Augmented Index and
Quantum Streaming Algorithms for Dyck(2)

Ashwin Nayak [*]   Dave Touchette [†]

October 16, 2016

Abstract

We show how two recently developed quantum information theoretic tools can be applied to obtain lower bounds on quantum information complexity. We also develop new tools with potential for broader applicability, and use them to establish a lower bound on the quantum information complexity for the Augmented Index function on an easy distribution. This approach allows us to handle superpositions rather than distributions over inputs, the main technical challenge faced previously. By providing a quantum generalization of the argument of Jain and Nayak [IEEE TIT'14], we leverage this to obtain a lower bound on the space complexity of multi-pass, unidirectional quantum streaming algorithms for the Dyck(2) language.

---

[*]Department of Combinatorics and Optimization, and Institute for Quantum Computing, University of Waterloo, 200 University Ave. W., Waterloo, ON, N2L 3G1, Canada. Email: ashwin.nayak@uwaterloo.ca. Research supported in part by NSERC Canada.

[†]Institute for Quantum Computing and Department of Combinatorics and Optimization, University of Waterloo, and the Perimeter Institute of Theoretical Physics, email: touchette.dave@gmail.com

1 Introduction

The first *bona fide* quantum computers that are built are likely to involve a few hundred qubits, and be limited to short computations. This prompted much research into the capabilities of space bounded quantum computation, especially of quantum finite automata, during the early development of the theory of quantum computation (see, e.g., Refs. [MC00, KW97, AF98, ANTV02]). More recently, this has led to the investigation of quantum *streaming* algorithms [LG06, GKK$^+$08, BKCG14].

Streaming algorithms were originally proposed as a means to process massive real-world data that cannot be stored in their entirety in computer memory [Mut05]. Instead of random access to the input data, these algorithms receive the input in the form of a *stream*, i.e., one input symbol at a time. The algorithms attempt to solve some information processing task using as little space and time as possible, on occasion using more than one sequential pass over the input stream.

Streaming algorithms provide a natural framework for studying simple, small-space quantum computation beyond the scope of quantum finite automata. Some of the works mentioned above (e.g., LeGall [LG06]) show how quantum streaming algorithms can accomplish certain specially crafted tasks with exponentially smaller space, as compared with classical algorithms. This led Jain and Nayak [JN14] to ask how much more efficient such quantum algorithms could be for other, more natural problems. They focused on DYCK(2), a well-studied and important problem from formal language theory. DYCK(2) consists of all well-formed expressions with two types of parenthesis, denoted below by $a, \overline{a}$ and $b, \overline{b}$, with the bar indicating a closing parenthesis. More formally, DYCK(2) is the language over the alphabet $\Sigma = \{a, \overline{a}, b, \overline{b}\}$ defined recursively as

$$\text{DYCK}(2) \quad = \quad \varepsilon + \left(a \cdot \text{DYCK}(2) \cdot \overline{a} + b \cdot \text{DYCK}(2) \cdot \overline{b}\right) \cdot \text{DYCK}(2) \ ,$$

where ε is the empty string, '·' indicates concatenation of strings (or subsets thereof) and '+' denotes set union.

The related problem of recognizing whether a given expression with parentheses is well-formed was originally studied by Magniez, Mathieu, and Nayak [MMN14] in the context of classical streaming algorithms. They discovered a remarkable phenomenon, that providing *bi-directional* access to the input stream leads to exponentially more space-efficient algorithm. They presented a streaming algorithm that makes one pass over the input, uses $O(\sqrt{n \log n})$ bits, and makes polynomially small probability of error to determine membership of expressions of length $O(n)$ in DYCK(2). Moreover, they proved that this space bound is optimal for error at most $1/(n \log n)$, and conjectured that a similar polynomial space bound holds for multi-pass algorithms as well. Magniez *et al.* complemented this with a second algorithm that makes two passes in *opposite* directions over the input, uses only $O(\log^2 n)$ space, and has polynomially small probability of error. Later, two sets of authors [CCKM13, JN14] independently and concurrently proved the conjectured hardness of DYCK(2) for multi-pass (unidirectional) streaming algorithms. They showed that any unidirectional randomized T-pass streaming algorithm that recognizes length n instances of DYCK(2) with a constant probability of error uses space $\Omega(\sqrt{n}/T)$.

The space lower bounds for DYCK(2) established in Refs. [MMN14, CCKM13, JN14] all rely on a connection with a two-party communication problem, Augmented Index, a variant of the Index function in two-party communication complexity. In the Index function problem, one party, Alice, is given a string $x \in \{0, 1\}^n$, and the other party, Bob, is given an index $k \in [n]$, for some positive integer n. Their goal is to communicate with each other and compute x_k, the kth bit of the string x. In the Augmented Index function problem, Bob is given the prefix $x[1, k-1]$ (the first $k-1$ bits of x) and a bit b in addition to the index k. The goal of the two parties is to determine if $x_k = b$ or not. The three works cited above (see also [CK11]) all prove information cost trade-offs for Augmented Index. As a result, in any bounded-error protocol for

the function, either Alice reveals $\Omega(n)$ information about her input x, or Bob reveals $\Omega(1)$ information about the index k (even under an easy distribution, the uniform distribution over zeros of the function).

Motivated by the abovementioned works, Jain and Nayak [JN14] studied quantum protocols for Augmented Index. They defined a notion of quantum information cost for distributions with a limited form of dependence, and then arrived at a similar tradeoff as in the classical case. This result, however, does not imply a lower bound on the space required by quantum streaming algorithms for DYCK(2). The issue is that the reduction from low information cost protocols for Augmented Index to small space streaming algorithms breaks down in the quantum case (for the notion of quantum information cost they proposed). They left open the possibility of more efficient unidirectional quantum streaming algorithms.

We establish the following lower bound on the space complexity of T-pass, unidirectional quantum streaming algorithms for the DYCK(2) language, thus solving the question left open by Jain and Nayak [JN14].

Theorem 1 *For any $T \geq 1$, any unidirectional T-pass quantum streaming algorithm that recognizes length n instances of* DYCK(2) *with a constant probability of error uses space $\Omega(\sqrt{n}/T^3)$.*

This shows that, possibly up to logarithmic terms and the dependence on the number of passes, quantum streaming algorithms are no more efficient than classical ones for this problem. In particular, this provides the first natural example for which classical bidirectional streaming algorithms perform exponentially better than unidirectional quantum streaming algorithms.

Theorem 1 is a consequence of a lower bound, holding for any quantum protocol Π computing the Augmented Index function, on the quantum information cost evaluated on an easy distribution μ_0: the uniform distribution over the zeros of the function. Due to the asymmetry of the Augmented Index function, we distinguish between the amount of information Alice transmits to Bob, denoted $\mathrm{QIC}_{\mathrm{A} \to \mathrm{B}}(\Pi, \mu_0)$ and the amount of information Bob transmits to Alice, denoted $\mathrm{QIC}_{\mathrm{B} \to \mathrm{A}}(\Pi, \mu_0)$; formal definitions for these notions are stated in Section 2.3. Our key technical contributions go into showing the following trade-off.

Theorem 2 *In any t-round quantum protocol Π computing the Augmented Index function f_n with constant error $\varepsilon \in [0, 1/4)$ on any input, either $\mathrm{QIC}_{\mathrm{A} \to \mathrm{B}}(\Pi, \mu_0) \in \Omega(n/t^2)$ or $\mathrm{QIC}_{\mathrm{B} \to \mathrm{A}}(\Pi, \mu_0) \in \Omega(1/t^2)$.*

A more precise statement is presented as Theorem 5. Establishing a lower bound on the quantum information cost for such an easy distribution is necessary; the direct sum argument that allows us to link quantum streaming algorithms to quantum protocols for Augmented Index crucially hinges on this.

Since the notion of quantum information cost that we use is a lower bound on quantum communication, this provides the first lower bounds on the communication complexity of quantum protocols for Augmented Index. The fact that Alice and Bob share part of the input for this function makes lower bound proofs more difficult in general. In terms of information lower bound, the work of Jain, Radhakrishnan and Sen [JRS09] can be understood as providing a lower bound on the quantum information cost of any bidirectional protocol that computes the Index function. However, the information is measured with respect to a hard distribution and their techniques do not seem to apply to the analysis of quantum information cost with respect to easy distributions.

In order to obtain the above quantum information cost trade-off for Augmented Index, we develop new tools for quantum communication complexity that we believe have broader applicability.

One tool is a generalization of the well-known average encoding theorem of (classical and) quantum complexity theory, which formalizes the intuition that weakly correlated systems are nearly independent. We call this generalized version the *superposition-average encoding theorem*, as it allows us to deal with arbitrary superpositions rather than only classical distributions over inputs to quantum communication protocols. A key technical ingredient in the proof of this result is the breakthrough result by Fawzi and Ren-

ner [FR15], linking the conditional quantum mutual information to the optimal recovery map acting on the conditioning system.

The analysis of superpositions over inputs was the main bottleneck faced by previous attempts at obtaining strong lower bounds on the quantum information cost of protocols for Augmented Index. In particular, Jain and Nayak [JN14] considered a different notion of quantum information cost for which they derive a trade-off similar to that in Theorem 2. While their definition is tailored to deal with superpositions over classical inputs, they sacrifice two properties which are crucial in the notion of quantum information cost we use: that it is a lower bound on quantum communication, and that it satisfies a direct sum property. These two properties are essential for linking quantum streaming algorithms for $\mathrm{DYCK}(2)$ and quantum protocols for Augmented Index. Showing how to maintain these properties while also maintaining near-independence of superpositions over inputs in low information protocols is perhaps our most important technical contribution. We believe that our approach with the use of the superposition-average encoding theorem is of broader applicability.

We go a step further; we provide an alternative way to achieve a similar result, by using a method which is more tailored to the Augmented Index problem. An important stepping stone in this approach is the recently developed *Information Flow Lemma* due to Laurière and Touchette [LT16]. This approach allows us to obtain a slightly better round-dependence in the information cost trade-off.

Another key ingredient in the proof of Theorem 2 is a *Quantum Cut-and-Paste Lemma*, a variant of a technique used in Refs. [JRS03, JN14], that allows us to deal with easy distributions over inputs. The cut-and-paste lemma for randomized communication protocols connects the distance between transcripts obtained by running protocols on inputs chosen from a two-by-two rectangle $\{x, x'\} \times \{y, y'\}$. The cut-and-paste lemma is very powerful, and a direct quantum analogue does not hold. We can nevertheless obtain the following weaker variant, linking any four possible pairs of inputs in a two-by-two rectangle: if the states for a fixed input y to Bob are close up to a local unitary operator on Alice's side and the states for a fixed input x to Alice are close up to a local unitary operator on Bob's side, then, up to local unitary operators on Alice's and Bob's sides, the states for all pairs (x'', y'') of inputs in the rectangle $\{x, x'\} \times \{y, y'\}$ are close to each other. This lemma allows us to link output states of protocols on inputs from an easy distribution, all mapping to the same output value, to an output state corresponding to a different output value. This helps derive a contradiction to the assumption of low quantum information cost, as states corresponding to different outputs are distinguishable with constant probability.

2 Preliminaries

2.1 Quantum Communication Complexity

We refer the reader to text books such as [Wat15, Wil13] for standard concepts and the associated notation from quantum information.

We use the following notation for interactive communication between two parties, called Alice and Bob by convention. An M-message protocol Π for a task with input registers $A_{\mathrm{in}}B_{\mathrm{in}}$ and output registers $A_{\mathrm{out}}B_{\mathrm{out}}$ is defined by a sequence of isometries $U_1, \ldots, U_{M+1}$ along with a pure state $\psi \in \mathcal{D}(T^{\mathrm{A}}T^{\mathrm{B}})$ shared between Alice and Bob, for some arbitrary but finite dimensional registers $T^{\mathrm{A}}T^{\mathrm{B}}$. We refer to ψ as the pre-shared entanglement. We have $M + 1$ isometries in an M-message protocol, as one isometry is applied before each message, and a final isometry is applied after the last message is received. We assume that Alice sends the first message. In the case of even M, the registers $A_1 A_3 \cdots A_{M-1} A'$ are held by Alice, the registers $B_2 B_4 \cdots B_{M-2} B'$ are held by Bob, and the registers $C_1 C_2 C_3 \cdots C_M$ represent the quantum

messages exchanged by Alice and Bob. The $M+1$ isometries act on these registers as indicated below (also see Figure 1):

$$U_1^{A_{\text{in}}T^{\text{A}}\to A_1C_1}, \qquad U_2^{B_{\text{in}}T^{\text{B}}C_1\to B_2C_2}, \qquad U_3^{A_1C_2\to A_3C_3}, \qquad U_4^{B_2C_3\to B_4C_4},$$

$$\cdots, \qquad U_M^{B_{M-2}C_{M-1}\to B_{\text{out}}B'C_M}, \qquad U_{M+1}^{A_{M-1}C_M\to A_{\text{out}}A'} . \tag{2.1}$$

We adopt the convention that, at the outset, $A_0 = A_{\text{in}}T^{\text{A}}$, $B_0 = B_{\text{in}}T^{\text{B}}$; for odd i with $1 \le i < M$, $B_i = B_{i-1}$; for even i with $1 < i \le M$, $A_i = A_{i-1}$; also $B_M = B_{M+1} = B_{\text{out}}B'$, and $A_{M+1} = A_{\text{out}}A'$. In this way, after the application of U_i, Alice holds register A_i, Bob holds register B_i and the communication register is C_i. In the case of an odd number of messages M, the registers corresponding to U_M, U_{M+1} are changed appropriately. We slightly abuse notation and also write Π to denote the channel from $A_{\text{in}}B_{\text{in}}$ to $A_{\text{out}}B_{\text{out}}$ implemented by the protocol. That is, for any $\rho \in \mathcal{D}(A_{\text{in}}B_{\text{in}})$,

$$\Pi(\rho) \quad := \quad \text{Tr}_{A'B'}\left[U_{M+1}U_M \cdots U_2U_1(\rho \otimes \psi)\right] . \tag{2.2}$$

The registers A' and B' that are discarded by Alice and Bob, respectively, are two of the registers at the end of the protocol.

We restrict our attention to protocols with classical inputs XY, with $A_{\text{in}}B_{\text{in}}$ initialized to XY, and to so-called "safe protocols". Safe protocols only use $A_{\text{in}}B_{\text{in}}$ as control registers. As explained in Section 2.3, this does not affect the results presented in this article.

We imagine that the joint classical input XY is purified by a register R. We often partition the purifying register as $R = R_X R_Y$, indicating that the classical input XY, distributed as ν, and represented by the quantum state ρ_ν:

$$\rho_\nu^{XY} \quad = \quad \sum_{x,y} \nu(x,y) \, |x\rangle\langle x|^X \otimes |y\rangle\langle y|^Y \tag{2.3}$$

is purified as

$$|\rho_\nu\rangle \quad = \quad \sum_{x,y} \sqrt{\nu(x,y)} \, |xxyy\rangle^{XR_XYR_Y} . \tag{2.4}$$

We also use other partitions more appropriate for our purposes, corresponding to particular preparations of the inputs X and Y.

