UC Irvine
Recent Work

Title

Capacity of Summation over a Symmetric Quantum Erasure MAC with Partially Replicated Inputs

Permalink

https://escholarship.org/uc/item/7b6397vh

Authors

Yao, Yuhang

Jafar, Syed A

Publication Date

2024-05-16

Capacity of Summation over a Symmetric Quantum Erasure MAC with Partially Replicated Inputs

Yuhang Yao, Syed A. Jafar

Center for Pervasive Communications and Computing (CPCC)

University of California Irvine, Irvine, CA 92697

Email: {yuhangy5, syed}@uci.edu

Abstract

The optimal quantum communication cost of computing a classical sum of distributed sources is studied over a quantum erasure multiple access channel (QEMAC). K classical messages comprised of finite-field symbols are distributed across S servers, who also share quantum entanglement in advance. Each server $s \in [S]$ manipulates its quantum subsystem $\mathcal{Q}_s$ according to its own available classical messages and sends $\mathcal{Q}_s$ to the receiver who then computes the sum of the messages based on a joint quantum measurement. The download cost from Server $s \in [S]$ is the logarithm of the dimension of $\mathcal{Q}_s$. The rate R is defined as the number of instances of the sum computed at the receiver, divided by the total download cost from all the servers. The main focus is on the symmetric setting with $K = \binom{S}{\alpha}$ messages where each message is replicated among a unique subset of α servers, and the answers from any β servers may be erased. If no entanglement is initially available to the receiver, then we show that the capacity (maximal rate) is precisely $C = \max\left\{\min\left\{\frac{2(\alpha-\beta)}{S}, \frac{S-2\beta}{S}\right\}, \frac{\alpha-\beta}{S}\right\}$. The capacity with arbitrary levels of prior entanglement (Δ_0) between the S data-servers and the receiver is also characterized, by including an auxiliary server (Server 0) that has no classical data, so that the communication cost from Server 0 is a proxy for the amount of receiver-side entanglement that is available in advance. The challenge on the converse side resides in the optimal application of the weak monotonicity property, while the achievability combines ideas from classical network coding and treating qudits as classical dits, as well as new constructions based on the N-sum box abstraction that rely on absolutely maximally entangled quantum states.

1 Introduction

Described by Schrodinger in 1935 [1] as the foremost distinctive feature of quantum mechanics, entanglement – especially among *many* parties — remains one of the theory's most intriguing aspects. From a network information theoretic perspective, a key objective is to quantify multiparty entanglement in terms of its utility as a resource, by the gains in communication efficiency that are enabled by entanglement, not only for communication tasks but more generally for multiparty *computation* tasks.

Going back at least four decades to the 1979 work of Korner and Marton in [2], it is understood in classical network information theory, that the generalization from communication tasks, where
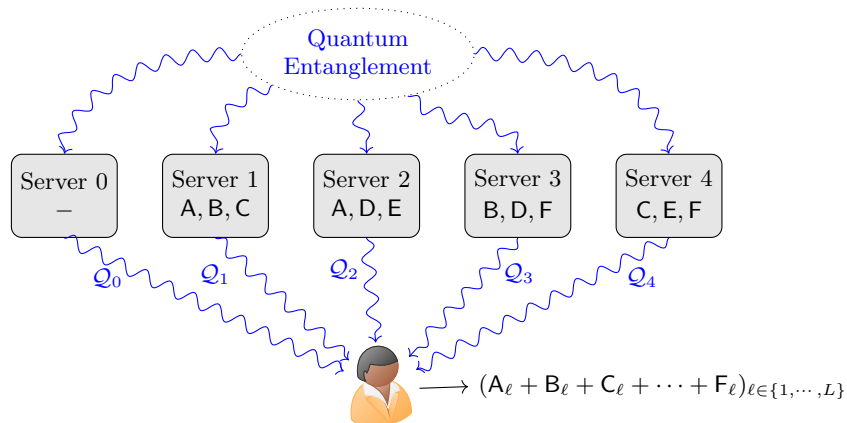

Figure 1: A Σ-QMAC example with $S = 4$ data-servers, one auxiliary server (Server 0), and $K = 6$ data streams $(\mathsf{A}, \mathsf{B}, \mathsf{C}, \cdots, \mathsf{F})$. A Σ-QEMAC setting allows some of the $\mathcal{Q}_i$ (e.g., any one of $\mathcal{Q}_1, \mathcal{Q}_2, \mathcal{Q}_3, \mathcal{Q}_4$) to be erased.

the receivers need to recover various desired input messages, to *computation* tasks, where the receivers need to recover some *functions* of the distributed input messages, is highly non-trivial. Remarkably, this is the case even when the function to be computed is simply a sum of inputs and the network is simply a multiple access channel, as in [2]. Despite the challenges, with accelerating trends towards distributed computing there has been an explosion of interest in the capacity of communication networks when used for (typically, linear) computation tasks. Examples from an abundance of literature on this topic include works on the capacity of *sum-networks* [3–5], *network function computation* [6–8] and *over-the-air computation* [9], to name a few.

By the same token, there is growing interest in the fundamental limits of classical linear computation over a *quantum* multiple access channel (QMAC), spurred by a variety of applications ranging from distributed quantum sensing and metrology [10–13] and quantum simultaneous message passing protocols [14–16] to quantum private information retrieval (QPIR) [17–22]. In particular, the Σ-QMAC model introduced in [21] is the most closely related to our work in this paper. Here we explore its generalization to a Σ-QEMAC, i.e., a Σ-QMAC that allows *erasures*.

