} \succeq 0$ be operators on a d-dimensional Hilbert space such that*

$$P_{x,i,z,y} \preceq \frac{1}{s} I, \qquad \sum_{x,i,z,y} P_{x,i,z,y} \preceq I.$$

For independent uniform matchings $F_i : X \to Z_i$, define $Q_{x,y}(F) := \sum_{i=1}^{s} P_{x,i,F_i(x),y}$. Then

$$\mathbb{E}_F \max_{x,y} \|Q_{x,y}(F)\| \le K \left(\frac{1}{r} + \frac{\log(2d) + \log(rs)}{s} \right).$$

Proof. Fix (x, y) and set $S_i = P_{x,i,F_i(x),y}$. Then, we know S_is are independent, $0 \preceq S_i \preceq I/s$, and

$$\mathbb{E} \sum_i S_i = \frac{1}{r} \sum_i \sum_{z \in Z_i} P_{x,i,z,y} \preceq \frac{1}{r} I.$$

For the matrix Bernstein applied to $S_i - \mathbb{E}S_i$, the variance term is at most

$$\left\| \sum_i \mathbb{E}(S_i - \mathbb{E}S_i)^2 \right\| \le \left\| \sum_i \mathbb{E}S_i^2 \right\| \le \frac{1}{s} \left\| \mathbb{E} \sum_i S_i \right\| \le \frac{1}{rs}.$$

Hence, for all $u \ge 0$,

$$\Pr\left[\|Q_{x,y}(F)\| > K \left(\frac{1}{r} + \frac{\log(2d) + u}{s} \right) \right] \le e^{-u}.$$

Taking a union bound over the rs choices of (x, y) and integrating the resulting tail bound gives

$$\mathbb{E}_F \max_{x,y} \|Q_{x,y}(F)\| \le K \left(\frac{1}{r} + \frac{\log(2d) + \log(rs)}{s} \right). \qquad \square$$

4.3 One-Way Communication Lower Bound

Theorem 4.7. *Assume $\sqrt{s} \le r \le s$. Any one-way quantum communication protocol without shared entanglement that solves $\mathsf{TripTri}(r, s)$ with success probability at least $3/5$ must send $\Omega(\sqrt{s})$ qubits.*

Proof. Suppose Alice sends k qubits, and let $d = 2^k$. On input (F, A), Alice sends a density matrix $\rho_{F,A}$. On input C, Bob uses a POVM

$$\{M^C_{x,i,z} : x \in X,\ i \in [s],\ z \in Z_i\} \cup \{M^C_\perp\}.$$

For fixed (F, A), define Bob's average success operator $H_{F,A} := \mathbb{E}_C \sum_{x \in X} \sum_{i=1}^{s} A_{x,C(i)}\, M^C_{x,i,F_i(x)}$ and the success probability is $p_{\text{succ}} = \mathbb{E}_{F,A} \operatorname{Tr}(\rho_{F,A} H_{F,A})$.

Define $A_{x,y} = 1/2 + \eta_{x,y}$. The constant part contributes at most $\frac{1}{2} I$, because for each C we sum only POVM elements. Therefore

$$p_{\text{succ}} \le \frac{1}{2} + \mathbb{E}_{F,A} \|G_{F,A}\|, \qquad G_{F,A} := \mathbb{E}_C \sum_{x,i} \eta_{x,C(i)} M^C_{x,i,F_i(x)}. \tag{8}$$

We decompose $G_{F,A}$ as a centered sum over the independent XY-bits. Define

$$P_{x,i,z,y} := \mathbb{E}_C \left[\mathbf{1}_{\{C(i)=y\}} M^C_{x,i,z} \right].$$

Then

$$P_{x,i,z,y} \preceq I/s \text{ and } \sum_{x,i,z,y} P_{x,i,z,y} = \mathbb{E}_C \sum_{x,i,z} M^C_{x,i,z} \preceq I.$$

For fixed F, let $Q_{x,y}(F) := \sum_{i=1}^{s} P_{x,i,F_i(x),y}$. Then

$$G_{F,A} = \sum_{x\in X} \sum_{y\in Y} \eta_{x,y} Q_{x,y}(F).$$

Conditioning on F and applying Lemma 4.4,

$$\mathbb{E}_A[\|G_{F,A}\| \mid F] \le K\sqrt{\log(2d)} \left\| \left(\sum_{x,y} Q_{x,y}(F)^2 \right)^{1/2} \right\|.$$