We define the quantum communication cost of Π from Alice to Bob as

$$\text{QCC}_{\text{A}\to\text{B}}(\Pi) \quad := \quad \sum_{0 \le i \le (M-1)/2} \log |C_{2i+1}| , \tag{2.5}$$

and the quantum communication cost of Π from Bob to Alice as

$$\text{QCC}_{\text{B}\to\text{A}}(\Pi) \quad := \quad \sum_{1 \le i \le M/2} \log |C_{2i}| , \tag{2.6}$$

where for a register D, the notation $|D|$ stands for the dimension of the state space associated with the register. The total communication cost of the protocol is then the sum of these two quantities.
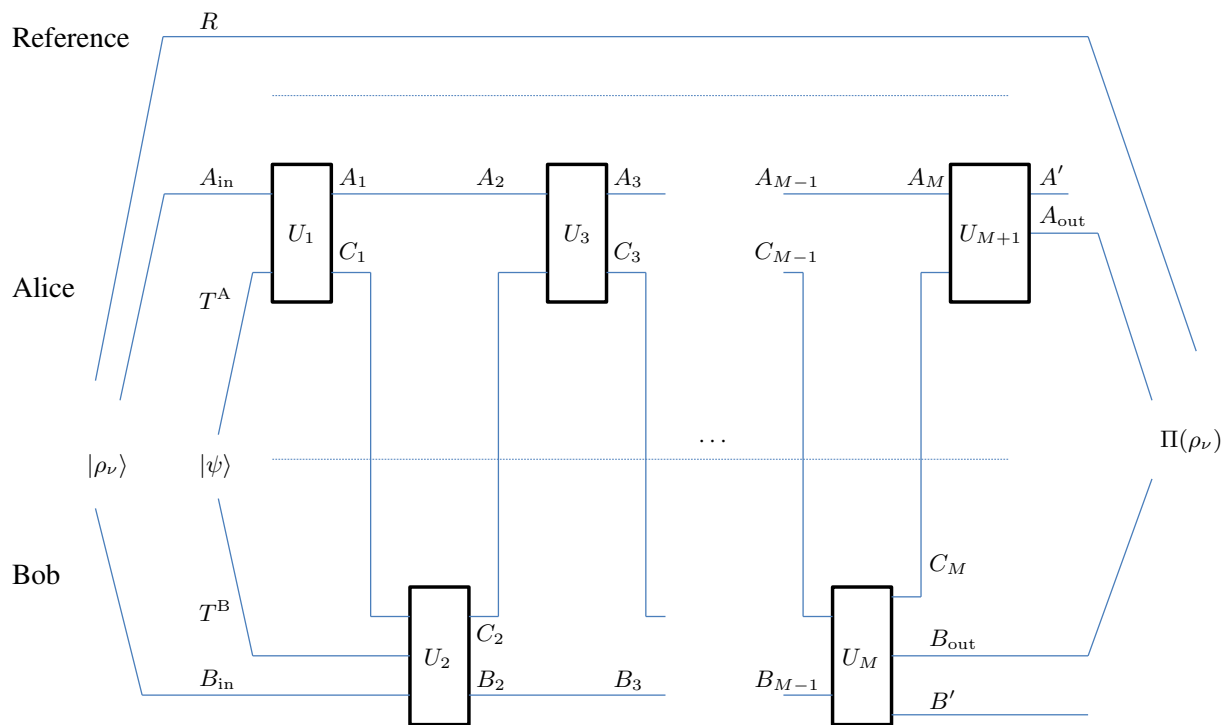
4

Figure 1: Depiction of an interactive quantum protocol, adapted from Ref. [Tou14, Figure 1], the full version of Ref. [Tou15].

2.2 Information Theory

2.2.1 Distance Measures

In order to distinguish between quantum states, we use two related distance measures: trace distance and Bures distance.

Trace Distance. The trace distance between two states ρ^A and σ^A on the same register is denoted as $\|\rho^A - \sigma^A\|_1$, where

$$\|O^A\|_1 \quad := \quad \mathrm{Tr}\left((O^\dagger O)^{\frac{1}{2}}\right) \tag{2.7}$$

is the trace norm for operators on system A. We sometimes omit the superscript if the system is clear from context. In operational terms, the trace distance between the two states ρ^A and σ^A is four times the best possible bias with which we can distinguish between the two states, given a single unknown copy of one of the two.

We use the following properties of trace distance. First, it is a metric, so it is symmetric in ρ, σ, non-negative, evaluates to 0 if and only if $\rho = \sigma$, and it satisfies the triangle inequality. Moreover, it is monotone under the action of channels: for any $\rho_1, \rho_2 \in \mathcal{D}(A)$ and channel $\mathcal{N}^{A \to B}$ from system A to system B,

$$\|\mathcal{N}(\rho_1) - \mathcal{N}(\rho_2)\|_1 \quad \leq \quad \|\rho_1 - \rho_2\|_1 \ . \tag{2.8}$$

For isometries, the inequality is tight, a property called isometric invariance of the trace distance. Hence, for any $\rho_1, \rho_2 \in \mathcal{D}(A)$ and any isometry $U^{A \to B}$, we have

$$\|U(\rho_1) - U(\rho_2)\|_1 \quad = \quad \|\rho_1 - \rho_2\|_1 \ . \tag{2.9}$$

Trace distance obeys a joint linearity property: for a classical system X and two states $\rho_1^{XA} = \sum_x p_X(x) \cdot |x\rangle\langle x|^X \otimes \rho_{1,x}^A$ and $\rho_2^{XA} = \sum_x p_X(x) \cdot |x\rangle\langle x|^X \otimes \rho_{2,x}^A$,

$$\|\rho_1 - \rho_2\|_1 \quad = \quad \sum_x p_X(x) \|\rho_{1,x} - \rho_{2,x}\|_1 \ . \tag{2.10}$$

Bures Distance. Bures distance $\mathfrak{h}$ is a fidelity based distance measure, defined for $\rho, \sigma \in \mathcal{D}(A)$ as

$$\mathfrak{h}(\rho, \sigma) \quad := \quad \sqrt{1 - \mathrm{F}(\rho, \sigma)} \ , \tag{2.11}$$

where fidelity F is defined as $\mathrm{F}(\rho, \sigma) := \|\sqrt{\rho}\sqrt{\sigma}\|_1$.

We use the following properties of Bures distance. First, it is a metric, so it is symmetric in ρ, σ; non-negative; evaluates to 0 if and only if $\rho = \sigma$; and it satisfies the triangle inequality. Moreover, it is monotone under the action of a channel: for any $\rho_1, \rho_2 \in \mathcal{D}(A)$ and quantum channel $\mathcal{N}^{A \to B}$,

$$\mathfrak{h}(\mathcal{N}(\rho_1), \mathcal{N}(\rho_2)) \quad \leq \quad \mathfrak{h}(\rho_1, \rho_2) \ . \tag{2.12}$$

For isometries, the inequality is tight, a property called isometric invariance of the Bures distance.

It is sometimes convenient to work with the square of the Bures distance. In particular, the square obeys a joint linearity property: for a classical system X and two states $\rho_1^{XA} = \sum_x p_X(x) \cdot |x\rangle\langle x|^X \otimes \rho_{1,x}^A$ and $\rho_2^{XA} = \sum_x p_X(x) \cdot |x\rangle\langle x|^X \otimes \rho_{2,x}^A$,

$$\mathfrak{h}^2(\rho_1, \rho_2) \quad = \quad \sum_x p_X(x) \cdot \mathfrak{h}^2(\rho_{1,x}, \rho_{2,x}) \ . \tag{2.13}$$

It also satisfies a weaker version of the triangle inequality: for any ρ_1, ρ_2 and $\sigma \in \mathcal{D}(A)$,

$$\mathfrak{h}^2(\rho_1, \rho_2) \quad \leq \quad 2\,\mathfrak{h}^2(\rho_1, \sigma) + 2\,\mathfrak{h}^2(\sigma, \rho_2) \quad . \tag{2.14}$$

Local Transition Lemma. The following lemma, a direct consequence of the Uhlmann theorem, is called the local transition lemma [KNTZ07], especially when expressed in terms of other metrics.

Lemma 1 *Let ρ_1, $\rho_2 \in \mathcal{D}(A)$ have purifications $\rho_1^{AR_1}$, $\rho_2^{AR_2}$, with $|R_1| \leq |R_2|$. Then, there exists an isometry $V^{R_1 \to R_2}$ such that*

$$\mathfrak{h}\big(\rho_1^A, \rho_2^A\big) \quad = \quad \mathfrak{h}\Big(V\big(\rho_1^{AR_1}\big), \rho_2^{AR_2}\Big) . \tag{2.15}$$

Bures distance is related to trace distance through a generalization of the Fuchs-van de Graaf inequalities [FvdG99]: for any $\rho_1, \rho_2 \in \mathcal{D}(A)$, it holds that

$$\mathfrak{h}^2(\rho_1, \rho_2) \quad \leq \quad \frac{1}{2}\,\|\rho_1 - \rho_2\|_1 \quad \leq \quad \sqrt{2}\,\mathfrak{h}(\rho_1, \rho_2) \quad . \tag{2.16}$$

2.2.2 Information Measures

In order to quantify the information content of a quantum state, we use a basic measure, von Neumann entropy, defined as

$$\mathrm{H}(A)_\rho \quad := \quad -\operatorname{Tr}\left(\rho \log \rho\right)$$

for any state $\rho \in \mathcal{D}(A)$. Here, we follow the convention that $0 \log 0 = 0$, which is justified by a continuity argument. The logarithm is in base 2. Note that H is invariant under isometries applied on ρ. If the state in question is clear from the context, we may omit the subscript. We also note that if system A is classical, then von Neumann entropy reduces to Shannon entropy.

For a state $\rho^{ABC} \in \mathcal{D}(ABC)$, the mutual information between registers A, B is defined as

$$\mathrm{I}(A\!:\!B)_\rho \quad := \quad \mathrm{H}(A) + \mathrm{H}(B) - \mathrm{H}(AB) \quad ,$$

and the conditional mutual information between them, given C, as

$$\mathrm{I}(A\!:\!B\,|\,C)_\rho \quad := \quad \mathrm{I}(A\!:\!BC) - \mathrm{I}(A\!:\!C) \quad .$$

If X is a classical system, $\mathrm{I}(X\!:\!B)$ is also called the Holevo information.

Mutual information and conditional mutual information are symmetric in A, B, and invariant under a local isometry applied to A, B or C. Since all purifications of a state are equivalent up to an isometry on the purification registers, we have that for any two pure states $|\phi\rangle^{ABCR'}$ and $|\psi\rangle^{ABCR}$ such that $\phi^{ABC} = \psi^{ABC}$,

$$\mathrm{I}(C\!:\!R'\,|\,B)_\phi \quad = \quad \mathrm{I}(C\!:\!R\,|\,B)_\psi \quad . \tag{2.17}$$

For any state $\rho \in \mathcal{D}(ABC)$, we have the bounds

$$0 \quad \leq \quad \mathrm{H}(A) \quad \leq \quad \log|A| \quad , \tag{2.18}$$

$$0 \quad \leq \quad \mathrm{I}(A\!:\!B\,|\,C) \quad \leq \quad 2\,\mathrm{H}(A) \quad . \tag{2.19}$$

For a multipartite quantum system $ABCD$, conditional mutual information satisfies a chain rule: for any $\rho \in \mathcal{D}(ABCD)$,

$$\mathrm{I}(AB\!:\!C\,|\,D) \quad = \quad \mathrm{I}(A\!:\!C\,|\,D) + \mathrm{I}(B\!:\!C\,|\,AD) \ . \tag{2.20}$$

For any product state $\rho^{A_1 B_1 A_2 B_2} := \rho_1^{A_1 B_1} \otimes \rho_2^{A_2 B_2}$, entropy is additive across the bi-partition, so that, for example,

$$\mathrm{H}(A_1 A_2) \quad = \quad \mathrm{H}(A_1) + \mathrm{H}(A_2) \ , \tag{2.21}$$

and the conditional mutual information between product systems vanishes:

$$\mathrm{I}(A_1\!:\!A_2\,|\,B_1 B_2) \quad = \quad 0 \ . \tag{2.22}$$

Two important properties of the conditional mutual information are non-negativity and the data processing inequality, both equivalent to a deep result in quantum information theory known as strong subadditivity [LR73]. For any state $\rho \in \mathcal{D}(ABC)$, channel $\mathcal{N}^{B \to B'}$, and state $\sigma := \mathcal{N}(\rho)$, we have

$$\mathrm{I}(A\!:\!B\,|\,C)_\rho \quad \geq \quad 0, \tag{2.23}$$
$$\mathrm{I}(A\!:\!B\,|\,C)_\rho \quad \geq \quad \mathrm{I}(A\!:\!B'\,|\,C)_\sigma \ . \tag{2.24}$$

For classical systems, conditioning is equivalent to taking an average: for any $\rho^{ABCX} := \sum_x p_X(x) \cdot |x\rangle\langle x|^X \otimes \rho_x^{ABC}$ with a classical system X and some appropriate $\rho_x \in \mathcal{D}(ABC)$,

$$\mathrm{I}(A\!:\!B\,|\,CX)_\rho \quad = \quad \sum_x p_X(x) \cdot \mathrm{I}(A\!:\!B\,|\,C)_{\rho_x} \ . \tag{2.25}$$

Average Encoding Theorem. The following lemma, known as the Average Encoding Theorem [KNTZ07], formalizes the intuition that if a classical and a quantum registers are weakly correlated, then they are nearly independent.

Lemma 2 *For any $\rho^{XA} = \sum_x p_X(x) \cdot |x\rangle\langle x|^X \otimes \rho_x^A$ with a classical system X and states $\rho_x \in \mathcal{D}(A)$,*

$$\sum_x p_X(x) \cdot \mathfrak{h}^2\big(\rho_x^A, \rho^A\big) \quad \leq \quad \mathrm{I}(X\!:\!A)_\rho \ . \tag{2.26}$$

Fawzi-Renner inequality. We use the following breakthrough result by Fawzi and Renner [FR15]. It provides a lower bound on the quantum conditional mutual information in terms of the fidelity for the optimal recovery map.

Lemma 3 *For any tripartite quantum state ρ^{ACR}, there exists a recovery map $\mathcal{R}^{A \to AC}$ from register A to registers AC satisfying*

$$\mathrm{I}(C\!:\!R\,|\,A) \quad \geq \quad -2 \cdot \log_2 \mathrm{F}(\rho^{ACR}, \mathcal{R}(\rho^{AR})) \ . \tag{2.27}$$

In particular, it follows that

$$\mathrm{I}(C\!:\!R\,|\,A) \quad \geq \quad \mathfrak{h}^2\big(\rho^{ACR}, \mathcal{R}(\rho^{AR})\big) \ . \tag{2.28}$$

2.3 Quantum Information Complexity

We rely on the notion of quantum information cost of a two-party communication protocol introduced by Touchette [Tou15]. We follow the notation associated with a two-party quantum communication protocol introduced in Section 2.1, and restrict ourselves to protocols with classical inputs XY distributed as ν.

Quantum information cost is defined in terms of the purifying register R, but is independent of the choice of purification. Given the asymmetric nature of the Augmented Index function, we consider the quantum information cost of messages from Alice to Bob and the ones from Bob to Alice separately. Such an asymmetric notion of quantum information cost was previously considered in Refs. [KLGR16, LT16].

Definition 1 *Given a quantum protocol Π with classical inputs distributed as ν, the* quantum information cost *(of the messages) from Alice to Bob is defined as*

$$\mathrm{QIC}_{\mathrm{A}\to\mathrm{B}}(\Pi,\nu) \quad = \quad \sum_{i \text{ odd}} \mathrm{I}(R\!:\!C_i \,|\, B_i) \ , \tag{2.29}$$

and the quantum information cost *(of the messages) from Bob to Alice is defined as*

$$\mathrm{QIC}_{\mathrm{B}\to\mathrm{A}}(\Pi,\nu) \quad = \quad \sum_{i \text{ even}} \mathrm{I}(R\!:\!C_i \,|\, A_i) \ . \tag{2.30}$$

It is immediate that quantum information cost is bounded above by quantum communication.