Fig. 1 illustrates an example of a Σ-QMAC setting of [21]. In the example shown in the figure, there are $K = 6$ data streams, denoted as $\mathsf{A}, \mathsf{B}, \cdots, \mathsf{F}$, comprised of $\mathbb{F}_d$ symbols. Various subsets of these data streams are made available to a set of servers who also have *entangled* quantum resources $(\mathcal{Q}_0, \cdots, \mathcal{Q}_4)$ distributed among them in advance (independent of the data). Any classical information available to a server may be suitably encoded into its quantum system through local operations, after which the quantum systems are sent to the receiver (Alice) through ideal (noiseless) quantum channels. Note that Server 0, which has no data inputs and simply forwards its quantum subsystems to Alice, is an auxiliary server that may be included to model any prior entanglement that the data-servers share in advance with Alice. The cost of communicating each quantum subsystem $\mathcal{Q}_s$ to Alice (say, in qubits) is equal to the (base 2) logarithm of its dimension, i.e., $\log |\mathcal{Q}_s|$. Based on a joint measurement of the received quantum systems, Alice must be able to recover the sum of the classical data streams. Communication rates are measured in terms of the number of instances of the sum that are computed by Alice, per qubit of communication cost from the data-servers, for any given rate from the auxiliary server (see Section 3.2 for formal definitions). The supremum of achievable rates defines the capacity.

2

As in the classical setting, the generalization from communication to computation tasks is also non-trivial in the quantum setting. For example, while the capacity of classical communication over a quantum multiple access channel (QMAC) is known under many fairly general noisy channel models for well over a decade [23,24], the recent capacity characterization for the Σ-QMAC in [21] is limited to ideal (noise-free) channels. The aforementioned studies of QPIR and Quantum Metrology also typically choose an ideal channel model. While the classical communication capacity of an ideal (noise-free) QMAC is trivial, what makes these problems non-trivial even with ideal channels is the multiparty computation aspect — that Alice needs to recover a function of the distributed inputs, instead of the inputs themselves. Indeed, instead of noisy channels, the focus in the Σ-QMAC is on quantifying the utility of multiparty entanglement as a resource that facilitates desired linear computations, by comparing the capacity with and without entanglement. What makes the Σ-QMAC especially interesting is the interplay between classical dependencies (replication of data across servers, mixing of inputs due to the desired computation), and multiparty quantum entanglement, which creates opportunities for synergistic gains from a confluence of ideas from the classical domain such as interference alignment [25], network coding [26], and network function computation [27] on one hand, and the quantum domain such as teleportation, superdense coding [28], and the N-sum box abstraction [29] on the other. The study of the Σ-QMAC in [21] takes a perspective similar to degrees-of-freedom (DoF) analyses in wireless networks [25], where noise is de-emphasized and the focus is entirely on quantifying the distributed accessibility of signal dimensions as the key resource. Note the similarity to the resource-theoretic accounting of quantum entanglement in facilitating classical and quantum communication in a *two-party* setting, also with simplified channels, in [30,31]. The capacity of the Σ-QMAC in [21], and its generalization to include erasures as in this work, can thus be seen as attempts to provide a *resource-theoretic* accounting of *multiparty* entanglement for an elemental multiparty computation task — computing a sum of distributed inputs.

Generalizing the Σ-QMAC model to a Σ-QEMAC, where erasures are possible, leads to interesting questions. For example, consider the counterpoint that multiparty entanglement in the presence of erasures could be a double-edged sword. On one hand, the quantum systems sent by distributed servers to Alice are capable of facilitating more efficient linear computation if they are entangled than if they are unentangled. But on the other hand, because Alice in general needs to jointly measure the entangled systems, it is possible that the loss of some of the sub-systems may turn the entanglement into a *disadvantage*, i.e., it is possible that the sub-systems that are received successfully may be useless without the sub-systems that are lost, *because* of their entanglement. Recall that in the point to point setting, quantum erasure correction is in general less efficient than classical erasure correction, as evident from their respective Singleton bounds [31]. In the classical case, in order to protect K symbols against $D - 1$ erasures, it suffices to encode them into N symbols, such that $N \geq K + D - 1$. However, in the quantum case, protecting K qudits from $D - 1$ erasures requires encoding them into at least $N \geq K + 2(D - 1)$ qudits. For example, 1 classical symbol can be protected from 1 erasure by simple repetition, i.e., by sending 2 symbols, which doubles the communication cost. Protecting quantum information carried by 1 qudit against one erasure on the other hand requires at least 3 qudits, tripling the communication cost. Without entanglement, qudits can always be used as classical dits, allowing classical erasure codes that are more efficient. With entanglement, especially in network computation settings, we have the potential for superdense coding gain to improve communication efficiency, but can this advantage overcome the potential loss of efficiency due to the greater cost of quantum erasures? Such a question exemplifies the insights that we seek in this work.