Let $Z_F = \max_{x,y} \|Q_{x,y}(F)\|$. Since each $Q_{x,y}(F)$ is positive semidefinite and satisfies $\|Q_{x,y}(F)\| \le Z_F$, we have

$$Q_{x,y}(F)^2 \preceq Z_F Q_{x,y}(F).$$

Moreover, the packing condition gives $\sum_{x,y} Q_{x,y}(F) \preceq I$. Therefore,$\sum_{x,y} Q_{x,y}(F)^2 \preceq Z_F I$, so the square-function term is at most $\sqrt{Z_F}$. Lemma 4.6 gives

$$\mathbb{E}_{F,A}\|G_{F,A}\| \le K\sqrt{(k+1)\left(\frac{1}{r} + \frac{k+1+\log(rs)}{s}\right)}.$$

If $k \le c\sqrt{s}$, then $\sqrt{s} \le r \le s$ and $\log(rs) = o(\sqrt{s})$ make the last display at most $K\sqrt{c + c^2 + o(1)}$. For a sufficiently small constant $c > 0$, this is less than $1/10$. By (8), such a protocol has success probability less than $3/5$. Hence $k = \Omega(\sqrt{s})$. □

Proof of Theorem 1.2. The case $\Delta_V = O(1)$ only asks for a constant lower bound, so assume $\Delta_V \to \infty$. For a target value of Δ_V, choose $s = \Theta(\Delta_V)$ and set $r = \lceil \sqrt{s} \rceil$.

Then, $\sqrt{s} \le r \le s$. Since $s \le m^{2/3}$, one graph instance of Definition 4.1 has $rs = \Theta(s^{3/2}) \le \Theta(m)$ edges. Take $q = \Theta\left(\frac{m}{rs}\right)$ disjoint copies of the graph instance, all generated from the same communication input $(F_1, \ldots, F_s, A, C)$ but placed on disjoint vertex sets. Adding isolated dummy edges, if necessary, makes the total edge count exactly m and does not change any triangle parameter.

By Proposition 4.3, one graph instance has $\Theta(rs)$ edges, $\Theta(rs)$ triangles, $\Delta_E \le 1$, and $\Delta_V = \Theta(s)$ with probability $1 - o(1)$. Therefore, the disjoint union has

$$|E| = \Theta(qrs) = \Theta(m), \qquad T = \Theta(qrs) = \Theta(m), \qquad \Delta_V = \Theta(s),$$

and still has $\Delta_E \le 1$.

Suppose a one-pass quantum streaming algorithm succeeds with probability at least $2/3$ and uses S qubits. Alice runs it on all Alice-owned edges in the q copies and sends the S-qubit memory state to Bob. Bob continues the stream with all Bob-owned edges. Any triangle output by the algorithm lies in one copy and has the form $(x, C(i), F_i(x))$ inside that copy, with $A_{x,C(i)} = 1$. Ignoring the copy label, Bob obtains a valid output $(x, i, F_i(x))$ for $\mathsf{TripTri}(r, s)$.

The bad event in Proposition 4.3 has probability $o(1)$, so the induced protocol succeeds with probability $2/3 - o(1)$, which is at least $3/5$ for large enough instances. Therefore, Theorem 4.7 gives $S = \Omega(\sqrt{s})$. Since $s = \Theta(\Delta_V)$ and $T = \Theta(m)$, we have: $S = \Omega(\sqrt{\Delta_V})$. □

Acknowledgment

The authors used ChatGPT Pro 5.4 as an AI-assisted research and writing tool throughout the preparation of this manuscript. The tool was used to help brainstorm ideas and explore proof strategies. Portions of the manuscript text were redrafted or modified with AI assistance across all sections. All final mathematical claims, algorithms, proofs, citations, and wording were reviewed, edited, and validated by the authors. The authors assume responsibility for all content of the submission.

References

[Aar02] Scott Aaronson. Quantum lower bound for the collision problem. In *Proceedings of the Thirty-Fourth Annual ACM Symposium on Theory of Computing (STOC 2002)*, pages 635–642, New York, NY, USA, 2002. Association for Computing Machinery.

[AD24] Srinivasan Arunachalam and Joao F Doriguello. Matrix hypercontractivity, streaming algorithms and LDCs: the large alphabet case. *ACM Transactions on Computation Theory*, 16(4):1–38, 2024.

[AKKR08] Noga Alon, Tali Kaufman, Michael Krivelevich, and Dana Ron. Testing triangle-freeness in general graphs. *SIAM Journal on Discrete Mathematics*, 22(2):786–819, 2008.

[ANTSV02] Andris Ambainis, Ashwin Nayak, Amnon Ta-Shma, and Umesh V. Vazirani. Dense quantum coding and quantum finite automata. *Journal of the ACM*, 49(4):496–511, 2002.