Remark 1 *For any quantum protocol Π with classical inputs distributed as ν, the following holds:*

$$\mathrm{QIC}_{\mathrm{A}\to\mathrm{B}}(\Pi,\nu) \quad \leq \quad 2\,\mathrm{QCC}_{A\to B}(\Pi) \ , \tag{2.31}$$
$$\mathrm{QIC}_{\mathrm{B}\to\mathrm{A}}(\Pi,\nu) \quad \leq \quad 2\,\mathrm{QCC}_{B\to A}(\Pi) \ . \tag{2.32}$$

As a result, we may bound quantum communication complexity of a protocol from below by analysing its information cost.

We further restrict ourselves to "safe protocols", in which the registers $A_{\mathrm{in}}, B_{\mathrm{in}}$ are only used as control registers in the local isometries. This restriction does not affect the results in this article, for the following reason. Let Π be any protocol with classical inputs distributed as ν, in which the two parties may apply arbitrary isometries to their quantum registers. In particular, these registers include $A_{\mathrm{in}}, B_{\mathrm{in}}$ which are initialized to the input. Let Π' be the protocol with the same registers as Π and two additional quantum registers $A'_{\mathrm{in}}, B'_{\mathrm{in}}$ of the same sizes as $A_{\mathrm{in}}, B_{\mathrm{in}}$, respectively. In the protocol Π', the two parties each make a coherent local copy of their inputs into $A'_{\mathrm{in}}, B'_{\mathrm{in}}$, respectively, at the outset. The registers $A'_{\mathrm{in}}, B'_{\mathrm{in}}$ are never touched hereafter, and the two parties simulate the original protocol Π on the remaining registers. Laurière and Touchette [LT16] show that the quantum information cost of Π is at least as much as that of the protocol Π':

$$\mathrm{QIC}_{\mathrm{A}\to\mathrm{B}}(\Pi',\nu) \quad \leq \quad \mathrm{QIC}_{\mathrm{A}\to\mathrm{B}}(\Pi,\nu) \ , \qquad \text{and}$$
$$\mathrm{QIC}_{\mathrm{B}\to\mathrm{A}}(\Pi',\nu) \quad \leq \quad \mathrm{QIC}_{\mathrm{B}\to\mathrm{A}}(\Pi,\nu) \ .$$

Thus, the quantum information cost trade-off we show for safe protocols holds for arbitrary protocols as well.

We use another result due to Laurière and Touchette [LT16]. The result states that the total gain in (conditional) information by a party over all the messages is precisely the net (conditional) information gain in the protocol. It allows us to keep track of the flow of information during interactive quantum protocols. For completeness, a proof is provided in Appendix B.

Lemma 4 (Information Flow Lemma) *Given a protocol* Π, *an input state* ρ *with purifying register R with arbitrary decompositions* $R = R_a^{\mathrm{A}} R_b^{\mathrm{A}} R_c^{\mathrm{A}} = R_a^{\mathrm{B}} R_b^{\mathrm{B}} R_c^{\mathrm{B}}$, *the following hold:*

$$\sum_{i \geq 0} \mathrm{I}(R_a^{\mathrm{B}} : C_{2i+1} \mid R_b^{\mathrm{B}} B_{2i+1}) - \sum_{i \geq 1} \mathrm{I}(R_a^{\mathrm{B}} : C_{2i} \mid R_b^{\mathrm{B}} B_{2i})$$
$$= \mathrm{I}(R_a^{\mathrm{B}} : B_{\mathrm{out}} B' \mid R_b^{\mathrm{B}}) - \mathrm{I}(R_a^{\mathrm{B}} : B_{\mathrm{in}} \mid R_b^{\mathrm{B}}) \ , \quad and$$

$$\sum_{i \geq 0} \mathrm{I}(R_a^{\mathrm{A}} : C_{2i+2} \mid R_b^{\mathrm{A}} A_{2i+2}) - \sum_{i \geq 0} \mathrm{I}(R_a^{\mathrm{A}} : C_{2i+1} \mid R_b^{\mathrm{A}} A_{2i+1})$$
$$= \mathrm{I}(R_a^{\mathrm{A}} : A_{\mathrm{out}} A' \mid R_b^{\mathrm{A}}) - \mathrm{I}(R_a^{\mathrm{A}} : A_{\mathrm{in}} \mid R_b^{\mathrm{A}}) \ .$$

2.4 Quantum Streaming Algorithms

We refer the reader to the text [Mut05] for an introduction to classical streaming algorithms. Quantum streaming algorithms are similarly defined, with restricted access to the input, and with limited workspace.

In more detail, an input $x \in \Sigma^n$, where Σ is some alphabet, arrives as a *data stream*, i.e., letter by letter in the order $x_1, x_2, \ldots, x_n$. An algorithm is said to make a *pass* on the input, when it reads the data stream once in this order, processing it as described next. For an integer $T \geq 1$, a T-pass (unidirectional) *quantum streaming algorithm* $\mathcal{A}$ with space $s(n)$ and time $t(n)$ is a collection of quantum channels $\{\mathcal{A}_{i\sigma} : i \in [T], \sigma \in \Sigma\}$. Each operator $\mathcal{A}_{i\sigma}$ is a channel defined on a register of $s(n)$-qubits, and can be implemented by a uniform family of circuits of size at most $t(n)$. On input stream $x \in \Sigma^n$,

1. The algorithm starts with a register W of $s(n)$ qubits, all initialized to a fixed state, say $|0\rangle$.

2. $\mathcal{A}$ performs T sequential passes, $i = 1, \ldots, T$, on x in the order $x_1, x_2, \ldots, x_n$.

3. In the ith pass, when symbol σ is read, channel $\mathcal{A}_{i\sigma}$ is applied to W.

4. The output of the algorithm is the state in a designated sub-register W_{out} of W, at the end of the T passes.

We may allow for some pre-processing before the input is read, and some post-processing at the end of the T passes, each with time complexity different from $t(n)$. As our work applies to streaming algorithms with any time complexity, we do not consider this refinement.

The probability of correctness of a streaming algorithm is defined in the standard way. If we wish to compute a family of Boolean functions $g_n : \Sigma^n \to \{0, 1\}$, the output register W_{out} consists of a single qubit. On input x, let $\mathcal{A}(x)$ denote the random variable corresponding to the outcome when the output register is measured in the standard basis. We say $\mathcal{A}$ computes g_n with (worst-case) error $\varepsilon \in [0, 1/2]$ if for all x, $\Pr[\mathcal{A}(x) = g_n(x)] \geq 1 - \varepsilon$.

In general, the implementation of a quantum channel used by a streaming algorithm with unitary operations involves one-time use of ancillary qubits (initialized to a fixed, known quantum state, say $|0\rangle$). These ancillary qubits are in addition to the $s(n)$-qubit register that is maintained by the algorithm. Fresh qubits may be an expensive resource in practice, for example, in NMR implementations, and one may argue that they be included in the space complexity of the algorithm. The lack of ancillary qubits severely restricts the kind of computations space-bounded algorithms can perform; see, for example, Ref. [ANTV02]. We choose the definition above so as to present the results we derive in the strongest possible model. Thus, the results

also apply to implementations in which the "flying qubits" needed for implementing non-unitary quantum channels are relatively easy to prepare.

In the same vein, we may provide a quantum streaming algorithm arbitrary read-only access to a sequence of random bits. In other words, we may also provide the algorithm with a register S of size at most $t(n)$ initialized to random bits from some distribution. Each quantum channel $\mathcal{A}_{i\sigma}$ now operates on registers SW, while using S only as a control register. The bounds we prove hold in this model as well.

3 Reduction from Augmented Index to DYCK(2)

The connection between low-information protocols for Augmented Index and streaming algorithms for DYCK(2) contains two steps. The first is a reduction from an intermediate multi-party communication problem ASCENSION, and the second is the relationship of the latter with Augmented Index.

3.1 Reduction from ASCENSION to DYCK(2)

In this section, we describe the connection between multi-party quantum communication protocols for the problem ASCENSION(m, n), and quantum streaming algorithms for DYCK(2). The reduction is an immediate generalization of the one in the classical case discovered by Magniez, Mathieu, and Nayak [MMN14], which also works with appropriate modifications for multi-pass classical streaming algorithms [CCKM13, JN14]. For the sake of completeness, we describe the reduction below.

Multi-party quantum communication protocols involving point-to-point communication may be defined as in the two-party case. As it is straightforward, and detracts from the thrust of this section, we omit a formal definition.

Let m, n be positive integers. The $(2m)$-party communication problem ASCENSION(m, n) consists of computing the logical OR of m independent instances of f_n, the Augmented Index function. Suppose we denote the $2m$ parties by $\mathsf{A}_1, \mathsf{A}_2, \ldots, \mathsf{A}_m$ and $\mathsf{B}_1, \mathsf{B}_2, \ldots, \mathsf{B}_m$. Player A_i is given $x^i \in \{0, 1\}^n$, player B_i is given $k^i \in [n]$, a bit z^i, and the prefix $x^i[1, k^i - 1]$ of x^i. Let $\mathbf{x} = (x^1, x^2, \ldots, x^m)$, $\mathbf{k} = (k^1, k^2, \ldots, k^m)$, and $\mathbf{z} = (z^1, z^2, \ldots, z^m)$. The goal of the communication protocol is to compute

$$F_{m,n}(\mathbf{x}, \mathbf{k}, \mathbf{z}) \quad = \quad \bigvee_{i=1}^{m} f_n(x^i, k^i, z^i) \quad = \quad \bigvee_{i=1}^{m} (x^i[k^i] \oplus z^i) \ ,$$

which is 0 if $x^i[k^i] = z^i$ for all i, and 1 otherwise.

The communication between the $2m$ parties is required to be T sequential iterations of communication in the following order, for some $T \geq 1$:

$$\mathsf{A}_1 \to \mathsf{B}_1 \to \mathsf{A}_2 \to \mathsf{B}_2 \to \cdots \mathsf{A}_m \to \mathsf{B}_m$$
$$\to \mathsf{A}_m \to \mathsf{A}_{m-1} \to \cdots \to \mathsf{A}_2 \to \mathsf{A}_1 \ . \tag{3.1}$$

In other words, for $t = 1, 2, \ldots, T$,

- for i from 1 to $m - 1$, player A_i sends register $C_{\mathsf{A}_i, t}$ to B_i, then B_i sends register $C_{\mathsf{B}_i, t}$ to A_{i+1},

- A_m sends register $C_{\mathsf{A}_m, t}$ to B_m, then B_m sends register $C_{B_m, t}$ to A_m,

- for i from m down to 2, A_i sends register $C'_{\mathsf{A}_i, t}$ to A_{i-1}.
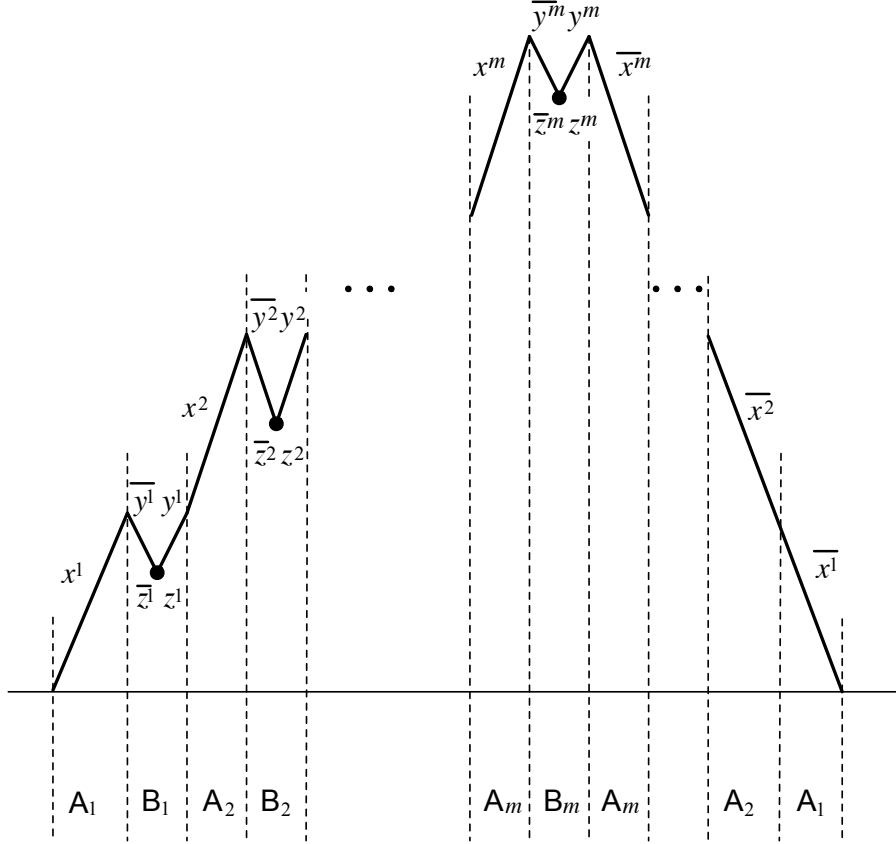
Figure 2: An instance of the form described in (3.2), as depicted in [MMN14, JN14]. A line segment with positive slope denotes a string over $\{a, b\}$, and a segment with negative slope denotes a string over $\{\overline{a}, \overline{b}\}$. A solid dot depicts a pair of the form $\overline{z}z$ for some $z \in \{a, b\}$. The entire string is distributed amongst $2m$ players $A_1, B_1, A_2, B_2, \ldots, A_m, B_m$ in a communication protocol for ASCENSION(m, n) as shown.

At the end of the T iterations, A_1 computes the output.

There is a bijection between instances of ASCENSION(m, n) and a subset of instances of DYCK(2) that we describe next. For any string $z = z_1 \cdots z_n \in \{a, b\}^n$, let $\overline{z}$ denote the matching string $\overline{z_n}\, \overline{z_{n-1}} \cdots \overline{z_1}$ corresponding to z. Let $z[i, j]$ denote the substring $z_i z_{i+1} \cdots z_j$ if $1 \le i \le j \le n$, and the empty string ε otherwise. We abbreviate $z[i, i]$ as $z[i]$ if $1 \le i \le n$. Consider strings of the form

$$w \quad = \quad (x^1\, \overline{y^1}\, \overline{z^1}\, z^1\, y^1)\, (x^2\, \overline{y^2}\, \overline{z^2}\, z^2\, y^2) \cdots (x^m\, \overline{y^m}\, \overline{z^m}\, z^m\, y^m)\, \overline{x^m} \cdots \overline{x^2}\, \overline{x^1} \ , \qquad (3.2)$$

where for every i, $x^i \in \{a, b\}^n$, and y^i is a suffix of x^i, i.e., $y^i = x^i[n - k^i + 2, n]$ for some $k^i \in \{1, 2, \ldots, n\}$, and $z^i \in \{a, b\}$. The string w is in DYCK(2) if and only if, for every i, $z^i = x^i[n - k^i + 1]$. Note that these instances have length in the interval $[2m(n + 1), 4mn]$.

The bijection between instances of ASCENSION(m, n) and DYCK(2) arises from a partition of the string w amongst the $2m$ players: player A_i is given x^i (and therefore $\overline{x^i}$), and player B_i is given y^i, z^i (and therefore $\overline{y^i}, \overline{z^i}$). See Figure 2 for a pictorial representation of the partition. For ease of notation, the strings x^i in ASCENSION(m, n) are taken to be the ones in DYCK(2) with the bits *in reverse order*. This converts the suffixes y^i into prefixes of the same length.

As a consequence of the bijection above, any quantum streaming algorithm for DYCK(2) results in a quantum protocol for ASCENSION(m, n), as stated in the following lemma.