Going back to the example in Fig. 1, and assuming for simplicity that no prior entanglement is available to Alice (i.e., ignoring Server 0), suppose any *one* of the 4 quantum systems ($\mathcal{Q}_1, \mathcal{Q}_2, \mathcal{Q}_3, \mathcal{Q}_4$) could be erased, e.g., lost in transit or known to be corrupted and therefore discarded by Alice. Consider first a few natural baselines for comparison. The first baseline scheme does not utilize quantum entanglement, it simply treats qudits as classical dits (TQC). The problem is reduced to a classical sum-network coding problem (cf. [3, 4]) with possible link failure as considered in [27]. Applying the result of [27], the rate achieved is $R = 1/4$. As another baseline, consider a scheme based on [21]. While the coding scheme in [21] does not allow for erasures, an erasure-tolerant scheme can be built from it as follows. In the absence of erasures, [21] shows that Alice can compute $\mathsf{B} + \mathsf{C} + \mathsf{E}$ with only the transmission from Server 1 and Server 2. Alternatively, the same can also be done with only the transmission from Server 3 and Server 4. Implementing both alternatives together produces a scheme that allows Alice to compute $\mathsf{B} + \mathsf{C} + \mathsf{E}$ even if any one of the quantum subsystems $\mathcal{Q}_1, \cdots, \mathcal{Q}_4$ is unavailable at the decoder. Similarly, Alice can compute $\mathsf{A} + \mathsf{D} + \mathsf{F}$ using only Servers 1 and 3, or by using only Servers 2 and 4. Combining both alternatives allows Alice to also compute $\mathsf{A} + \mathsf{D} + \mathsf{F}$ while tolerating the erasure of any one quantum system, i.e., by tolerating any one unresponsive server. Overall, this approach also achieves the rate $R = 1/4$. Note that while this approach combines entanglement-assisted coding schemes, the redundancy required to tolerate erasures is such that the benefits of entanglement are lost, as reflected in the fact that the rate achieved is the same as without entanglement assistance in the first baseline scheme. Fortunately, it turns out that the optimal (capacity achieving) scheme improves upon these baselines, and the benefits of entanglement do *not* vanish due to erasures. Applying the main result of this work from Theorem 1 to this particular example will show that the rate $R = 1/2$ is achievable and optimal. With this brief preview of our main result, let us now summarize the relevant background that we need for this work.

2   Preliminaries

2.1   Miscellaneous

$\mathbb{N}$ denotes the set of positive integers. For $n_1, n_2 \in \mathbb{N}$, $[n_1 : n_2]$ denotes the set $\{n_1, n_1 + 1, \cdots, n_2\}$ if $n_1 \leq n_2$ and $\emptyset$ otherwise. $[n] \triangleq [1 : n]$ for $n \in \mathbb{N}$. $\mathbb{C}$ denotes the set of complex numbers. $\mathbb{R}_+$ denotes the set of non-negative real numbers. $\mathbb{F}_q$ denotes the finite field with $q = p^r$ a power of a prime. Define compact notations $A^{[n]} \triangleq (A^{(1)}, A^{(2)}, \cdots, A^{(n)})$ and $A_{[n]} \triangleq (A_1, A_2, \cdots, A_n)$. $\mathcal{S}^{a \times b}$ denotes the set of $a \times b$ matrices with elements in $\mathcal{S}$. For an element $x \in \mathbb{F}_q = \mathbb{F}_{p^r}$, define $\mathrm{tr}(x)$ as the *field trace* of x that maps it to an element in $\mathbb{F}_p$. For a set $\mathcal{A}$, the set of its cardinality-m sub-sets is denoted as $\binom{\mathcal{A}}{m} \triangleq \{\mathcal{A} \subseteq \mathcal{A} \mid |\mathcal{A}| = m\}$. The notation $2^{\mathcal{A}}$ denotes the power set of $\mathcal{A}$. The notation $f : \mathcal{A} \mapsto \mathcal{B}$ denotes a map f from $\mathcal{A}$ to $\mathcal{B}$. $M^{\dagger}$ denotes the conjugate transpose of a matrix M, and $\mathrm{Tr}(M)$ denotes the trace of a square matrix M. $\mathcal{H}$ denotes a finite-dimensional Hilbert space. $\mathcal{D}(\mathcal{H})$ denotes the set of density operators acting on $\mathcal{H}$, i.e., the set of positive semi-definite matrices that have trace one. $\mathcal{L}(\mathcal{H})$ denotes the set of square linear operators acting on $\mathcal{H}$. $\mathsf{Pr}(E)$ denotes the probability of an event E.

2.2   Quantum information and entropy

For a classical random variable X, the support set and probability mass function are denoted as $\mathcal{X}$ and $p_X(x)$ by default. For a quantum system A, $\mathcal{H}_A$ is used to denote its underlying Hilbert space

by default, so that a pure state of A is described by a unit vector in $\mathcal{H}_A$. A general (mixed) state of A is described a density operator $\rho_A \in \mathcal{D}(\mathcal{H}_A)$. We may write $\mathcal{D}(\mathcal{H}_A)$ as $\mathcal{D}(A)$ for simplicity. A classical random variable X may be regarded as a special quantum system with density operator $\rho_X = \sum_{x \in \mathcal{X}} p_X(x) |x\rangle \langle x|_X$ where $\{|x\rangle\}_{x \in \mathcal{X}}$ is an orthonormal basis of $\mathcal{H}_X$. For quantum systems $A_1, A_2, \cdots, A_S$, the composite system is compactly written as $A_1 A_2 \cdots A_S$. The underlying Hilbert space for the composite system is $\mathcal{H}_{A_1 A_2 \cdots A_S} = \mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2} \otimes \cdots \otimes \mathcal{H}_{A_S}$.

Let $S_v(\rho) \triangleq -\mathrm{Tr}(\rho \log \rho)$ be the von-Neumann entropy of a density operator ρ. For a quantum system A in the state $\rho_A \in \mathcal{D}(A)$, define $H(A)_{\rho_A} \triangleq S_v(\rho_A)$ as the entropy of A. The subscript ρ_A in $H(A)_{\rho_A}$ may be omitted for compact notation when it is obvious from the context.

For a bipartite quantum system AB in the (joint) state $\rho_{AB} \in \mathcal{D}(AB)$, the reduced state on A is described by $\rho_A = \mathrm{Tr}_B(\rho_{AB}) \in \mathcal{D}(A)$, where $\mathrm{Tr}_B(\rho_{AB})$ is the *partial trace* with respect to system B. $H(A)_{\rho_{AB}} \triangleq S_v(\mathrm{Tr}_B(\rho_{AB}))$ and similarly $H(B)_{\rho_{AB}} \triangleq S_v(\mathrm{Tr}_A(\rho_{AB}))$.