[AYZ97] Noga Alon, Raphael Yuster, and Uri Zwick. Finding and counting given length cycles. *Algorithmica*, 17(3):209–223, 1997.

[BARdW08] Avraham Ben-Aroya, Oded Regev, and Ronald de Wolf. A hypercontractive inequality for matrix-valued functions with applications to quantum computing and LDCs. In *2008 49th Annual IEEE Symposium on Foundations of Computer Science*, pages 477–486. IEEE, 2008.

[BC17] Suman K. Bera and Amit Chakrabarti. Towards Tighter Space Bounds for Counting Triangles and Other Substructures in Graph Streams. In Heribert Vollmer and Brigitte Vallée, editors, *34th Symposium on Theoretical Aspects of Computer Science (STACS 2017)*, volume 66 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 11:1–11:14, Dagstuhl, Germany, 2017. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[BFM18] Balthazar Bauer, Pooya Farshim, and Sogol Mazaheri. Combiners for backdoored random oracles. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology – CRYPTO 2018, Part II*, volume 10992 of *Lecture Notes in Computer Science*, pages 272–302, Cham, 2018. Springer.

[BGK+18] Mark Braverman, Ankit Garg, Young Kun Ko, Jieming Mao, and Dave Touchette. Near-optimal bounds on the bounded-round quantum communication complexity of disjointness. *SIAM Journal on Computing*, 47(6):2277–2314, 2018.

[BHT98] Gilles Brassard, Peter Høyer, and Alain Tapp. Quantum cryptanalysis of hash and claw-free functions. In Claudio L. Lucchesi and Arnaldo V. Moura, editors, *LATIN'98: Theoretical Informatics*, volume 1380 of *Lecture Notes in Computer Science*, pages 163–169, Berlin, Heidelberg, 1998. Springer.

[BOV13] Vladimir Braverman, Rafail Ostrovsky, and Dan Vilenchik. How hard is counting triangles in the streaming model? In Fedor V. Fomin, Rūsiņš Freivalds, Marta Kwiatkowska, and David Peleg, editors, *Automata, Languages, and Programming*, volume 7965 of *Lecture Notes in Computer Science*, pages 244–254, Berlin, Heidelberg, 2013. Springer.

[BW25] Paul Beame and Michael Whitmeyer. Multiparty Communication Complexity of Collision-Finding and Cutting Planes Proofs of Concise Pigeonhole Principles. In Keren Censor-Hillel, Fabrizio Grandoni, Joël Ouaknine, and Gabriele Puppis, editors, *52nd International Colloquium on Automata, Languages, and Programming (ICALP 2025)*, volume 334 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 21:1–21:20, Dagstuhl, Germany, 2025. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[BYJK08] Ziv Bar-Yossef, T. S. Jayram, and Iordanis Kerenidis. Exponential separation of quantum and classical one-way communication complexity. *SIAM Journal on Computing*, 38(1):366–384, 2008.

[BYKS02] Ziv Bar-Yossef, Ravi Kumar, and D. Sivakumar. Reductions in streaming algorithms, with an application to counting triangles in graphs. In *Proceedings of the Thirteenth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA 2002)*, pages 623–632, Philadelphia, PA, USA, 2002. Society for Industrial and Applied Mathematics.

[CJ17] Graham Cormode and Hossein Jowhari. A second look at counting triangles in graph streams (corrected). *Theoretical Computer Science*, 683:22–30, 2017.

[CPZ19] Yi-Jun Chang, Seth Pettie, and Hengjie Zhang. Distributed triangle detection via expander decomposition. In *Proceedings of the Thirtieth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA 2019)*, pages 821–840. Society for Industrial and Applied Mathematics, 2019.

[FMP+12] Samuel Fiorini, Serge Massar, Sebastian Pokutta, Hans Raj Tiwary, and Ronald de Wolf. Linear vs. semidefinite extended formulations: Exponential separation and strong lower bounds. In *Proceedings of the Forty-Fourth Annual ACM Symposium on Theory of Computing (STOC 2012)*, pages 95–106, New York, NY, USA, 2012. Association for Computing Machinery.

[GJ22] Mika Göös and Siddhartha Jain. Communication Complexity of Collision. In Amit Chakrabarti and Chaitanya Swamy, editors, *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM 2022)*, volume 245 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 19:1–19:9, Dagstuhl, Germany, 2022. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[GKK+07] Dmitry Gavinsky, Julia Kempe, Iordanis Kerenidis, Ran Raz, and Ronald De Wolf. Exponential separations for one-way quantum communication complexity, with appli-

cations to cryptography. In *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, pages 516–525, 2007.