Lemma 5 *For any $\varepsilon \in [0, 1/2]$, $n, m \in \mathbb{N}$, and for any ε-error (unidirectional) T-pass quantum streaming algorithm $\mathcal{A}$ for DYCK(2) that on instances of size $N \in \Theta(mn)$ uses $s(N)$ qubits of memory, there exists an ε-error, T-round sequential $(2m)$-party quantum communication protocol for ASCENSION(m, n) in which each message is of length $s(N)$. The protocol may use public randomness, but does not use pre-shared entanglement between any of the parties. Moreover, the local operations of the parties are memory-less, i.e., do not require access to the qubits used in generating the previous messages.*

Proof. Any random sequence of bits used by the streaming algorithm is provided as shared randomness to all the $2m$ parties in the communication protocol for ASCENSION(m, n). Each input for the communication problem corresponds to an instance of DYCK(2), as described above. In each of the T iterations, a player simulates the quantum streaming algorithm on appropriate part of the input for DYCK(2), and sends the length $s(N)$ workspace to the next player in the sequence. (If needed, non-unitary quantum operations may be replaced with an isometry, as follows from the Stinespring Representation theorem [Wat15].) The output of the protocol is the output of algorithm, and is contained in the register held by the final party A_1. ∎

3.2 Reduction from Augmented Index to ASCENSION

Recall that ASCENSION(m, n) is composed of m instances of Augmented Index on n bits. Magniez, Mathieu, and Nayak [MMN14] showed how we may derive a low-information classical protocol for Augmented Index f_n from one for ASCENSION(m, n) through a direct sum argument (see Refs. [CCKM13, JN14] for the details of its working in the multi-pass case). This is not as straightforward to execute as it might first appear; it entails deriving a sequence of protocols for Augmented Index in which the communication from Alice to Bob corresponds to messages from different parties in the original multi-party protocol. We show that the same kind of construction, suitably adapted to the notion of quantum information cost we use, also works in the quantum case.

Let μ_0 be the uniform distribution on the 0-inputs of the Augmented Index function f_n. If X is a uniformly random n-bit string, K is a uniformly random index from $[n]$ independent of X, and the random variable B is set as $B = X_K$, the joint distribution of $X, K, X[1, K-1], B$ is μ_0. We denote the random variables $K, X[1, K-1], B$ given as input to Bob by Y. Since $X_K = B$ under this distribution, we abbreviate Bob's input as $K, X[1, K]$. Let μ be the uniform distribution over all inputs. Under this distribution, the bit B is uniformly random, independent of XK, while XK are as above.

Lemma 6 *Suppose $\varepsilon \in [0, 1/2]$, $n, m \in \mathbb{N}$ and that there is an ε-error, T-round sequential quantum protocol Π_{Asc} for ASCENSION(m, n), that is memory-less, does not have pre-shared entanglement between any of the parties (but might use public randomness), and only has messages of length at most s (cf. Lemma 5). Then, there exists an ε-error, $2T$-message, two-party quantum protocol Π_{AI} for the Augmented Index function f_n that satisfies*

$$\mathrm{QIC}_{\mathrm{A} \to \mathrm{B}}(\Pi_{\mathrm{AI}}, \mu_0) \leq 2sT \,, \tag{3.3}$$

$$\mathrm{QIC}_{\mathrm{B} \to \mathrm{A}}(\Pi_{\mathrm{AI}}, \mu_0) \leq 2sT/m \,. \tag{3.4}$$

Proof. Starting from the $(2m)$-party protocol Π_{Asc} for ASCENSION(m, n), we construct a protocol Π_j for f_n, for each $j \in [m]$.

Fix one such j. Suppose Alice and Bob get inputs x and y, respectively, where $y := (k, x[1, k-1], b)$. They embed these into an instance of ASCENSION(m, n): they set $x_j = x$, and $y_j = y$. They sample the inputs for the remaining $m - 1$ coordinates independently, according to μ_0. Let $X_i Y_i$, with $Y_i = (K_i, X_i[1, K_i])$, be registers corresponding to inputs drawn from μ_0 in coordinate i. Let R_i be a purification register for these, which we may decompose as $R_i^X R_i^Y$, denoting the standard purification of the $X_i Y_i$ registers. Let $S_A S_B$ be registers initialized to $\sum_s \sqrt{\nu_s} |ss\rangle$, so as to simulate the public random string $S \sim \nu$ used in the protocol Π_{Asc}.

For each $i \neq j$, we give X_i to Alice, and $(K_i, X_i[1, K_i])$ to Bob. For $i > j$, we give R_i to Bob, and for $i < j$, we give R_i to Alice. Then Alice and Bob simulate the roles of the $2m$ parties $(A_i, B_i)_{i \in [m]}$ in the following way for each of the T rounds in Π_{Asc}. For $t = 1, 2, \ldots, T$:

1. Alice simulates $A_1 \to B_1 \to A_2 \to \cdots \to A_j$, accessing the inputs for B_i, for $i < j$, in the register R_i. We denote the ancillary register she uses to simulate A_1's local isometry by D_{t1}, and for all other $i < j$, the ancillary registers she uses for B_i and A_{i+1} together by D_{ti}.

2. Alice transmits the message from A_j to B_j to Bob.

3. Bob simulates $B_j \to A_{j+1} \to \cdots \to B_m$, accessing the input for A_i, for $i > j$, in the register R_i. For all i such that $j \leq i < m$ we denote the ancillary registers Bob uses for simulating B_i and A_{i+1}'s local isometry together by D_{ti}, and the ancillary register he uses for B_m by D_{tm}.

4. Bob transmits the message from B_m to A_m to Alice.

5. Alice simulates $A_m \to A_{m-1} \to \cdots \to A_1$. We denote the ancillary registers Alice uses for simulating the local isometries of $A_m, A_{m-1}, \ldots, A_1$ by E_t.

We let E_0 denote a dummy register initialized to a fixed state, say $|0\rangle$.

Since the inputs for Augmented Index for $i \neq j$ are distributed according to μ_0, the protocol Π_j computes Augmented Index for the instance (x, y) with error at most ε.

The quantum information cost from Alice to Bob $\text{QIC}_{A \to B}(\Pi_j, \lambda)$ is bounded by $2sT$, for any distribution λ over the inputs, as each of her T messages has at most s qubits.

The bound on quantum information cost from Bob to Alice arises from the following direct sum result. Suppose that the inputs for the protocol Π_j for Augmented Index are drawn from the distribution μ_0. Denote these inputs by $X_j Y_j$, with $Y_j = (K_j, X_j[1, K_j])$, and the corresponding purification register by R_j. We are interested in the quantum information cost $\text{QIC}_{B \to A}(\Pi_j, \mu_0)$.

For $t \in [T]$, let C_t denote the tth message from Bob to Alice in the protocol Π_j. At the time Alice receives message C_t, her other registers are $X_1 \cdots X_m, S_A, R_1 \cdots R_{j-1}, (E_{r-1} D_{r1} D_{r2} \cdots D_{rj})_{r \in [t]}$. Note that the corresponding state ρ_t at that point on registers

$$X_1 \cdots X_m \ S_A \ (E_{r-1} D_{r1} D_{r2} \cdots D_{rm})_{r \in [t]} \ R_1 \cdots R_m \ C_t$$

is the same for all derived protocols Π_j, as all of them simulate Π_{Asc} on the same input distribution $\mu_0^{\otimes m}$, using the above registers.

We have

$$\mathrm{QIC}_{\mathrm{B}\to\mathrm{A}}(\Pi_j, \mu_0)$$
$$= \sum_{t\in[T]} \mathrm{I}(R_j : C_t \mid X_1\cdots X_m S_{\mathrm{A}}(E_{r-1}D_{r1}D_{r2}\cdots D_{rj})_{r\in[t]} R_1\cdots R_{j-1})_{\rho_t}$$
$$\leq \sum_{t\in[T]} \mathrm{I}(R_j(D_{rj})_{r\in[t]} : C_t \mid X_1\cdots X_m S_{\mathrm{A}}(E_{r-1}D_{r1}D_{r2}\cdots D_{r(j-1)})_{r\in[t]} R_1\cdots R_{j-1})_{\rho_t} .$$

Using the chain rule, we get

$$\sum_{j\in[m]} \mathrm{QIC}_{\mathrm{B}\to\mathrm{A}}(\Pi_j, \mu_0)$$
$$\leq \sum_{t\in[T]} \mathrm{I}(R_1\cdots R_m(D_{r1}D_{r2}\cdots D_{rm})_{r\in[t]} : C_t \mid X_1\cdots X_m S_{\mathrm{A}}(E_{r-1})_{r\in[t]})_{\rho_t} .$$

Since each summand in the expression above is bounded by $2\log|C_t| \leq 2s$, we have that the sum is bounded by $2sT$. It follows that there exists an index j^* such that

$$\mathrm{QIC}_{\mathrm{B}\to\mathrm{A}}(\Pi_{j^*}, \mu_0) \quad \leq \quad 2sT/m , \tag{3.5}$$

as desired. As noted before, $\mathrm{QIC}_{\mathrm{A}\to\mathrm{B}}(\Pi_{j^*}, \mu_0) \leq 2sT$. This completes the reduction. ∎

4   QIC Lower Bound for Augmented Index

In this section, we develop the tools needed to analyze the quantum information cost of protocols for Augmented Index, and then establish a lower bound for this cost.

Throughout this section, we deviate slightly from the notation for the registers used in the definition of two-party protocols presented in Section 2.1; we adapt it for safe quantum protocols with classical inputs. We refer to the input registers $A_{\mathrm{in}}, B_{\mathrm{in}}$ by X, Y, respectively. Since we focus on safe protocols, the registers XY are only used as control registers. We express Alice's local registers after the ith message is generated as XA_i, and the local registers of Bob by YB_i. As before, the message register is not included in any of the local registers, and is denoted by C_i.

4.1   Superposition-Average Encoding Theorem

We first generalize the Average Encoding Theorem [KNTZ07], to relate the quality of approximation of any intermediate state in a two-party quantum communication protocol to its information cost. This also allows us to analyze states arising from arbitrary superpositions over inputs in such protocols. Informally, the resulting statement is that if the (incremental) information contained in the messages received by a party is "small", then she can approximate the message entirely on her own correspondingly well. The main technical ingredient of its proof is the Fawzi-Renner inequality [FR15].

Theorem 3 (Superposition-Average Encoding Theorem) *Given any safe quantum protocol* Π *with input registers* XY *initialized according to distribution* ν, *let*

$$|\rho_i\rangle = \sum_{x,y} \sqrt{\nu(x,y)} |xxyy\rangle^{XR_X Y R_Y} |\rho_i^{xy}\rangle^{A_i B_i C_i}$$

be the state on registers $XYRA_iB_iC_i$ in round i with the register R initially purifying the registers XY, with a decomposition R_XR_Y into coherent copies of X and Y, respectively. Let $\varepsilon_i := \mathrm{I}(R\!:\!C_i\,|\,YB_i)$ for odd i, and $\varepsilon_i := \mathrm{I}(R\!:\!C_i\,|\,XA_i)$ for even i. There exist registers E_i, isometries V_i and states

$$|\theta_i\rangle \;=\; \sum_{x,y}\sqrt{\nu(x,y)}\,|xxyy\rangle^{XR_XYR_Y}\,|\theta_i^y\rangle^{B_iC_iE_i}$$

for odd i satisfying

$$\mathfrak{h}\!\left(\rho_i^{RYB_iC_i},\theta_i^{RYB_iC_i}\right) \;\leq\; \sum_{p\leq i,\,p\text{ odd}}\sqrt{\varepsilon_p}\;, \qquad \text{and}$$

$$V_i\,|y\rangle^Y \;=\; |y\rangle^Y\otimes|\theta_i^y\rangle^{B_iC_iE_i}\;,$$

and states

$$|\sigma_i\rangle \;=\; \sum_{x,y}\sqrt{\nu(x,y)}\,|xxyy\rangle^{XR_XYR_Y}\,|\sigma_i^x\rangle^{A_iC_iE_i}$$

for even i satisfying

$$\mathfrak{h}\!\left(\rho_i^{RXA_iC_i},\sigma_i^{RXA_iC_i}\right) \;\leq\; \sum_{p\leq i,\,p\text{ even}}\sqrt{\varepsilon_p}\;, \qquad \text{and}$$

$$V_i\,|x\rangle^X \;=\; |x\rangle^X\otimes|\sigma_i^x\rangle^{A_iC_iE_i}\;.$$

Proof. The result for odd and even i's is proved similarly; we focus on even i's. Given $\varepsilon_p = \mathrm{I}(R\!:\!C_p\,|\,XA_p)$ for even p, let $\mathcal{R}_p^{XA_p\to XA_pC_p}$ be the recovery map given by the Fawzi-Renner inequality, Lemma 3, such that

$$\mathfrak{h}\!\left(\rho_p^{RXA_pC_p},\mathcal{R}_p(\rho_p^{RXA_p})\right) \;\leq\; \sqrt{\varepsilon_p}\;,$$

and take $U_{\mathcal{R}_p}^{XA_p\to XA_pC_pF_p}$ to be an isometric extension of $\mathcal{R}_p$. Since register R contains a coherent copy of X, we can assume without loss of generality that $U_{\mathcal{R}_p}^{XA_p\to XA_pC_pF_p}$ is of the form

$$U_{\mathcal{R}_p}^{XA_p\to XA_pC_pF_p}\,|x\rangle^X\,|\phi_x\rangle^{A_pG_p} \;=\; |x\rangle^X\,|\phi_x'\rangle^{A_pC_pF_pG_p}\;,$$

for any ancillary register G_p. I.e., X is used only as a control register. Consider an isometry $V_0^{X\to XT_AT_B}$ such that for all x,

$$V_0\,|x\rangle^X \;=\; |x\rangle^X\,|\psi\rangle^{T_AT_B}\;,$$

i.e., V_0 is an isometry that locally creates the same state $|\psi\rangle^{T_AT_B}$, used as pre-shared entanglement in Π, for any input x. Let ρ_ν denote the purified initial state of the protocol:

$$|\rho_\nu\rangle \;:=\; \sum_{x,y}\sqrt{\nu(x,y)}\,|xxyy\rangle^{XR_XYR_Y}\;.$$

We show that the isometry V_i, state σ_i, and register E_i defined as follows

$$\begin{aligned}
V_i &:= U_{\mathcal{R}_i} U_{i-1} \cdots U_{\mathcal{R}_4} U_3 U_{\mathcal{R}_2} U_1 V_0 ~, \\
|\sigma_i\rangle &:= V_i |\rho_\nu\rangle ~, \qquad \text{and} \\
E_i &:= T_{\mathrm{B}} \otimes C_1 \otimes F_2 \otimes C_3 \otimes F_4 \otimes \cdots \otimes C_{i-1} \otimes F_i
\end{aligned}$$

satisfy the conditions of the theorem. We show this by induction on i.

First, note that V_i is of the desired form, and uses X as a control register. For the base case, $i = 2$, we start with

$$|\rho_0\rangle^{XYR_XR_YT_AT_B} = V_0 |\rho_\nu\rangle^{XYR_XR_Y} ~,$$

apply $U_1^{XT_A \to XA_1C_1}$ to obtain $|\rho_1\rangle^{XYR_XR_YA_1C_1T_B}$, and furthermore apply $U_2^{YC_1T_B \to YC_2B_2}$ to obtain $|\rho_2\rangle = U_2 U_1 V_0 |\rho_\nu\rangle^{XYR_XR_Y}$. It holds that

$$\begin{aligned}
\mathfrak{h}\left(\rho_2^{RXA_2C_2}, \mathcal{R}_2^{XA_2 \to XA_2C_2}(\rho_2^{RXA_2})\right) &= \mathfrak{h}\left(\rho_2^{RXA_2C_2}, \mathcal{R}_2^{XA_1 \to XA_2C_2}(\rho_1^{RXA_1})\right) \\
&\leq \sqrt{\varepsilon_2} ~,
\end{aligned}$$

in which we used that $\rho_2^{RXA_2} = \rho_1^{RXA_1}$ since the registers YC_2B_2 on which U_2 acts have been traced out, and $A_2 = A_1$. Since it also holds that $\mathcal{R}_2(\rho_1^{RXA_1}) = \mathrm{Tr}_{YT_BC_1F_2}(U_{\mathcal{R}_2}U_1V_0 |\rho_\nu\rangle) = \sigma_2^{RXA_2C_2}$, the result follows.