Define the conditional entropy (A conditioned on B) as $H(A \mid B)_{\rho_{AB}} \triangleq H(AB)_{\rho_{AB}} - H(B)_{\rho_{AB}}$. Define the mutual information (between A and B) as $I(A; B)_{\rho_{AB}} \triangleq H(A) + H(B) - H(AB) = H(A) - H(A \mid B) = H(B) - H(B \mid A)$. For a tripartite quantum system ABC in the state ρ_{ABC}, the conditional mutual information is defined as $I(A; B \mid C)_{\rho_{ABC}} \triangleq H(A \mid C) + H(B \mid C) - H(AB \mid C) = H(AC) + H(BC) - H(C) - H(ABC) = H(A \mid C) - H(A \mid BC) = H(B \mid C) - H(B \mid AC) = I(A; BC) - I(A; C) = I(AC; B) - I(C; B)$.

For a classical-quantum system XA where X is classical, if conditioned on $X = x$, A is in the state $\rho_A^{(x)}$ for $x \in \mathcal{X}$, then XA is in the joint state $\rho_{XA} \triangleq \sum_{x \in \mathcal{X}} p_X(x) |x\rangle \langle x|_X \otimes \rho_A^{(x)}$. In this case, the reduced state on A becomes $\rho_A = \mathrm{Tr}_X(\rho_{XA}) = \sum_{x \in \mathcal{X}} p_X(x) \rho_A^{(x)}$. We say that $H(A)_{\rho_A^{(x)}}$ is the entropy for A conditioned on $X = x$, which is also written as $H(A \mid X = x)_{\rho_{XA}}$. With these definitions, $H(A \mid X)_{\rho_{XA}} = \sum_{x \in \mathcal{X}} p_X(x) H(A \mid X = x)_{\rho_{XA}}$ (e.g., see [32, Eq. (11.54)]), similar to classical information measures.

We similarly define $H(A \mid B, X = x)_{\rho_{XAB}} = H(A \mid B)_{\rho_{AB}^{(x)}}$, $I(A; B \mid X = x)_{\rho_{XAB}} \triangleq I(A; B)_{\rho_{AB}^{(x)}}$ and $I(A; B \mid C, X = x)_{\rho_{XABC}} \triangleq I(A; B \mid C)_{\rho_{ABC}^{(x)}}$ as the corresponding information measures with conditioning on $X = x$. It is also true that $H(A \mid BX)_{\rho_{XAB}} = \sum_{x \in \mathcal{X}} p_X(x) H(A \mid B, X = x)_{\rho_{XAB}}$, $I(A; B \mid X)_{\rho_{XAB}} = \sum_{x \in \mathcal{X}} p_X(x) I(A; B \mid X = x)_{\rho_{XAB}}$ and $I(A; B \mid CX)_{\rho_{XABC}} = \sum_{x \in \mathcal{X}} p_X(x) I(A; B \mid C, X = x)_{\rho_{XABC}}$.

2.3 Quantum channel

A quantum channel is a completely positive trace-preserving (CPTP) map $\Phi \colon \mathcal{L}(\mathcal{H}) \mapsto \mathcal{L}(\mathcal{H}')$ between two spaces of square linear operators. It has a Choi-Kraus decomposition as $\Phi(M) = \sum_{i=1}^{n} V_i M V_i^\dagger$ for any $M \in \mathcal{L}(\mathcal{H})$, where V_i is a linear operation that takes $\mathcal{L}(\mathcal{H})$ to $\mathcal{L}(\mathcal{H}')$ for $i \in [n]$, such that $\sum_{i=1}^{n} V_i^\dagger V_i = I$ is the identity matrix [32, Thm. 4.4.1]. $\{V_i\}$ are referred to as the Kraus operators of the quantum channel Φ. For two quantum channels $\Phi_A \colon \mathcal{L}(\mathcal{H}_A) \mapsto \mathcal{L}(\mathcal{H}'_A)$ and $\Phi_B \colon \mathcal{L}(\mathcal{H}_B) \mapsto \mathcal{L}(\mathcal{H}'_B)$, $\Phi_A \otimes \Phi_B \colon \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B) \mapsto \mathcal{L}(\mathcal{H}'_A \otimes \mathcal{H}'_B)$ denotes their parallel concatenation. Trace and partial trace are quantum channels. The identity channel is denoted as the identity matrix $\mathbf{I}$ which maps any input operator to the same output.

In this paper, quantum channels are used to model encoding operations and measurements on quantum systems. When we say that an operation Φ (a quantum channel) is applied to a quantum system A, we mean that the system A with initial state ρ_A has state $\rho'_A = \Phi(\rho_A)$ after the operation.

A quantum measurement Ψ is a quantum channel that maps any density operator ρ_A to $\Psi(\rho_A) = \sum_{x \in \mathcal{X}} \mathrm{Tr}(\Lambda_A^{(x)} \rho_A) |x\rangle \langle x|_X$ with $\{\Lambda^{(x)}\}_{x \in \mathcal{X}}$ a set of matrices that define a POVM (positive operator

valued measurement) and $\{|x\rangle\}$ an orthonormal basis [32, Sec. 4.6.6]. $\Psi(\rho_A)$ thus corresponds to the density operator of a classical random variable X with $p_X(x) = \text{Tr}(\Lambda_A^{(x)} \rho_A)$ for $x \in \mathcal{X}$. When we say that a quantum system A in the state ρ_A is measured by Ψ (a quantum measurement), we define a classical random variable X such that $p_X(x) = \text{Tr}(\Lambda^{(x)} \rho)$ for $x \in \mathcal{X}$, and we refer to X as the output of that measurement.