[HRS22] Samuel B. Hopkins, Prasad Raghavendra, and Abhishek Shetty. Matrix discrepancy from quantum communication. In *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing (STOC 2022)*, pages 637–648, New York, NY, USA, 2022. Association for Computing Machinery.

[ILG17] Taisuke Izumi and François Le Gall. Triangle finding and listing in CONGEST networks. In *Proceedings of the ACM Symposium on Principles of Distributed Computing (PODC 2017)*, pages 381–389, New York, NY, USA, 2017. Association for Computing Machinery.

[ILGM20] Taisuke Izumi, François Le Gall, and Frédéric Magniez. Quantum Distributed Algorithm for Triangle Finding in the CONGEST Model. In Christophe Paul and Markus Bläser, editors, *37th International Symposium on Theoretical Aspects of Computer Science (STACS 2020)*, volume 154 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 23:1–23:13, Dagstuhl, Germany, 2020. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[IR78] Alon Itai and Michael Rodeh. Finding a minimum circuit in a graph. *SIAM Journal on Computing*, 7(4):413–423, 1978.

[IR21] Dmitry Itsykson and Artur Riazanov. Proof Complexity of Natural Formulas via Communication Arguments. In Valentine Kabanets, editor, *36th Computational Complexity Conference (CCC 2021)*, volume 200 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 3:1–3:34, Dagstuhl, Germany, 2021. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[JK21] Rajesh Jayaram and John Kallaugher. An Optimal Algorithm for Triangle Counting in the Stream. In Mary Wootters and Laura Sanità, editors, *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM 2021)*, volume 207 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 11:1–11:11, Dagstuhl, Germany, 2021. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[JRS03a] Rahul Jain, Jaikumar Radhakrishnan, and Pranab Sen. A direct sum theorem in communication complexity via message compression. In *International Colloquium on Automata, Languages, and Programming*, pages 300–315. Springer, 2003.

[JRS03b] Rahul Jain, Jaikumar Radhakrishnan, and Pranab Sen. A lower bound for the bounded round quantum communication complexity of set disjointness. In *Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2003)*, pages 220–229. IEEE Computer Society, 2003.

[Kal22] John Kallaugher. A quantum advantage for a natural streaming problem. In *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 897–908. IEEE Computer Society, 2022.

[KdW04] Iordanis Kerenidis and Ronald de Wolf. Exponential lower bound for 2-query locally decodable codes via a quantum argument. *Journal of Computer and System Sciences*, 69(3):395–420, 2004.

[KKP18] John Kallaugher, Michael Kapralov, and Eric Price. The sketching complexity of graph and hypergraph counting. In *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 556–567. IEEE Computer Society, 2018.

[Kla07a] Hartmut Klauck. Lower bounds for quantum communication complexity. *SIAM Journal on Computing*, 37(1):20–46, 2007.

[Kla07b] Hartmut Klauck. One-way communication complexity and the Nečiporuk lower bound on formula size. *SIAM Journal on Computing*, 37(2):552–583, 2007.

[KP17] John Kallaugher and Eric Price. A hybrid sampling scheme for triangle counting. In *Proceedings of the Twenty-Eighth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA 2017)*, pages 1778–1797. Society for Industrial and Applied Mathematics, 2017.

[KP22] John Kallaugher and Ojas Parekh. The quantum and classical streaming complexity of quantum and classical max-cut. In *Proceedings of the 63rd IEEE Annual Symposium on Foundations of Computer Science (FOCS 2022)*, pages 498–506, 2022.

[KPV25] John Kallaugher, Ojas Parekh, and Nadezhda Voronova. How to design a quantum streaming algorithm without knowing anything about quantum computing. In *2025 Symposium on Simplicity in Algorithms (SOSA)*, pages 9–45. SIAM, 2025.

[Lat08] Matthieu Latapy. Main-memory triangle computations for very large (sparse (power-law)) graphs. *Theoretical Computer Science*, 407(1–3):458–473, 2008.

[LG14] François Le Gall. Improved quantum algorithm for triangle finding via combinatorial arguments. In *Proceedings of the 55th IEEE Annual Symposium on Foundations of Computer Science (FOCS 2014)*, pages 216–225. IEEE Computer Society, 2014.

[LMS13] Troy Lee, Frédéric Magniez, and Miklos Santha. Improved quantum query algorithms for triangle finding and associativity testing. In *Proceedings of the Twenty-Fourth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA 2013)*, pages 1486–1502. Society for Industrial and Applied Mathematics, 2013.

[LRS15] James R Lee, Prasad Raghavendra, and David Steurer. Lower bounds on the size of semidefinite programming relaxations. In *Proceedings of the forty-seventh annual ACM symposium on Theory of computing*, pages 567–576, 2015.