For the induction step, we note that for even $i > 2$, $V_i = U_{\mathcal{R}_i} U_{i-1} V_{i-2}$, $E_i = F_i \otimes C_{i-1} \otimes E_{i-2}$, and $|\sigma_i\rangle = U_{\mathcal{R}_i} U_{i-1} |\sigma_{i-2}\rangle$. The result follows from the chain of inequalities below:

$$\begin{aligned}
\mathfrak{h}\left(\rho_i^{RXA_iC_i}, \sigma_i^{RXA_iC_i}\right) &\leq \mathfrak{h}\left(\rho_i^{RXA_iC_i}, \mathcal{R}_i^{XA_i \to XA_iC_i}(\rho_i^{RXA_i})\right) \\
&\quad + \mathfrak{h}\left(\mathcal{R}_i^{XA_i \to XA_iC_i}(\rho_i^{RXA_i}), \sigma_i^{RXA_iC_i}\right) \\
&\leq \sqrt{\varepsilon_i} + \mathfrak{h}\left(\rho_i^{RXA_i}, \mathrm{Tr}_{C_{i-1}YE_{i-2}}(U_{i-1} |\sigma_{i-2}\rangle)\right) \\
&\leq \sqrt{\varepsilon_i} + \mathfrak{h}\left(\rho_{i-2}^{RXA_{i-2}C_{i-2}}, \sigma_{i-2}^{RXA_{i-2}C_{i-2}}\right) \\
&\leq \sqrt{\varepsilon_i} + \sum_{p \leq i-2, ~ p \text{ even}} \sqrt{\varepsilon_p} ~.
\end{aligned}$$

The first step is an application of the triangle inequality, and the second follows by the definition of $\mathcal{R}_i$ and monotonicity of h under the CPTP map $\mathcal{R}_i = \mathrm{Tr}_{F_i} \circ U_{\mathcal{R}_i}$. The third inequality holds because $\rho_i^{RXA_i} = \rho_{i-1}^{RXA_{i-1}} = \mathrm{Tr}_{C_{i-1}YB_{i-2}}(U_{i-1} |\rho_{i-2}\rangle)$, the isometry U_{i-1} does not act on registers E_{i-2} or YB_{i-2}, and by the monotonicity of h under the map $\mathrm{Tr}_{C_{i-1}} \circ U_{i-1}$. The last inequality holds by the induction hypothesis. ∎

4.2 Quantum Cut-and-Paste Lemma

The direct quantum analogue to the Cut-and-Paste Lemma [BJKS04] from classical communication complexity does not hold. We can nevertheless obtain the following weaker property, linking the states in a two-party protocol corresponding to any four possible pairs of inputs in a two-by-two rectangle. The result says that if the states corresponding to two inputs x, x' to Alice and a fixed input y to Bob are close up to a

local unitary operation on Alice's side, and the states for two inputs y, y' to Bob and a fixed input x to Alice are close up to a local unitary operation on Bob's side, then, up to local unitary operations on Alice's and Bob's sides, the states for all pairs (x'', y'') of inputs in the rectangle $\{x, x'\} \times \{y, y'\}$ are close. The lemma is a variant of the hybrid argument developed in Refs. [JRS03, JN14]. A similar, albeit slightly weaker statement may be inferred from the said hybrid argument.

Lemma 7 (Quantum Cut-and-Paste) *Given any safe quantum protocol* Π *with classical inputs, consider distinct inputs* x, x' *for Alice, and* y, y' *for Bob. Let* $|\rho_0\rangle^{A_0 B_0}$ *be the shared initial state of Alice and Bob for any pair* $(x'', y'') \in \{x, x'\} \times \{y, y'\}$ *of inputs. (The state* ρ_0 *may depend on the set* $\{x, x'\} \times \{y, y'\}$.*) Let* $\left|\rho_{i,x''y''}\right\rangle^{A_i B_i C_i}$ *be the state on registers* $A_i B_i C_i$ *after the ith message is sent, when the input is* (x'', y''). *For odd* i, *let*

$$h_i \quad := \quad \mathfrak{h}\left(\rho_{i,xy}^{B_i C_i}, \rho_{i,x'y}^{B_i C_i}\right)$$

and $V_{i,x\to x'}^{A_i}$ *denote the unitary operation acting on* A_i *given by the local transition lemma (Lemma 1) such that*

$$h_i \quad = \quad \mathfrak{h}\left(V_{i,x\to x'}^{A_i} |\rho_{i,xy}\rangle\ , \left|\rho_{i,x'y}\right\rangle\right) \quad .$$

For even i, *let*

$$h_i \quad := \quad \mathfrak{h}\left(\rho_{i,xy}^{A_i C_i}, \rho_{i,xy'}^{A_i C_i}\right)$$

and $V_{i,y\to y'}^{B_i}$ *denote the unitary operation acting on* B_i *given by the local transition lemma such that*

$$h_i \quad = \quad \mathfrak{h}\left(V_{i,y\to y'}^{B_i} |\rho_{i,xy}\rangle, \left|\rho_{i,xy'}\right\rangle\right) \quad .$$

Define $V_{0,y\to y'}^{B_0} := \mathbb{I}^{B_0}$ *and* $h_0 := 1$. *Recall that* $B_i = B_{i-1}$ *for odd* i *and* $A_i = A_{i-1}$ *for even* i. *It holds that for odd* i,

$$\mathfrak{h}\left(V_{i-1,y\to y'}^{B_i} |\rho_{i,xy}\rangle, \left|\rho_{i,xy'}\right\rangle\right) \quad = \quad h_{i-1} \ , \tag{4.1}$$

$$\mathfrak{h}\left(V_{i,x\to x'}^{A_i} V_{i-1,y\to y'}^{B_i} |\rho_{i,xy}\rangle, \left|\rho_{i,x'y'}\right\rangle\right) \quad \leq \quad h_i + h_{i-1} + 2\sum_{j=1}^{i-2} h_j \ , \tag{4.2}$$

and for even i,

$$\mathfrak{h}\left(V_{i-1,x\to x'}^{A_i} |\rho_{i,xy}\rangle, \left|\rho_{i,x'y}\right\rangle\right) \quad = \quad h_{i-1} \ , \tag{4.3}$$

$$\mathfrak{h}\left(V_{i,y\to y'}^{B_i} V_{i-1,x\to x'}^{A_i} |\rho_{i,xy}\rangle, \left|\rho_{i,x'y'}\right\rangle\right) \quad \leq \quad h_i + h_{i-1} + 2\sum_{j=1}^{i-2} h_j \ . \tag{4.4}$$

Proof. We have $\left|\rho_{0,x''y''}\right\rangle = |\rho_0\rangle$, and define C_0 to be a trivial register. For odd i, let $U_{i,x''}$ be the protocol isometry U_i conditional on the content of X being x''. Then we have that

$$U_{i,x''}^{A_{i-1}C_{i-1}\to A_i C_i} \left|\rho_{i-1,x''y''}\right\rangle^{A_{i-1} B_{i-1} C_{i-1}} \quad = \quad \left|\rho_{i,x''y''}\right\rangle^{A_i B_i C_i} \quad .$$

It follows by the isometric invariance of h and because $V_{i-1,y\to y'}$ and $U_{i,x}$ act on distinct registers that

$$\mathfrak{h}\left(V_{i-1,y\to y'}^{B_i}\left|\rho_{i,xy}\right\rangle,\left|\rho_{i,xy'}\right\rangle\right) = \mathfrak{h}\left(V_{i-1,y\to y'}^{B_{i-1}}\left|\rho_{i-1,xy}\right\rangle,\left|\rho_{i-1,xy'}\right\rangle\right)$$
$$= h_{i-1} \ .$$

Similarly, for even i,

$$U_{i,y''}^{B_{i-1}C_{i-1}\to B_iC_i}\left|\rho_{i-1,x''y''}\right\rangle^{A_{i-1}B_{i-1}C_{i-1}} = \left|\rho_{i,x''y''}\right\rangle^{A_iB_iC_i}$$

and

$$\mathfrak{h}\left(V_{i-1,x\to x'}^{A_i}\left|\rho_{i,xy}\right\rangle,\left|\rho_{i,x'y}\right\rangle\right) = h_{i-1} \ .$$

We show by induction on i that (4.2) and (4.4) hold for odd and even i's, respectively. For the base case ($i=1$), we have that

$$\left|\rho_{1,x''y''}\right\rangle^{A_1B_1C_1} := U_{x''}^{A_0\to A_1C_1}\left|\rho_0\right\rangle^{A_0B_0}$$

is independent of y''. So

$$\left|\rho_{1,xy}\right\rangle = \left|\rho_{1,xy'}\right\rangle , \qquad \text{and} \qquad \left|\rho_{1,x'y}\right\rangle = \left|\rho_{1,x'y'}\right\rangle ,$$

and the result follows by taking $V_{0,y\to y'}^{B_0} := \mathbb{I}^{B_0}$:

$$\mathfrak{h}\left(V_{1,x\to x'}^{A_1}\left|\rho_{1,xy}\right\rangle,\left|\rho_{1,x'y'}\right\rangle\right) = h_1 \ .$$

For the induction step, the case of even and odd i's are proven similarly; we focus on even i's. Assume the result holds for $i-1$, we show it also holds for i by the following chain of inequalities, which are explained below:

$$\mathfrak{h}\left(V_{i,y\to y'}^{B_i}V_{i-1,x\to x'}^{A_i}\left|\rho_{i,xy}\right\rangle,\left|\rho_{i,x'y'}\right\rangle\right) \leq \mathfrak{h}\left(V_{i,y\to y'}^{B_i}V_{i-1,x\to x'}^{A_i}\left|\rho_{i,xy}\right\rangle,V_{i-1,x\to x'}^{A_i}\left|\rho_{i,xy'}\right\rangle\right)$$
$$+ \mathfrak{h}\left(V_{i-1,x\to x'}^{A_i}\left|\rho_{i,xy'}\right\rangle,\left|\rho_{i,x'y'}\right\rangle\right)$$
$$= h_i + \mathfrak{h}\left(V_{i-1,x\to x'}^{A_{i-1}}\left|\rho_{i-1,xy'}\right\rangle,\left|\rho_{i-1,x'y'}\right\rangle\right)$$
$$\leq h_i + \mathfrak{h}\left(V_{i-1,x\to x'}^{A_{i-1}}\left|\rho_{i-1,xy'}\right\rangle,V_{i-1,x\to x'}^{A_{i-1}}V_{i-2,y\to y'}^{B_{i-1}}\left|\rho_{i-1,xy}\right\rangle\right)$$
$$+ \mathfrak{h}\left(V_{i-1,x\to x'}^{A_{i-1}}V_{i-2,y\to y'}^{B_{i-1}}\left|\rho_{i-1,xy}\right\rangle,\left|\rho_{i-1,x'y'}\right\rangle\right)$$
$$\leq h_i + h_{i-2} + h_{i-1} + h_{i-2} + 2\sum_{j=1}^{i-3} h_j \ .$$

The first step is by the triangle inequality. In the second step, we used the unitary invariance of $\mathfrak{h}$ along with the definition of h_i for the first term, and along with the property that $V_{i-1}^{A_i}$ and $U_{i,y'}^{B_{i-1}C_{i-1}\to B_iC_i}$ act on distinct registers for the second term. The next step is by the triangle inequality, and the last by Eq. (4.1) for one term, and by Eq. (4.2) and the induction hypothesis for the other term. ∎

19

4.3 Relating Alice's states to $\mathrm{QIC}_{\mathrm{B}\to A}$

We study the quantum information cost of protocols for Augmented Index on input distribution μ_0 (the uniform distribution over $f_n^{-1}(0)$), and relate it to the distance between the states on two different inputs. We first focus on the quantum information cost from Bob to Alice, arising from the messages with even i's. We show that if this cost is low, then Alice's reduced states on different inputs for Bob are close to each other. (This high level intuition is the same as that described in Ref. [JN14].)

We state and prove our results for inputs with even length n; a similar result can be shown for odd n by suitably adapting the proof.

We consider the following purification of the input registers, corresponding to a particular preparation method for the K register, and to a preparation of the X register also depending on the preparation of register K. Recall that the content k of register K is uniformly distributed in $[n]$. The following registers are each initialized to uniform superpositions over the domain indicated: R_S^1 over $\{0,1\}$ (with a coherent copy in R_S^2), register R_J^1 over indices $j \in [n/2]$ (with a coherent copy in R_J^2), register R_L^1 over $\ell \in [n/2+1,n]$ (with a quantum copy in R_L^2). Register R_K holds a coherent copy of register K, whose content k is set to the value j in R_J^1 when R_S^1 is 0, and to ℓ when R_S^1 is 1. Depending on the value ℓ of R_L^1, the following registers are initialized to uniform superpositions to prepare the X register, itself in uniform over $\{0,1\}^n$: register R_Z^1 over $z \in \{0,1\}^\ell$, and register R_W^1 over $w \in \{0,1\}^{n-\ell}$. The register X is set to $x = zw$, so together $R_Z^1 R_W^1$ hold a coherent copy of X, and a second coherent copy is held in $R_Z^2 R_W^2$. If ℓ is clear from the context, we sometimes use the notation Z and W to refer to the parts of the X register holding z and w, respectively. Depending on the value j of R_J^1, we also refer to a further decomposition $z = z'z''$ with $z' \in \{0,1\}^j$ and $z'' \in \{0,1\}^{\ell-j}$. We denote by X_{1K} the register held by Bob and containing the first $k-1$ bits of x and the verification bit b, always equal to x_k under μ_0 (X_{1K} thus contains the first k bits of x in this case); it is set to z' when R_S^1 is 0, to z when R_S^1 is 1, and register $R_{X_{1K}}$ holds a coherent copy of it.

In summary, the resulting input state $\rho_{\mu_0}^{XKX_{1K}}$ distributed according to μ_0 is purified by register R, which decomposes as

$$R \quad := \quad R_J^1 R_J^2 R_L^1 R_L^2 R_Z^1 R_Z^2 R_W^1 R_W^2 R_S^1 R_S^2 R_K R_{X_{1K}} \ .$$

Using the normalization factor $c := 1/\sqrt{(n/2)\cdot(n/2)\cdot 2^\ell \cdot 2^{n-\ell} \cdot 2}$, the purified state is:

$$|\rho_0\rangle^{RXKX_{1K}} \quad = \quad c \sum_{j,\ell,z,w} |jj\ell\ell zzww\rangle \left(|00\rangle |jz'\rangle |zw\rangle^X |jz'\rangle^{KX_{1K}} + |11\rangle |\ell z\rangle |zw\rangle^X |\ell z\rangle^{KX_{1K}} \right) \ .$$

(4.5)

Starting with the above purification and using pre-shared entanglement $|\psi\rangle^{T_A T_B}$ in the initial state, the state ρ_i after round i in the protocol is

$$|\rho_i\rangle \quad := \quad c \sum_{j,\ell,z,w} |jj\ell\ell zzww\rangle \left(|00\rangle |jz'\rangle |zw\rangle |jz'\rangle \left|\rho_i^{zw,(j,z')}\right\rangle + |11\rangle |\ell z\rangle |zw\rangle |\ell z\rangle \left|\rho_i^{zw,(\ell,z)}\right\rangle \right) \ ,$$

(4.6)

where $\left|\rho_i^{x,(k,x[1,k])}\right\rangle$ denotes the pure state in registers $A_i B_i C_i$ conditional on input $(x,(k,x[1,k]))$.