An important set of operations, referred to as the Pauli operations, are defined as follows. Let $\{|a\rangle\}_{a \in \mathbb{F}_q}$ denote the standard basis of a q-dimensional quantum system such that $q = p^r$ is a power of a prime. For $x \in \mathbb{F}_q$, define the $\mathsf{X}(x)$ operation on the system such that $\mathsf{X}(x)|a\rangle = |a + x\rangle$ for $a \in \mathbb{F}_q$. Define the $\mathsf{Z}(z)$ operation on the system such that $\mathsf{Z}(z)|b\rangle = \omega^{\text{tr}(bz)}|b\rangle$ for $b \in \mathbb{F}_q$.

2.4 Useful Lemmas

For our converse proofs, the following lemmas will be useful.

Lemma 1 (No-signaling [33, 34]). *Let XAB be a classical-quantum system where X is classical. Say AB is in the state $\rho_{AB}^{\text{init}} \in \mathcal{D}(AB)$ initially. Let $\{\Phi_A^{(x)}\}_{x \in \mathcal{X}}$ be a set of quantum channels (to be applied to A). Let $\rho_{AB}^{(x)} = \Phi_A^{(x)} \otimes \mathbf{I}_B(\rho_{AB}^{\text{init}})$ for $x \in \mathcal{X}$ and let $\rho_{XAB} = \sum_{x \in \mathcal{X}} p_X(x)|x\rangle\langle x| \otimes \rho_{AB}^{(x)}$. Then $I(B; X)_{\rho_{XAB}} = 0$.*

Proof. It suffices to show that $H(B)_{\rho_{XAB}} = H(B \mid X)_{\rho_{XAB}}$. First note that $\text{Tr}_A(\rho_{AB}^{(x)}) = \text{Tr}_A(\rho_{AB}^{\text{init}})$ for $x \in \mathcal{X}$ because only the identity operation is applied to B. By definition,

$$H(B)_{\rho_{XAB}} = S_v\big(\text{Tr}_{AX}(\rho_{XAB})\big) = S_v\big(\text{Tr}_A \text{Tr}_X(\rho_{XAB})\big) = S_v\big(\text{Tr}_A(\sum_{x \in \mathcal{X}} p_X(x)\rho_{AB}^{(x)})\big)$$

$$= S_v\big(\sum_{x \in \mathcal{X}} p_X(x)\text{Tr}_A(\rho_{AB}^{(x)})\big) = S_v\big(\sum_{x \in \mathcal{X}} p_X(x)\text{Tr}_A(\rho_{AB}^{\text{init}})\big) = S_v\big(\text{Tr}_A(\rho_{AB}^{\text{init}})\big) \qquad (1)$$

On the other hand, by definition, $H(B \mid X = x)_{\rho_{XAB}} = S_v\big(\text{Tr}_A(\rho_{AB}^{(x)})\big) = S_v\big(\text{Tr}_A(\rho_{AB}^{\text{init}})\big)$ for all $x \in \mathcal{X}$, and thus $H(B \mid X)_{XAB} = \sum_{x \in \mathcal{X}} p_X(x)H(B \mid X = x)_{\rho_{XAB}} = S_v\big(\text{Tr}_A(\rho_{AB}^{\text{init}})\big)$. $\qquad \square$

Lemma 2 (Holevo Bound [35]). *Let XA be a classical-quantum system where X is classical, $\rho_A^{(x)} \in \mathcal{D}(A)$ for $x \in \mathcal{X}$ and $\rho_{XA} = \sum_{x \in \mathcal{X}} p_X(x)|x\rangle\langle x| \otimes \rho_A^{(x)}$. Let Ψ be a quantum measurement that measures A in the state $\rho_A = \text{Tr}_X(\rho_{XA})$, and denote the output as Y. Then, $I(X; Y) \leq I(X; A)_{\rho_{XA}}$.*

Proof. Since the density operator for Y after the measurement is $\rho_Y = \Psi(\rho_A)$ where Ψ is a given channel, quantum data processing inequality [32, Thm. 11.9.4] implies $I(X; Y) \leq I(X; A)_{\rho_{XA}}$. $\qquad \square$

3 Problem Statement

3.1 Σ-QEMAC Model

The Σ-QEMAC problem is specified by a finite field $\mathbb{F}_d$, a set of S data-servers with indices $1, \cdots, S$, an auxiliary server (Server 0) with index 0 that may be included to explicitly model prior shared entanglement between Alice and the data-servers, K data streams, T erasure patterns, the data replication map $\mathcal{W} : [K] \mapsto 2^{[S]}$ that specifies the subsets of data-servers among which a data stream is replicated, and the map $\mathcal{E} : [T] \mapsto 2^{[S]}$ that specifies the subsets of servers from which the transmissions may be unavailable (erased). Specifically, for $k \in [K]$, the kth data stream, W_k

is comprised of symbols $W_k^{(\ell)} \in \mathbb{F}_d$ for $\ell \in \mathbb{N}$. The data stream W_k is available at Servers s for all $s \in \mathcal{W}(k) \subseteq [S]$. The coding scheme must allow Alice to recover $W_1 + W_2 + \cdots + W_K$ given that the answers from a subset of servers $\mathcal{E}(t) \subseteq [S]$ are unavailable to the receiver (Alice), for any $t \in [T]$. Note that no data stream is available to Server 0, and the answer from Server 0 cannot be erased, because it represents the shared entanglement that is already available in advance to Alice. Define $\mathcal{S} = \{0\} \cup [S]$ as a compact notation for the set of all $S+1$ server indices.