[LS09a] Troy Lee and Adi Shraibman. Lower bounds in communication complexity. *Foundations and Trends in Theoretical Computer Science*, 3(4):263–399, 2009.

[LS09b] Nati Linial and Adi Shraibman. Lower bounds in communication complexity based on factorization norms. *Random Structures & Algorithms*, 34(3):368–394, 2009.

[LT91] Michel Ledoux and Michel Talagrand. *Probability in Banach Spaces: Isoperimetry and Processes*. Springer, 1991.

[LZ10] Troy Lee and Shengyu Zhang. Composition theorems in communication complexity. In *Automata, Languages and Programming (ICALP 2010)*, volume 6198 of *Lecture Notes in Computer Science*, pages 475–489, Berlin, Heidelberg, 2010. Springer.

[MSOI+02] Ron Milo, Shai S. Shen-Orr, Shalev Itzkovitz, Nadav Kashtan, Dmitri B. Chklovskii, and Uri Alon. Network motifs: Simple building blocks of complex networks. *Science*, 298(5594):824–827, 2002.

[MSS07] Frédéric Magniez, Miklos Santha, and Mario Szegedy. Quantum algorithms for the triangle problem. *SIAM Journal on Computing*, 37(2):413–424, 2007.

[Nay99] 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, 1999.

[NPRR12] Hung Q. Ngo, Ely Porat, Christopher Ré, and Atri Rudra. Worst-case optimal join algorithms. In *Proceedings of the 31st ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems (PODS 2012)*, pages 37–48, New York, NY, USA, 2012. Association for Computing Machinery.

[NT17] Ashwin Nayak and Dave Touchette. Augmented index and quantum streaming algorithms for DYCK(2). In *Proceedings of the 32nd Computational Complexity Conference (CCC 2017)*, volume 79 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 23:1–23:21, 2017.

[Raz03] Alexander A. Razborov. Quantum communication complexity of symmetric predicates. *Izvestiya: Mathematics*, 67(1):145–159, 2003.

[RVW11] Liam Roditty and Virginia Vassilevska Williams. Minimum weight cycles and triangles: Equivalences and algorithms. In *Proceedings of the 52nd Annual IEEE Symposium on Foundations of Computer Science (FOCS 2011)*, pages 180–189. IEEE Computer Society, 2011.

[She11] Alexander A. Sherstov. The pattern matrix method. *SIAM Journal on Computing*, 40(6):1969–2000, 2011.

[Shi02] Yaoyun Shi. Quantum lower bounds for the collision and the element distinctness problems. In *Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science (FOCS 2002)*, pages 513–519. IEEE Computer Society, 2002.

[SV11] Siddharth Suri and Sergei Vassilvitskii. Counting triangles and the curse of the last reducer. In *Proceedings of the 20th International Conference on World Wide Web (WWW 2011)*, pages 607–614, New York, NY, USA, 2011. Association for Computing Machinery.

[SW05] Thomas Schank and Dorothea Wagner. Finding, counting and listing all triangles in large graphs, an experimental study. In Sotiris E. Nikoletseas, editor, *Experimental and Efficient Algorithms (WEA 2005)*, volume 3503 of *Lecture Notes in Computer Science*, pages 606–609, Berlin, Heidelberg, 2005. Springer.

[SZ09] Yaoyun Shi and Yufan Zhu. Quantum communication complexity of block-composed functions. *Quantum Information & Computation*, 9(5–6):444–460, 2009.

[Tou15] Dave Touchette. Quantum information complexity. In *Proceedings of the Forty-Seventh Annual ACM Symposium on Theory of Computing (STOC 2015)*, pages 317–326, New York, NY, USA, 2015. Association for Computing Machinery.

[Tro15] Joel A. Tropp. An introduction to matrix concentration inequalities. *Foundations and Trends in Machine Learning*, 8(1–2):1–230, 2015.

[Ver18] Roman Vershynin. *High-Dimensional Probability: An Introduction with Applications in Data Science*. Number 47 in Cambridge Series in Statistical and Probabilistic Mathematics. Cambridge University Press, Cambridge New York Melbourne New Delhi Singapore, 2018.

[VWW18] Virginia Vassilevska Williams and R. Ryan Williams. Subcubic equivalences between path, matrix, and triangle problems. *Journal of the ACM*, 65(5):27:1–27:38, 2018.

[YZ24] Guangxu Yang and Jiapeng Zhang. Communication lower bounds for collision problems via density increment arguments. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing (STOC 2024)*, pages 630–639, New York, NY, USA, 2024. Association for Computing Machinery.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il