Define $R_A := R_J^1 R_L^1 R_S^1 R_K R_W^1 R_W^2$. All of R_A's sub-registers except $R_W^1 R_W^2$ are classical in $\rho_i^{R_A X A_i C_i}$, since one of their coherent copies is traced out from the global purification register R. The Z part of the X register is also classical. We can write the reduced state of ρ_i on registers $R_A X A_i C_i$ as

$$\rho_i^{R_A X A_i C_i} \quad = \quad c' \sum_{j,\ell,z} |j\ell\rangle\langle j\ell| \otimes \left(|0j\rangle\langle 0j| \otimes |z\rangle\langle z|^Z \otimes \rho_{i,\ell z j z'} + |1\ell\rangle\langle 1\ell| \otimes |z\rangle\langle z|^Z \otimes \rho_{i,\ell z \ell z} \right) \ ,$$

in which we used normalization $c' := 1/((n/2) \cdot (n/2) \cdot 2^\ell \cdot 2)$ and the shorthands

$$\rho_{i,\ell z k x[1,k]} \quad := \quad \mathrm{Tr}_{B_i}\left(\left|\rho_i^{\ell z k x[1,k]}\right\rangle\left\langle\rho_i^{\ell z k x[1,k]}\right|\right) \;, \qquad \text{where} \tag{4.7}$$

$$\left|\rho_i^{\ell z k x[1,k]}\right\rangle \quad := \quad 1/\sqrt{2^{n-\ell}}\sum_w |www\rangle^{R_W^1 R_W^2 W}\left|\rho_i^{zw,(k,x[1,k])}\right\rangle^{A_i B_i C_i} \;. \tag{4.8}$$

The indices $\ell z k x[1,k]$ have the following meaning: ℓ and z indicate that Alice's input register X is in superposition after the length ℓ prefix $z = x[1,\ell]$, and k and $x[1,k]$ tell us the index k in Bob's input, the prefix $x[1,k-1]$ of x given as input to Bob, and Bob's verification bit b (which is equal to x_k under μ_0), respectively. Using this notation along with the superposition-average encoding theorem, we show the following result.

Lemma 8 *Given any even $n \geq 2$, let J and L be random variables uniformly distributed in $[n/2]$ and $[n] \setminus [n/2]$, respectively. Conditional on some value ℓ for L, let Z be a random variable chosen uniformly at random in $\{0,1\}^\ell$. The following then holds for any M-message safe quantum protocol Π for Augmented Index f_n, for any even $i \leq M$:*

$$\mathrm{QIC}_{\mathrm{B}\to\mathrm{A}}(\Pi,\mu_0) \quad \geq \quad \frac{1}{2M}\,\mathbb{E}_{j\ell z \sim JLZ}\left[\mathfrak{h}^2\left(\rho_{i,\ell z j z'}^{R_W^1 R_W^2 W A_i C_i}, \rho_{i,\ell z \ell z}^{R_W^1 R_W^2 W A_i C_i}\right)\right] \;.$$

Proof. Considering the same purification of the input state as in (4.5), we get the following states from the superposition-average encoding theorem

$$|\sigma_i\rangle \quad := \quad c\sum_{j,\ell,z,w}|jj\ell\ell zzww\rangle\left(|00\rangle\,|jz'\rangle\,|zw\rangle\,|jz'\rangle\,|\sigma_i^{zw}\rangle^{A_i C_i E_i} + |11\rangle\,|\ell z\rangle\,|zw\rangle\,|\ell z\rangle\,|\sigma_i^{zw}\rangle^{A_i C_i E_i}\right) \;,$$

satisfying

$$\mathfrak{h}(\rho_i^{RXA_iC_i}, \sigma_i^{RXA_iC_i}) \quad \leq \quad \sum_{p\leq i,\; p \text{ even}} \sqrt{\mathrm{I}(C_p:R\,|\,XA_p)} \;.$$

The reduced state of σ_i on registers $R_\mathrm{A} X A_i C_i$ is

$$\sigma_i^{R_\mathrm{A}XA_iC_i} \quad = \quad c'\sum_{j,\ell,z}|j\ell\rangle\langle j\ell| \otimes \left(|0j\rangle\langle 0j| \otimes |z\rangle\langle z|^Z \otimes \sigma_{i,\ell z} + |1\ell\rangle\langle 1\ell| \otimes |z\rangle\langle z|^Z \otimes \sigma_{i,\ell z}\right) \;,$$

in which we use the shorthands

$$\sigma_{i,\ell z} \quad := \quad \mathrm{Tr}_{E_i}\left(\left|\sigma_i^{\ell z}\right\rangle\left\langle\sigma_i^{\ell z}\right|\right) \;, \quad \text{where}$$

$$\left|\sigma_i^{\ell z}\right\rangle \quad := \quad \frac{1}{\sqrt{2^{n-\ell}}}\sum_w |www\rangle^{R_W^1 R_W^2 W}|\sigma_i^{zw}\rangle^{A_i C_i E_i} \;.$$

The lemma then follows from the next chain of inequalities, as explained below:

$$
\begin{aligned}
\frac{i}{2} \sum_{p \leq i,\ p \text{ even}} \mathrm{I}(C_p : R \mid X A_p) \quad & \geq \quad \left(\sum_{p \leq i,\ p \text{ even}} \sqrt{\mathrm{I}(C_p : R \mid X A_p)} \right)^2 \\
& \geq \quad \mathfrak{h}^2 \left(\rho_i^{R_{\mathrm{A}} Z W A_i C_i}, \sigma_i^{R_{\mathrm{A}} Z W A_i C_i} \right) \\
& = \quad \frac{1}{2} \, \mathbb{E}_{j\ell z \sim JLZ} \left[\mathfrak{h}^2 \left(\rho_{i,\ell z j z'}^{R_W^1 R_W^2 W A_i C_i}, \sigma_{i,\ell z}^{R_W^1 R_W^2 W A_i C_i} \right) \right] \\
& \quad + \frac{1}{2} \, \mathbb{E}_{j\ell z \sim JLZ} \left[\mathfrak{h}^2 \left(\rho_{i,\ell z \ell z}^{R_W^1 R_W^2 W A_i C_i}, \sigma_{i,\ell z}^{R_W^1 R_W^2 W A_i C_i} \right) \right] \\
& \geq \quad \frac{1}{4} \, \mathbb{E}_{j\ell z \sim JLZ} \left[\mathfrak{h}^2 \left(\rho_{i,\ell z j z'}^{R_W^1 R_W^2 W A_i C_i}, \rho_{i,\ell z \ell z}^{R_W^1 R_W^2 W A_i C_i} \right) \right] \quad .
\end{aligned}
$$

The first inequality is by the concavity of the square root function and the Jensen inequality, and the second by the superposition-average encoding theorem along with the monotonicity of $\mathfrak{h}$ under tracing part of R. The equality is by the joint-linearity of $\mathfrak{h}^2$, by expanding the expectation over R_S^1 and by fixing k accordingly. The last inequality is by the weak triangle inequality of $\mathfrak{h}^2$. ∎

4.4   Relating Bob's states to $\mathrm{QIC}_{\mathrm{A} \to \mathrm{B}}$

We continue with the notation from the previous section, and now focus on the quantum information cost from Alice to Bob, arising from messages with odd i's. We go via an alternative notion of information cost used by Jain and Nayak [JN14], and studied further by Laurière and Touchette [LT16]. This notion is a direct generalization of the internal information cost of classical protocols (see, e.g., Refs. [BJKS04, BBCR13]), and is called the Holevo information cost in Ref. [LT16].

Definition 2 *Given a safe quantum protocol Π with classical inputs, and distribution ν over inputs, the* Holevo information cost *(of the messages) from Alice to Bob in round i is defined as*

$$
\widetilde{\mathrm{QIC}}_{\mathrm{A} \to \mathrm{B}}^i(\Pi, \nu) \quad = \quad \mathrm{I}(X : B_i C_i \mid Y) \ ,
$$

and the cumulative Holevo information cost *from Alice to Bob is defined as*

$$
\widetilde{\mathrm{QIC}}_{\mathrm{A} \to \mathrm{B}}(\Pi, \nu) \quad = \quad \sum_{i \text{ odd}} \widetilde{\mathrm{QIC}}_{\mathrm{A} \to \mathrm{B}}^i(\Pi, \nu) \ . \tag{4.9}
$$

Given a bit string z of length at least $\ell \geq 1$, let $z^{(\ell)}$ denote the string in which z_ℓ has been flipped. The following result can be inferred from the proof of Lemma 4.9 in Ref. [JN14].

Lemma 9 *Given any even $n \geq 2$, let J and L be random variables uniformly distributed in $[n/2]$ and $[n] \setminus [n/2]$, respectively. Conditional on some value ℓ for L, let Z be a random variable chosen uniformly at random in $\{0,1\}^\ell$. The following holds for any M-message safe quantum protocol Π for the Augmented Index function f_n, for any odd $i \leq M$:*

$$
\frac{1}{n} \, \widetilde{\mathrm{QIC}}_{\mathrm{A} \to \mathrm{B}}^i(\Pi, \mu_0) \quad \geq \quad \frac{1}{16} \, \mathbb{E}_{j\ell z \sim JLZ} \left[\mathfrak{h}^2 \left(\rho_{i,\ell z j z'}^{B_i C_i} \,,\ \rho_{i,\ell z^{(\ell)} j z'}^{B_i C_i} \right) \right] \ ,
$$

with $\rho_{i,\ell z j z'}$ defined by Eqs. (4.7) and (4.8).

22

For completeness, we provide a proof of this lemma in Appendix A using our notation.

Laurière and Touchette [LT16] prove that Holevo information cost is a lower bound on quantum information cost QIC.

Lemma 10 *Given any M-message quantum protocol Π and any input distribution ν, the following holds for any odd $i \leq M$:*

$$\widetilde{\mathrm{QIC}}^i_{\mathrm{A}\to\mathrm{B}}(\Pi,\nu) \quad \leq \quad \mathrm{QIC}_{\mathrm{A}\to\mathrm{B}}(\Pi,\nu) \ .$$

This may be derived from the Information Flow Lemma (Lemma 4) by initializing the purification register R so that R_a^{B} is be a coherent copy of X and R_b^{B} is a coherent copy of Y, and R_c^{B} is a coherent copy of both X, Y.

4.5   Lower bound on QIC

We are now ready to prove a slightly weaker variant of our main lower bound on the quantum information cost of Augmented Index, i.e., Theorem 5.

Theorem 4 *Given any even n, the following holds for any M-message safe quantum protocol Π computing the Augmented Index function f_n with error at most ε on any input:*

$$\frac{1}{4}(1 - 2\varepsilon) \quad \leq \quad \left(\frac{2(M+1)^2}{n} \cdot \mathrm{QIC}_{\mathrm{A}\to\mathrm{B}}(\Pi, \mu_0) \right)^{1/2} + \left(\frac{M^3}{4} \cdot \mathrm{QIC}_{\mathrm{B}\to\mathrm{A}}(\Pi, \mu_0) \right)^{1/2} \ . \tag{4.10}$$

The stronger version is proven similarly in Section 5 using a strengthening of Lemma 8. Our argument follows ideas similar to those in Ref. [JN14]. Using the notation from the two previous sections, we start by fixing values of j, ℓ, z in their respective domains, and defining $\hat{A}_i = R_W^1 R_W^2 W A_i$. Define, for odd i,

$$
\begin{aligned}
h_i(j,\ell,z) \quad &:= \quad \mathfrak{h}\left(\rho_{i,\ell z j z'}^{B_i C_i} , \ \rho_{i,\ell z^{(\ell)} j z'}^{B_i C_i} \right) \\
&= \quad \mathfrak{h}\left(V_{i,z\to z^{(\ell)}}^{\hat{A}_i} \left| \rho_i^{\ell z j z'} \right\rangle^{\hat{A}_i B_i C_i} , \ \left| \rho_i^{\ell z^{(\ell)} j z'} \right\rangle^{\hat{A}_i B_i C_i} \right) \ ,
\end{aligned}
$$

and for even i,

$$
\begin{aligned}
h_i(j,\ell,z) \quad &:= \quad \mathfrak{h}\left(\rho_{i,\ell z j z'}^{\hat{A}_i C_i}, \rho_{i,\ell z \ell z}^{\hat{A}_i C_i} \right) \\
&= \quad \mathfrak{h}\left(V_{i,(j,z')\to(\ell,z)}^{B_i} \left| \rho_i^{\ell z j z'} \right\rangle^{\hat{A}_i B_i C_i} , \ \left| \rho_i^{\ell z \ell z} \right\rangle^{\hat{A}_i B_i C_i} \right) \ ,
\end{aligned}
$$

where the unitary operations $V_{i,z\to z^{(\ell)}}^{\hat{A}_i}$ and $V_{i,(j,z')\to(\ell,z)}^{B_i}$ are given by the Local Transition Lemma. We define the following states, analogous to the states consistent with μ_0 in Eqs. (4.7) and (4.8):

$$
\begin{aligned}
\rho_{i,\ell z^{(\ell)} \ell z} \quad &:= \quad \mathrm{Tr}_{B_i}\left(\left| \rho_i^{\ell z^{(\ell)} \ell z} \right\rangle\left\langle \rho_i^{\ell z^{(\ell)} \ell z} \right| \right) \ , \\
\left| \rho_i^{\ell z^{(\ell)} \ell z} \right\rangle \quad &:= \quad \frac{1}{\sqrt{2^{n-\ell}}} \sum_w |www\rangle^{R_W^1 R_W^2 W} \left| \rho_i^{z^{(\ell)} w, (\ell,z)} \right\rangle^{A_i B_i C_i} \ .
\end{aligned}
$$

Given protocol Π, we define a protocol $\Pi(j,\ell,z)$ that behaves as Π but starts with preshared entanglement $|\psi\rangle^{T_\mathrm{A} T_\mathrm{B}} \otimes |\psi_W\rangle$, with $|\psi_W\rangle := \sqrt{1/2^{n-\ell}} \sum_w |www\rangle^{R_W^1 R_W^2 W}$ given to Alice. We consider runs of

$\Pi(j, \ell, z)$ on four pairs of inputs: Alice gets inputs $u = z$ or $u' = z^{(\ell)}$, and Bob gets inputs $y = (j, z')$ or $y' = (\ell, z)$. On these inputs u, u' of length ℓ for Alice, $\Pi(j, \ell, z)$ uses the content w of register W to complete an input of length n for Alice in order to run Π. Note that regardless of w, the only input pair for $\Pi(j, \ell, z)$ for which Augmented Index evaluates to 1 is $(u', y') = (z^{(\ell)}, (\ell, z))$.