A quantum coding scheme is specified by a 5-tuple

$$\left(L, \delta_{\mathcal{S}}, \rho^{\mathsf{init}}, \mathsf{Enc}_{[S]}, \mathsf{Dec}\right).$$

Here, $L \in \mathbb{N}$ is the batch size, which specifies the number of instances of the data to be encoded together, i.e., the data to be encoded is $W_{[K]}^{[L]} = (W_1^{[L]}, W_2^{[L]}, \cdots, W_K^{[L]})$. We use $w = (w_1, w_2, \cdots, w_K) \in \mathbb{F}_d^{KL}$ to represent a realization of $(W_1^{[L]}, W_2^{[L]}, \cdots, W_K^{[L]})$, where w_k is the realization of the kth data stream. The superscript '$[L]$' over the data streams may be omitted for compact notation. Given w, for $s \in [S]$, let x_s be the part of w that is available to Server s, i.e., $x_s \triangleq (w_k \colon s \in \mathcal{W}(k))$.

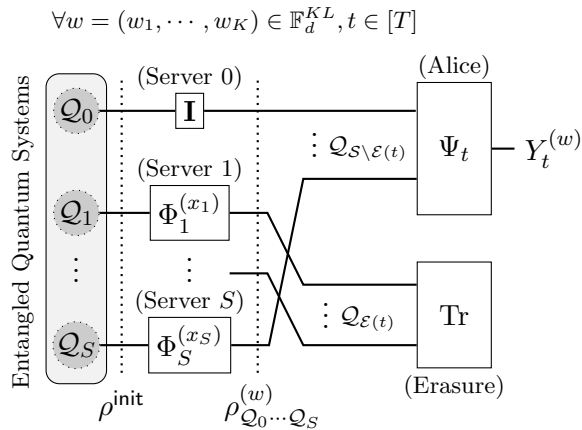$$\forall w = (w_1, \cdots, w_K) \in \mathbb{F}_d^{KL}, t \in [T]$$

Figure 2: A quantum coding scheme for the Σ-QEMAC. The output measured at the receiver, $Y_t^{(w)}$, must be the sum $w_1 + w_2 + \cdots + w_K$.

A quantum system $\mathcal{Q}_{\mathcal{S}} = \mathcal{Q}_0 \mathcal{Q}_1 \cdots \mathcal{Q}_S$ is prepared in advance in the initial state ρ^{init} and shared among the servers so that Server s has the subsystem $\mathcal{Q}_s$ for $s \in \mathcal{S}$. For any data realization $w \in \mathbb{F}_d^{KL}$, the encoder Enc_s at Server $s \in [S]$ is represented by a quantum channel $\Phi_s^{(x_s)}$ that depends on x_s. The output dimension is upper bounded by $\delta_s, s \in \mathcal{S}$ for all w. For $w \in \mathbb{F}_d^{KL}$,

$$\rho_{\mathcal{Q}_0 \cdots \mathcal{Q}_S}^{(w)} \triangleq \mathbf{I} \otimes \Phi_1^{(x_1)} \otimes \cdots \otimes \Phi_S^{(x_S)}\left(\rho^{\mathsf{init}}\right) \tag{2}$$

denotes the output state for the joint quantum system $\mathcal{Q}_0 \mathcal{Q}_1 \cdots \mathcal{Q}_S$, after the channel $\Phi_s^{(x_s)}$ is applied to $\mathcal{Q}_s$, for each $s \in [S]$.

For $t \in [T]$, the decoder Dec is represented by a quantum measurement, Ψ_t, that depends on t, i.e., the erasure pattern that is encountered. For the case when the answers from Servers $s \in \mathcal{E}(t)$ are unavailable at Alice, the remaining subsystem $\mathcal{Q}_{\mathcal{S} \setminus \mathcal{E}(t)}$ in the reduced state,

$$\rho_{\mathcal{Q}_{\mathcal{S} \setminus \mathcal{E}(t)}}^{(w)} = \mathrm{Tr}_{\mathcal{Q}_{\mathcal{E}(t)}}(\rho_{\mathcal{Q}_0 \cdots \mathcal{Q}_S}^{(w)})$$

7

is measured by Ψ_t, with the output represented by the random variable $Y_t^{(w)}$. It is required that the decoding must be always correct, i.e.,

$$\Pr\big(Y_t^{(w)} = w_1 + w_2 + \cdots + w_K\big) = 1 \tag{3}$$

for all data realizations $w \in \mathbb{F}_d^{KL}$, and for *any* case of erasure indexed by $t \in [T]$.

For such a coding scheme, we define $\Delta_s = \log_d \delta_s / L$ as the (normalized) download cost from Server s for $s \in \mathcal{S}$, and $\boldsymbol{\Delta} \triangleq (\Delta_0, \Delta_1, \cdots, \Delta_S)$ as the cost tuple achieved by the scheme.

Let $\mathfrak{C}_L$ be the set of coding schemes with batch size L. Define $\mathfrak{D}^*$ as the closure of the cost tuples achieved by the schemes in $\mathfrak{C}_L$ as $L \to \infty$. The ultimate goal is to study $\mathfrak{D}^*$.

3.2 Symmetric setting

To counter the combinatorial complexity of the problem, we will focus especially on a particular symmetric setting of the Σ-QEMAC. For clarity, it will be useful to identify the symmetric setting by including a superscript s (for symmety), as in Σ^s-QEMAC. The Σ^s-QEMAC setting is specified by a tuple $(\mathbb{F}_d, S, \alpha, \beta)$. The data symbols are from $\mathbb{F}_d$. S, α, β are integers and $S \geq \alpha > \beta \geq 0$ for the problem to be feasible. As in the general Σ-QEMAC, the Σ^s-QEMAC contains S data-servers, indexed by $[S] = \{1, \cdots, S\}$ and an auxiliary server, Server 0 is included if prior shared entanglement is available to Alice. There are $K = \binom{S}{\alpha}$ data streams, each replicated among a unique cardinality-α subset of the data-servers. The answers from any β-subset of the data-servers may be erased. Mathematically, the storage is specified as $\mathcal{W} : [\binom{S}{\alpha}] \mapsto \binom{[S]}{\alpha}$ and the erasure map as $\mathcal{E} : [\binom{S}{\beta}] \mapsto \binom{[S]}{\beta}$, both being bijections. As before, note that none of the K data streams is available to Server 0 and we assume that the answer from Server 0 cannot be erased.

For an illustration of a Σ^s-QEMAC setting, consider Figure 1, where we have $S = 4$ data-servers and an auxiliary Server 0, with $\alpha = 2$ so that there are $K = \binom{4}{2} = 6$ classical data streams, $\mathsf{W}_1, \mathsf{W}_2, \mathsf{W}_3, \mathsf{W}_4, \mathsf{W}_5, \mathsf{W}_6$, relabeled as $\mathsf{A}, \mathsf{B}, \mathsf{C}, \mathsf{D}, \mathsf{E}, \mathsf{F}$, respectively, in the figure for convenience. There is a data stream corresponding to each subset of cardinality $\alpha = 2$ out of the $S = 4$ data-servers, that is available precisely to those $\alpha = 2$ servers. Specifically, the data stream W_1 (equivalently, A) is available to the data-servers with indices in the set $\mathcal{W}(1) = \{1, 2\}$, B to $\mathcal{W}(2) = \{1, 3\}$, C to $\mathcal{W}(3) = \{1, 4\}$, D to $\mathcal{W}(4) = \{2, 3\}$, E to $\mathcal{W}(5) = \{2, 4\}$, F to $\mathcal{W}(6) = \{3, 4\}$. Say in this example $\beta = 1$, which means any one of $\mathcal{Q}_1, \mathcal{Q}_2, \mathcal{Q}_3, \mathcal{Q}_4$ may be erased. Thus, there are $T = \binom{4}{1} = 4$ erasure cases that must be tolerated, comprised of all cardinality-1 subsets of the 4 data-servers, i.e., the indices of the erased servers can be any one of the sets $\{1\}, \{2\}, \{3\}, \{4\}$. Note that Server 0 has no data stream and $\mathcal{Q}_0$ is not subject to erasures.

Recall that the closure of the cost tuples $\boldsymbol{\Delta} = (\Delta_0, \Delta_1, \cdots, \Delta_S)$ achieved by the coding schemes is denoted as $\mathfrak{D}^*$. We are interested in the trade-off between Δ_0 and $\Delta_1 + \cdots + \Delta_S$, i.e., the (normalized) cost of entanglement provided by Server 0 (modeling entanglement previously available to Alice) and the sum (normalized) download cost from the data-servers. $R = (\Delta_1 + \cdots + \Delta_S)^{-1}$ is referred to as the data-server rate (reciprocal of the sum-download cost from the data-servers). For each $\Delta_0 \in \mathbb{R}_+$, we wish to find the capacity, which is defined as $C(\Delta_0) \triangleq \max_{(\Delta_0, \Delta_1, \cdots, \Delta_S) \in \mathfrak{D}^*} R$. Due to the symmetry among data-servers, there is no loss of generality in the assumption that $\Delta_1 = \Delta_2 = \cdots = \Delta_S = \Delta$. Therefore, the optimal tradeoff is equivalently represented as $\Delta^*(\Delta_0) \triangleq \min_{(\Delta_0, \Delta, \cdots, \Delta) \in \mathfrak{D}^*} \Delta$. Note that $C(\Delta_0) = (S\Delta^*(\Delta_0))^{-1}$.

4 Result

4.1 Achievability for an arbitrary Σ-QEMAC

The following theorem states our achievability result for an arbitrary (not necessarily symmetric) Σ-QEMAC.

Theorem 1 (General Achievability). *For the Σ-QEMAC with parameters $(\mathbb{F}_d, \mathcal{S}, K, T, \mathcal{W}, \mathcal{E})$, we have $\mathfrak{D}_{\mathsf{achi}} \subseteq \mathfrak{D}^*$, where*

$$\mathfrak{D}_{\mathsf{achi}} = \mathrm{conv}(\mathfrak{D}_{\mathrm{AME}}^+ \cup \mathfrak{D}_{\mathrm{TQC}}^+), \tag{4}$$

$$\mathfrak{D}_x^+ \triangleq \{(\Delta_0^+, \cdots, \Delta_S^+) \in \mathbb{R}_+^{S+1} \mid \exists (\Delta_0, \cdots, \Delta_S) \in \mathfrak{D}_x, \ \Delta_s^+ \geq \Delta_s, \forall s \in \mathcal{S}\}, \ x \in \{\mathrm{AME}, \mathrm{TQC}\}, \tag{5}$$

$$\mathfrak{D}_{\mathrm{AME}} = \left\{ \boldsymbol{\Delta} \in \mathbb{R}_+^{S+1} \ \middle| \ \min\left\{\sum_{s \in \mathcal{S}} \Delta_s, \sum_{s \in \mathcal{W}(k)} 2\Delta_s\right\} - \sum_{s \in \mathcal{E}(t)} 2\Delta_s \geq 1, \forall k \in [K], t \in [T] \right\}, \tag{6}$$

$$\mathfrak{D}_{\mathrm{TQC}} = \left\{ \boldsymbol{\Delta} \in \mathbb{R}_+^{S+1} \ \middle| \ \sum_{s \in \mathcal{W}(k)} \Delta_s - \sum_{s \in \mathcal{E}(t)} \Delta_s \geq 1, \forall k \in [K], t \in [T] \right\}. \tag{7}$$