If M is even, denote by $\rho^{A_M C_M}_{M,\ell z^{(\ell)} wkx[1,k]}$ the reduced state of $\rho^{W A_M C_M}_{M,\ell z^{(\ell)} kx[1,k]}$ for a particular content w of W. The function f_n has different values on inputs $(z^{(\ell)} w, (j, z'))$ and $(z^{(\ell)} w, (\ell, z))$. Since the protocol Π has error at most ε on any input, we can distinguish between these two values with probability at least $1 - \varepsilon$ for any w, by applying $U_{M+1, z^{(\ell)} w}$ to the corresponding states $\rho^{A_M C_M}_{M,\ell z^{(\ell)} wjz'}$ and $\rho^{A_M C_M}_{M,\ell z^{(\ell)} wlz}$. By relationship of trace distance with distinguishability of states, and its monotonicity under quantum operations, we get that

$$
\left\| \rho^{W A_M C_M}_{M,\ell z^{(\ell)} jz'} - \rho^{W A_M C_M}_{M,\ell z^{(\ell)} \ell z} \right\|_1 = \frac{1}{2^{n-\ell}} \sum_w \left\| \rho^{A_M C_M}_{M,\ell z^{(\ell)} wjz'} - \rho^{A_M C_M}_{M,\ell z^{(\ell)} w\ell z} \right\|_1
$$

$$
\geq 2 - 4\varepsilon .
$$

Here we also used the joint linearity of the trace distance to expand over the values W takes. We now link the $h_i(j, \ell, z)$'s to the above inequality:

$$
\frac{1}{\sqrt{2}}(1 - 2\varepsilon)
$$

$$
\leq \frac{1}{2\sqrt{2}} \left\| \rho^{W A_M C_M}_{M,\ell z^{(\ell)} jz'} - \rho^{W A_M C_M}_{M,\ell z^{(\ell)} \ell z} \right\|_1
$$

$$
\leq \mathfrak{h}\left(\rho^{W A_M C_M}_{M,\ell z^{(\ell)} jz'} , \rho^{W A_M C_M}_{M,\ell z^{(\ell)} \ell z} \right)
$$

$$
\leq \mathfrak{h}\left(V^{B_M}_{M,(j,z')\to(\ell,z)} \left| \rho_{M,\ell z^{(\ell)} jz'} \right\rangle^{\hat{A}_M B_M C_M} , \left| \rho_{M,\ell z^{(\ell)} \ell z} \right\rangle^{\hat{A}_M B_M C_M} \right)
$$

$$
\leq \mathfrak{h}\left(V^{B_M}_{M,(j,z')\to(\ell,z)} \left| \rho_{M,\ell z^{(\ell)} jz'} \right\rangle^{\hat{A}_M B_M C_M} , V^{B_M}_{M,(j,z')\to(\ell,z)} V^{\hat{A}_M}_{M-1, z\to z^{(\ell)}} \left| \rho_{M,\ell zjz'} \right\rangle^{\hat{A}_M B_M C_M} \right)
$$

$$
+ \mathfrak{h}\left(V^{B_M}_{M,(j,z')\to(\ell,z)} V^{\hat{A}_M}_{M-1, z\to z^{(\ell)}} \left| \rho_{M,\ell zjz'} \right\rangle^{\hat{A}_M B_M C_M} , \left| \rho_{M,\ell z^{(\ell)} \ell z} \right\rangle^{\hat{A}_M B_M C_M} \right)
$$

$$
\leq h_{M-1}(j, \ell, z) + h_M(j, \ell, z) + h_{M-1}(j, \ell, z) + 2 \sum_{i=1}^{M-2} h_i(j, \ell, z)
$$

$$
\leq 2 \sum_{i=1}^{M} h_i(j, \ell, z) .
$$

The second inequality follows from Eq. (2.16), and the third from monotonicity of $\mathfrak{h}$ under partial trace. The fourth inequality follows by the triangle inequality, and the fifth by the quantum cut-and-paste lemma using $\hat{A}_i = R^1_W R^2_W W A_i$ as Alice's local register in round i.

In order to relate this to quantum information cost, we use Lemma 8 together with the concavity of the square root function and Jensen's inequality to obtain, for any even i,

$$
\sqrt{2M \cdot \text{QIC}_{\text{B}\to\text{A}}(\Pi, \mu_0)} \geq \mathbb{E}_{j\ell z \sim JLZ}[h_i(j, \ell, z)] . \tag{4.11}
$$

Similarly, using Lemma 9 for any odd i,

$$
\sqrt{\frac{16}{n} \cdot \widetilde{\text{QIC}}^i_{\text{A}\to\text{B}}(\Pi, \mu_0)} \geq \mathbb{E}_{j\ell z \sim JLZ}[h_i(j, \ell, z)] .
$$

Combining the above and Lemma 10, we get

$$
\begin{align}
\frac{1}{4}(1 - 2\varepsilon) \quad &\leq \quad \sum_{i \text{ odd}} \left(\frac{8}{n} \cdot \widetilde{\text{QIC}}^i_{\text{A}\to\text{B}}(\Pi, \mu_0) \right)^{1/2} + \sum_{i \text{ even}} (M \cdot \text{QIC}_{\text{B}\to\text{A}}(\Pi, \mu_0))^{1/2} \tag{4.12} \\
&\leq \quad \left(\frac{4(M+1)}{n} \cdot \sum_{i \text{ odd}} \widetilde{\text{QIC}}^i_{\text{A}\to\text{B}}(\Pi, \mu_0) \right)^{1/2} + \left(\frac{M^3}{4} \cdot \text{QIC}_{\text{B}\to\text{A}}(\Pi, \mu_0) \right)^{1/2} \tag{4.13} \\
&\leq \quad \left(\frac{2(M+1)^2}{n} \cdot \text{QIC}_{\text{A}\to\text{B}}(\Pi, \mu_0) \right)^{1/2} + \left(\frac{M^3}{4} \cdot \text{QIC}_{\text{B}\to\text{A}}(\Pi, \mu_0) \right)^{1/2} , \tag{4.14}
\end{align}
$$

which completes the proof in the case that M is even.

The proof for odd M is similar, and follows by comparing states $\rho^{B_M C_M}_{M, \ell z \ell z}$ and $\rho^{B_M C_M}_{M, \ell z^{(\ell)} \ell z}$. The different outputs can then be generated by applying $U_{M+1, (\ell, z)}$ to these states.

5   A Stronger QIC Trade-off for Augmented Index

We consider a different notion of quantum information cost, more specialized to the Augmented Index function, for which we obtain better dependence on M for the information lower bound, from M^3 to M. We also show that this notion is at least $1/M$ times $\text{QIC}_{\text{B}\to\text{A}}$, and thus we get an overall improvement by a factor of M for the M-pass streaming lower bound. The following is a precise statement of Theorem 2.

Theorem 5 *Given any even n, the following holds for any M-message quantum protocol Π computing the Augmented Index function f_n with error ε on any input:*

$$
\frac{1}{4}(1 - 2\varepsilon) \quad \leq \quad \left(\frac{2(M+1)^2}{n} \cdot \text{QIC}_{\text{A}\to\text{B}}(\Pi, \mu_0) \right)^{1/2} + \left(\frac{M^2}{2} \cdot \text{QIC}_{\text{B}\to\text{A}}(\Pi, \mu_0) \right)^{1/2} . \tag{5.1}
$$

Our lower bound on quantum streaming algorithms for $\text{DYCK}(2)$, Theorem 1, follows by combining this with Lemmas 5 and 6, and taking $m = n$ so that $N \in \Theta(n^2)$.

We consider the same purification of the input registers as in Section 4.3, and the following alternative notion of quantum information cost.

Definition 3 *Given a safe quantum protocol Π for Augmented Index, the* superposed-Holevo information cost *(of the messages) from Bob to Alice in round i is defined as*

$$
\widetilde{\text{QIC}}^i_{\text{B}\to\text{A}}(\Pi, \mu_0) \quad := \quad I(R_K R^1_J R^1_S : R^1_W R^2_W W A_i C_i \mid R^1_L Z)_{\rho_i} ,
$$

with ρ_i as defined in Eq. (4.6), and the cumulative superposed-Holevo information cost *(of the messages) from Bob to Alice is defined as*

$$
\widetilde{\text{QIC}}_{\text{B}\to\text{A}}(\Pi, \mu_0) \quad := \quad \sum_{i \text{ even}} \widetilde{\text{QIC}}^i_{\text{B}\to\text{A}}(\Pi, \mu_0) . \tag{5.2}
$$

We first show the following.

Lemma 11 *Given any even $n \geq 2$, let J and L be random variables uniformly distributed in $[n/2]$ and $[n] \setminus [n/2]$, respectively. Conditional on some value ℓ for L, let Z be a random variable chosen uniformly at random from $\{0,1\}^\ell$. The following then holds for any M-message safe quantum protocol Π for the Augmented Index function f_n, for even $i \leq M$:*

$$\widetilde{\mathrm{QIC}}^i_{\mathrm{B}\to\mathrm{A}}(\Pi, \mu_0) \quad \geq \quad \frac{1}{4}\, \mathbb{E}_{j\ell z \sim JLZ}\left[\mathfrak{h}^2\left(\rho_{i,\ell z j z'}^{R^1_W R^2_W W A_i C_i}, \rho_{i,\ell z \ell z}^{R^1_W R^2_W W A_i C_i}\right)\right] \quad,$$

with $\rho_{i,\ell z k x[1,k]}$ defined by Eqs. (4.7) and (4.8).

Proof. The Average Encoding Theorem along with monotonicity of conditional mutual information gives us the desired bound, with $\rho_{i,\ell z}$ the state $\rho_{i,\ell z k x[1,k]}$ in registers $R^1_W R^2_W W A_i C_i$ averaged over registers $R_K R^1_J R^1_S$:

$$\mathrm{I}(R_K R^1_J R^1_S : R^1_W R^2_W W A_i C_i \mid R^1_L Z)$$
$$\geq \quad \frac{1}{2}\, \mathbb{E}_{j\ell z \sim JLZ}\left[\mathfrak{h}^2\left(\rho_{i,\ell z j z'}^{R^1_W R^2_W W A_i C_i}, \rho_{i,\ell z}^{R^1_W R^2_W W A_i C_i}\right)\right]$$
$$+ \frac{1}{2}\, \mathbb{E}_{j\ell z \sim JLZ}\left[\mathfrak{h}^2\left(\rho_{i,\ell z \ell z}^{R^1_W R^2_W W A_i C_i}, \rho_{i,\ell z}^{R^1_W R^2_W W A_i C_i}\right)\right]$$
$$\geq \quad \frac{1}{4}\, \mathbb{E}_{j\ell z \sim JLZ}\left[\mathfrak{h}^2\left(\rho_{i,\ell z j z'}^{R^1_W R^2_W W A_i C_i}, \rho_{i,\ell z \ell z}^{R^1_W R^2_W W A_i C_i}\right)\right] \quad.$$

∎

We now show that this notion of information cost is a lower bound on $\mathrm{QIC}_{\mathrm{B}\to\mathrm{A}}(\Pi, \mu_0)$:

Lemma 12 *Given any M-message safe quantum protocol Π for Augmented Index and any even $i \leq M$, the following holds:*

$$\widetilde{\mathrm{QIC}}^i_{\mathrm{B}\to\mathrm{A}}(\Pi, \mu_0) \quad \leq \quad \mathrm{QIC}_{\mathrm{B}\to\mathrm{A}}(\Pi, \mu_0) \quad.$$

Proof. The lemma is implied by the following chain of inequalities, which are explained below:

$$\mathrm{I}(R_K R^1_J R^1_S : R^1_W R^2_W W A_i C_i \mid R^1_L Z)_{\rho_i}$$
$$= \quad \mathrm{I}(R_K R^1_J R^1_S : R^1_W R^2_W \mid R^1_L Z)_{\rho_i} + \mathrm{I}(R_K R^1_J R^1_S : W A_i C_i \mid R^1_L Z R^1_W R^2_W)_{\rho_i}$$
$$\leq \quad \mathrm{I}(R_K R^1_J R^1_S : Z W A_i C_i \mid R^1_L R^1_W R^2_W)_{\rho_i}$$
$$= \sum_{p \leq i,\ p \text{ even}} \mathrm{I}(R_K R^1_J R^1_S : C_p \mid Z W A_p R^1_L R^1_W R^2_W)_{\rho_p}$$
$$- \sum_{p \leq i,\ p \text{ odd}} \mathrm{I}(R_K R^1_J R^1_S : C_p \mid Z W A_p R^1_L R^1_W R^2_W)_{\rho_p} + \mathrm{I}(R_K R^1_J R^1_S : Z W \mid R^1_L R^1_W R^2_W)_{\rho_0}$$
$$\leq \sum_{p \leq i,\ p \text{ even}} \mathrm{I}(R_K R^1_J R^1_S R^1_L R^1_W R^2_W : C_p \mid Z W A_p)_{\rho_p} + \mathrm{I}(R_K R^1_J R^1_S : Z W R^1_W R^2_W \mid R^1_L)_{\rho_0}$$
$$= \sum_{p \leq i,\ p \text{ even}} \mathrm{I}(R_K R^1_J R^1_S R^1_L R^1_W R^2_W : C_p \mid Z W A_p)_{\rho_p}$$
$$+ \mathrm{I}(R_K R^1_J R^1_S : Z \mid R^1_L)_{\rho_0} + \mathrm{I}(R_K R^1_J R^1_S : W R^1_W R^2_W \mid Z R^1_L)_{\rho_0}$$
$$= \sum_{p \leq i,\ p \text{ even}} \mathrm{I}(R_K R^1_J R^1_S R^1_L R^1_W R^2_W : C_p \mid Z W A_p)_{\rho_p} \quad.$$

The first equality holds by the chain rule. The first inequality holds because the first term evaluates to zero, and because the second term is dominated by the subsequent expression (as may be seen by applying the chain rule). The second equality is from the information flow lemma, the second inequality follows from the chain rule and the non-negativity of the conditional mutual information, and the third equality is by the chain rule. The last equality follows because $R_K R_J^1 R_S^1$ is independent of Z and because the registers $R_W^1 R_W^1 W$ of ρ_0 are in a pure state.

The last term is seen to be upper bounded by $\mathrm{QIC}_{\mathrm{B}\to\mathrm{A}}(\Pi, \mu_0)$ by applying the data processing inequality to the R register. ∎

The improved lower bound on QIC follows along the same lines as in Section 4.5, but we use Lemma 11 instead of Lemma 8 for even i's in Eq. (4.11). Then Eqs. (4.12) to (4.14) become

$$
\begin{aligned}
\frac{1}{4}(1 - 2\varepsilon) \quad &\leq \quad \sum_{i \text{ odd}} \left(\frac{8}{n} \cdot \widetilde{\mathrm{QIC}}_{\mathrm{A}\to\mathrm{B}}^i (\Pi, \mu_0) \right)^{1/2} + \sum_{i \text{ even}} \left(2 \cdot \widetilde{\mathrm{QIC}}_{\mathrm{B}\to\mathrm{A}}^i (\Pi, \mu_0) \right)^{1/2} \\
&\leq \quad \left(\frac{4(M+1)}{n} \cdot \sum_{i \text{ odd}} \widetilde{\mathrm{QIC}}_{\mathrm{A}\to\mathrm{B}}^i (\Pi, \mu_0) \right)^{1/2} + \left(M \cdot \sum_{i \text{ even}} \widetilde{\mathrm{QIC}}_{\mathrm{B}\to\mathrm{A}}^i (\Pi, \mu_0) \right)^{1/2} \\
&\leq \quad \left(\frac{2(M+1)^2}{n} \cdot \mathrm{QIC}_{\mathrm{A}\to\mathrm{B}}(\Pi, \mu_0) \right)^{1/2} + \left(\frac{M^2}{2} \cdot \mathrm{QIC}_{\mathrm{B}\to\mathrm{A}}(\Pi, \mu_0) \right)^{1/2} ,
\end{aligned}
$$

completing the proof of Theorem 5 for even M. The case of odd M is similar.

Acknowlegements

We are grateful to Mark Braverman, Ankit Garg, Young Kun Ko and Jieming Mao for useful discussions related to the development of the superposition-average encoding theorem and quantum cut-and-paste lemma.

A   Relating Bob's states to $\mathrm{QIC}_{\mathrm{A}\to\mathrm{B}}$

Lemma 9 can be inferred from the proof of Lemma 4.9 in Ref. [JN14]. For completeness, we provide a proof using our notation.

Lemma 13 *Given any even n, let J and L be random variables uniformly distributed in $[n/2]$ and $[n]\backslash[n/2]$, respectively. Conditional on some value ℓ for L, let Z be a random variable chosen uniformly at random in $\{0,1\}^\ell$. The following then holds for any M-message safe quantum protocol Π for the Augmented Index function f_n, for any odd $i \leq M$:*

$$
\frac{1}{n} \widetilde{\mathrm{QIC}}_{\mathrm{A}\to\mathrm{B}}^i (\Pi, \mu_0) \quad \geq \quad \frac{1}{16} \, \mathbb{E}_{j\ell z \sim JLZ} \left[\mathfrak{h}^2 \left(\rho_{i,\ell z j z'}^{B_i C_i} , \ \rho_{i,\ell z^{(\ell)} j z'}^{B_i C_i} \right) \right] ,
$$

with $\rho_{i,\ell z j z'}$ defined by Eqs. (4.7) and (4.8).

Proof. We start with the following chain of inequalities:

$$
\widetilde{\mathrm{QIC}}^{\,i}_{\mathrm{A}\to\mathrm{B}}(\Pi,\mu_0)
$$

$$
= \quad \mathrm{I}(X:B_iC_i\,|\,KX[1,K])
$$

$$
\geq \quad \frac{1}{2}\,\mathrm{I}(X:B_iC_i\,|\,JX[1,J])
$$

$$
= \quad \frac{1}{2}\cdot\frac{2}{n}\sum_{j\leq n/2}\frac{1}{2^j}\sum_{z'}\mathrm{I}(X[j+1,n]:B_iC_i\,|\,J=j,X[1,j]=z')
$$

$$
\geq \quad \frac{1}{n}\sum_{j\leq n/2}\frac{1}{2^j}\sum_{z'}\mathrm{I}(X[n/2+1,n]:B_iC_i\,|\,X[j+1,n/2],J=j,X[1,j]=z')
$$

$$
= \quad \frac{1}{n}\sum_{j\leq n/2,\ell>n/2}\frac{1}{2^j}\sum_{z'}\mathrm{I}(X_\ell:B_iC_i\,|\,X[j+1,\ell-1],J=j,X[1,j]=z')
$$

$$
= \quad \frac{1}{n}\sum_{j\leq n/2,\ell>n/2}\frac{1}{2^{\ell-1}}\sum_{z[1,\ell-1]}\mathrm{I}(X_\ell:B_iC_i\,|\,J=j,X[1,\ell-1]=z[1,\ell-1])\ . \tag{A.1}
$$

The first equality holds by definition, the first inequality holds because we can generate the classical random variable K by setting it equal to J with probability one half (and then equal to L also with probability one half), the second equality follows by expanding over J and $X[1,J]$, the second inequality follows by the chain rule and non-negativity of mutual information, the third equality holds by the chain rule, and the last equality follows by expanding over $X[j+1,\ell-1]$.

We also get the following bound by the Average Encoding Theorem (Lemma 2) and the weak triangle inequality for $\mathfrak{h}^2$, with $\rho_{i,\ell z[1,\ell-1]jz'}$ being the state $\rho_{i,\ell z[1,\ell-1]x_\ell jz'}$ in register B_iC_i averaged over X_ℓ:

$$
\mathrm{I}(X_\ell:B_iC_i\,|\,J=j,X[1,\ell-1]=z[1,\ell-1])
$$

$$
\geq \quad \frac{1}{2}\,\mathfrak{h}^2\!\left(\rho^{B_iC_i}_{i,\ell zjz'}\,,\,\rho^{B_iC_i}_{i,\ell z[1,\ell-1]jz'}\right)+\frac{1}{2}\,\mathfrak{h}^2\!\left(\rho^{B_iC_i}_{i,\ell z^{(\ell)}jz'}\,,\,\rho^{B_iC_i}_{i,\ell z[1,\ell-1]jz'}\right)
$$

$$
\geq \quad \frac{1}{4}\,\mathfrak{h}^2\!\left(\rho^{B_iC_i}_{i,\ell zjz'}\,,\,\rho^{B_iC_i}_{i,\ell z^{(\ell)}jz'}\right)\ .
$$

Taking expectation over JLZ in the above inequality and expanding, we get the desired result by comparing it with Eq. (A.1):

$$
\mathbb{E}_{j\ell z\sim JLZ}\left[\mathfrak{h}^2\!\left(\rho^{B_iC_i}_{i,\ell zjz'}\,,\,\rho^{B_iC_i}_{i,\ell z^{(\ell)}jz'}\right)\right]
$$

$$
\leq \quad 4\,\mathbb{E}_{j\ell z\sim JLZ}\,\mathrm{I}(X_\ell:B_iC_i\,|\,J=j,X[1,\ell-1]=z[1,\ell-1])
$$

$$
= \quad 4\left(\frac{2}{n}\right)^2\sum_{j\leq n/2,\ell>n/2}\frac{1}{2^{\ell-1}}\sum_{z[1,\ell-1]}\mathrm{I}(X_\ell:B_iC_i\,|\,J=j,X[1,\ell-1]=z[1,\ell-1])
$$

$$
\leq \quad \frac{16}{n}\,\widetilde{\mathrm{QIC}}^{\,i}_{\mathrm{A}\to\mathrm{B}}(\Pi,\mu_0)\ .
$$

∎

B   Information Flow Lemma

We use the following bound on the transfer of information in interactive quantum protocols, obtained in Ref. [LT16]. We provide a proof for completeness.

Lemma 14 *Given a protocol* Π, *an input state* ρ *with purifying register* R *with arbitrary decompositions* $R = R_a^{\mathrm{A}} R_b^{\mathrm{A}} R_c^{\mathrm{A}} = R_a^{\mathrm{B}} R_b^{\mathrm{B}} R_c^{\mathrm{B}}$, *the following hold:*

$$\sum_{i\geq 0} \mathrm{I}(R_a^{\mathrm{B}} : C_{2i+1} \mid R_b^{\mathrm{B}} B_{2i+1}) - \sum_{i\geq 1} \mathrm{I}(R_a^{\mathrm{B}} : C_{2i} \mid R_b^{\mathrm{B}} B_{2i})$$
$$= \mathrm{I}(R_a^{\mathrm{B}} : B_{\mathrm{out}} B' \mid R_b^{\mathrm{B}}) - \mathrm{I}(R_a^{\mathrm{B}} : B_{\mathrm{in}} \mid R_b^{\mathrm{B}}) \ ,$$

$$\sum_{i\geq 0} \mathrm{I}(R_a^{\mathrm{A}} : C_{2i+2} \mid R_b^{\mathrm{A}} A_{2i+2}) - \sum_{i\geq 0} \mathrm{I}(R_a^{\mathrm{A}} : C_{2i+1} \mid R_b^{\mathrm{A}} A_{2i+1})$$
$$= \mathrm{I}(R_a^{\mathrm{A}} : A_{\mathrm{out}} A' \mid R_b^{\mathrm{A}}) - \mathrm{I}(R_a^{\mathrm{A}} : A_{\mathrm{in}} \mid R_b^{\mathrm{A}}) \ .$$

Proof. We focus on the first identity, that for the messages received by Bob; the identity for the messages received by Alice follows similarly. In the rest of the proof, we omit the superscripts on the purifying registers; they are meant to be B.

We show that

$$\mathrm{I}(R_a : B_{2k+1} C_{2k+1} \mid R_b)$$
$$= \sum_{0\leq i \leq k} \mathrm{I}(R_a : C_{2i+1} \mid R_b B_{2i+1}) - \sum_{1\leq i \leq k} \mathrm{I}(R_a : C_{2i} \mid R_b B_{2i}) + \mathrm{I}(R_a : B_{\mathrm{in}} \mid R_b)$$

by induction on k, with $2k + 1 \leq M$. If M is odd, Bob receives the last message and $\mathrm{I}(R_a : B_{\mathrm{out}} B' \mid R_b) = \mathrm{I}(R_A : B_M C_M \mid R_b)$, and the result follows. If M is even and Bob sends the last message, the result follows since $B_M = B_{\mathrm{out}} B'$ and $\mathrm{I}(R_a : B_M \mid R_b) = \mathrm{I}(R_a : B_{M-1} C_{M-1} \mid R_b) - \mathrm{I}(R_a : C_M \mid R_b B_M)$ by using the chain rule and isometric invariance under the map that takes $B_{M-1} C_{M-1} \to B_M C_M$.

The base case for the induction follows from

$$\mathrm{I}(R_a : B_1 C_1 \mid R_b) = \mathrm{I}(R_a : B_1 \mid R_b) + \mathrm{I}(R_a : C_1 \mid R_b B_1)$$
$$= \mathrm{I}(R_a : B_{\mathrm{in}} \mid R_b) + \mathrm{I}(R_a : C_1 \mid R_b B_1) \ .$$

Here, the first equality holds by the chain rule. The second holds because $B_1 = B_0 = B_{\mathrm{in}} T_B$, and because the state in T_B is in tensor product with the initial state in the registers $R_a R_b B_{\mathrm{in}}$.

For the induction step, we have

$$\mathrm{I}(R_a : B_{2k+3} C_{2k+3} \mid R_b)$$
$$= \mathrm{I}(R_a : B_{2k+3} \mid R_b) + \mathrm{I}(R_a : C_{2k+2} \mid R_b B_{2k+2}) + \mathrm{I}(R_a : C_{2k+3} \mid R_b B_{2k+3})$$
$$\quad - \mathrm{I}(R_a : C_{2k+2} \mid R_b B_{2k+2})$$
$$= \mathrm{I}(R_a : B_{2k+2} C_{2k+2} \mid R_b) + \mathrm{I}(R_a : C_{2k+3} \mid R_b B_{2k+3}) - \mathrm{I}(R_a : C_{2k+2} \mid R_b B_{2k+2})$$
$$= \mathrm{I}(R_a : B_{2k+1} C_{2k+1} \mid R_b) + \mathrm{I}(R_a : C_{2k+3} \mid R_b B_{2k+3}) - \mathrm{I}(R_a : C_{2k+2} \mid R_b B_{2k+2}) \ ,$$

in which the first equality holds by the chain rule and by adding and subtracting the same term, the second also holds by the chain rule and because $B_{2k+3} = B_{2k+2}$, and the third holds by the isometric invariance under the map that takes $B_{2k+1} C_{2k+1} \to B_{2k+2} C_{2k+2}$. The induction step follows by comparing terms. ∎

References

[AF98]   Andris Ambainis and Rūsiņš Freivalds. 1-way quantum finite automata: Strengths, weaknesses and generalizations. In *Proceedings of the 39th Annual IEEE Symposium on Foundations of Computer Science*, pages 332–341, 1998.

[ANTV02]   Andris Ambainis, Ashwin Nayak, Amnon Ta-Shma, and Umesh Vazirani. Dense quantum coding and quantum finite automata. *Journal of the ACM*, 49(4):1–16, July 2002.

[BBCR13]   Boaz Barak, Mark Braverman, Xi Chen, and Anup Rao. How to compress interactive communication. *SIAM Journal on Computing*, 42(3):1327–1363, 2013.

[BJKS04]   Ziv Bar-Yossef, T. S. Jayram, Ravi Kumar, and D. Sivakumar. An information statistics approach to data stream and communication complexity. *Journal of Computer and System Sciences*, 68(4):702–732, 2004. Special issue on FOCS 2002.

[BKCG14]   Robin Blume-Kohout, Sarah Croke, and Daniel Gottesman. Streaming universal distortion-free entanglement concentration. *IEEE Transactions on Information Theory*, 60(1):334–350, Jan 2014.

[CCKM13]   Amit Chakrabarti, Graham Cormode, Ranganath Kondapally, and Andrew McGregor. Information cost tradeoffs for augmented index and streaming language recognition. *SIAM Journal on Computing*, 42(1):61–83, 2013.

[CK11]   Amit Chakrabarti and Ranganath Kondapally. Everywhere-tight information cost tradeoffs for Augmented Index. In *Proceedings of the 14th International Workshop on Approximation Algorithms for Combinatorial Optimization Problems, and the 15th International Workshop on Randomization and Computation*, APPROX'11/RANDOM'11, pages 448–459, Berlin, Heidelberg, 2011. Springer-Verlag.

[FR15]   Omar Fawzi and Renato Renner. Quantum conditional mutual information and approximate Markov chains. *Communications in Mathematical Physics*, 340(2):575–611, 2015.

[FvdG99]   Christopher A. Fuchs and Jeroen van de Graaf. Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Transactions on Information Theory*, 45(4):1216–1227, 1999.

[GKK+08]   Dmitry Gavinsky, Julia Kempe, Iordanis Kerenidis, Ran Raz, and Ronald de Wolf. Exponential separation for one-way quantum communication complexity, with applications to cryptography. *SIAM Journal on Computing*, 38(5):1695–1708, 2008.

[JN14]   Rahul Jain and Ashwin Nayak. The space complexity of recognizing well-parenthesized expressions in the streaming model: the index function revisited. *IEEE Transactions on Information Theory*, 60(10):6646–6668, October 2014.

[JRS03]   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*, pages 220–229. IEEE Computer Society Press, Los Alamitos, CA, USA, 2003.

[JRS09]   Rahul Jain, Jaikumar Radhakrishnan, and Pranab Sen. A property of quantum relative entropy with an application to privacy in quantum communication. *Journal of the ACM*, 56(6):1–32, 2009.

[KLGR16]   Iordanis Kerenidis, Mathieu Laurière, François Le Gall, and Mathys Rennela. Information cost of quantum communication protocols. *Quantum Information and Computation*, 16(3-4):181–196, 2016.

[KNTZ07]   Hartmut Klauck, Ashwin Nayak, Amnon Ta-Shma, and David Zuckerman. Interaction in quantum communication. *IEEE Transactions on Information Theory*, 53(6):1970–1982, June 2007.

[KW97]   Attila Kondacs and John Watrous. On the power of quantum finite state automata. In *Proceedings of the 38th Annual IEEE Symposium on Foundations of Computer Science*, pages 66–75, 1997.

[LG06]   François Le Gall. Exponential separation of quantum and classical online space complexity. In *Proceedings of the Eighteenth Annual ACM Symposium on Parallelism in Algorithms and Architectures*, SPAA '06, pages 67–73, New York, NY, USA, 2006. ACM.

[LR73]   Elliott H. Lieb and Mary Beth Ruskai. Proof of the strong subadditivity of quantum mechanical entropy. *Journal of Mathematical Physics*, 14(12):1938–1941, 1973.

[LT16]   Mathieu Laurière and Dave Touchette. Information flow in quantum communication: The cost of forgetting classical information. 2016. Submitted.

[MC00]   Cristopher Moore and James P. Crutchfield. Quantum automata and quantum grammars. *Theoretical Computer Science*, 237(1-2):275–306, April 2000.

[MMN14]   Frédéric Magniez, Claire Mathieu, and Ashwin Nayak. Recognizing well-parenthesized expressions in the streaming model. *SIAM Journal on Computing*, 43(6):1880–1905, December 2014.

[Mut05]   S. Muthukrishnan. *Data Streams: Algorithms and Applications*, volume 1, number 2 of *Foundations and Trends in Theoretical Computer Science*. Now Publishers Inc., Hanover, MA, USA, 2005.

[Tou14]   Dave Touchette. Quantum information complexity and amortized communication. Technical Report arXiv:1404.3733, arXiv.org Preprint, http://arxiv.org/abs/1404.3733, April 14, 2014.

[Tou15]   Dave Touchette. Quantum information complexity. In *Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing*, pages 317–326. ACM, 2015.

[Wat15]   John Watrous. *Theory of Quantum Information*. 2015. Manuscript of a book, available at https://cs.uwaterloo.ca/~watrous/.

[Wil13]   Mark M. Wilde. *Quantum Information Theory*. Cambridge University Press, New York, 2013.