Theorem 1 is an inner bound (based on an achievability argument) on the optimal tradeoff region $\mathfrak{D}^*$. The proof appears in Section 6. We first prove $\mathfrak{D}_{\mathrm{AME}} \subseteq \mathfrak{D}^*$ by constructing coding schemes that make use of quantum entanglement. The name 'AME' comes from the fact that the quantum state in the scheme is an "absolutely maximally entangled" state (e.g., see [36–38]). The design is facilitated by the N-sum box protocol in [29]. On the other hand, $\mathfrak{D}_{\mathrm{TQC}} \subseteq \mathfrak{D}^*$ is directly implied by a classical network coding result in [27] together with the idea of 'treating qudits as classical dits' (TQC). It then follows that $\mathfrak{D}_{\mathrm{AME}}^+ \subseteq \mathfrak{D}^*$ and $\mathfrak{D}_{\mathrm{TQC}}^+ \subseteq \mathfrak{D}^*$. Finally, by a time-sharing argument, any convex combination of the tuples in $\mathfrak{D}_{\mathrm{AME}}^+ \cup \mathfrak{D}_{\mathrm{TQC}}^+$ is also in $\mathfrak{D}^*$. This means that $\mathfrak{D}_{\mathsf{achi}} = \mathrm{conv}(\mathfrak{D}_{\mathrm{AME}}^+ \cup \mathfrak{D}_{\mathrm{TQC}}^+) \subseteq \mathfrak{D}^*$.

4.2 Known converse bounds

Let us recall a useful bound from [30,31], which we present here under the framework of Σ^s-QEMAC to make the connection more transparent.

Theorem 2 (EACQ singleton bound [31]). *Consider the Σ^s-QEMAC with S data-servers and an auxiliary Server 0, with $\alpha = S$ so that we have only $K = 1$ data stream W, which is available only to the data-servers, and the answers from any β of the data-servers may be erased. Then any $(\Delta_0, \Delta_1, \cdots, \Delta_S) \in \mathfrak{D}^*$ must satisfy the bounds,*

$$\sum_{s \in \mathcal{I}} \Delta_s \geq 1/2, \quad \forall \mathcal{I} \in \binom{[S]}{S - \beta}, \tag{8}$$

$$and \ \ \Delta_0 + \Delta_1 + \cdots + \Delta_S \geq \frac{S}{S - \beta}. \tag{9}$$

Note that in this theorem since there is only one data stream, computing the sum is equivalent to recovering the data stream. So the Σ-QEMAC problem reduces to a standard communication problem. Thus, this theorem essentially follows from the EACQ singleton bound [31], for the special case of trading *qudits and entanglement* for *classical information*. Since the erasure in our model is assumed to be server-wise instead of channel-wise as assumed in [31], for the sake of completeness we provide in this paper the proof for our model in Appendix D.

In some cases, following a cut-set argument (separating the parties into into two groups and allowing full cooperation within each group, e.g., [5]), the converse for the resulting point to point communication problem yields useful outer bounds on $\mathfrak{D}^*$ for our computation problem. However, we will see that this approach does not suffice in general, and new converse bounds are needed.

4.3 The Capacity of the Σ^s-QEMAC

Next we specialize from arbitrary Σ-QEMAC settings to symmetric settings, and present a sharp capacity characterization for the Σ^s-QEMAC, which is the main contribution of this work. Recall that the feasibility for the symmetric case requires that $S \geq \alpha > \beta \geq 0$.

Theorem 3. *For $\Delta_0 \in \mathbb{R}_+$, the capacity of the Σ^s-QEMAC is $C(\Delta_0) = (S\Delta^*)^{-1}$, where*

$$
\begin{aligned}
\Delta^* &\triangleq \min_{(\Delta_0, \Delta, \cdots, \Delta) \in \mathfrak{D}^*} \Delta \\
&= \begin{cases} \max\left\{ \frac{1}{2(\alpha-\beta)}, \frac{1-\Delta_0}{S-2\beta} \right\}, & S \geq \alpha + \beta \\ \max\left\{ \frac{1}{2(\alpha-\beta)}, \frac{1}{\alpha-\beta} - \frac{\Delta_0}{2\alpha-S} \right\}, & S < \alpha + \beta \end{cases} .
\end{aligned}
\tag{10}
$$

The proof appears in Section 7. Note that Theorem 3 is a capacity result, and as such requires both a proof of achievability and a tight converse. The achievability is obtained by letting $\Delta_0 \in \mathbb{R}_+$ and $\Delta_1 = \Delta_2 = \cdots = \Delta_S = \Delta$ in Theorem 1 and evaluating the smallest Δ with respect to Δ_0 such that $(\Delta_0, \Delta, \cdots, \Delta) \in \mathfrak{D}_{\mathsf{achi}}$. The smallest Δ turns out to be Δ^* in (10). Then $C(\Delta_0) \geq (S\Delta^*)^{-1}$ establishes the inner (lower) bound for $C(\Delta_0)$. The outer (upper) bound $C(\Delta_0) \leq (S\Delta^*)^{-1}$ utilizes not only the EACQ singleton bound (Theorem 2) combined with a cut-set argument, but also a new bound that is derived in this work, where weak monotonicity [39, 40] of quantum entropy plays an important role. Insufficiency of the EACQ singleton bound and cut-set argument is demonstrated by an example in Section 5.

The next two corollaries follow directly from Theorem 3. The first corollary considers the case $\Delta_0 = 0$, i.e., when no entanglement is shared initially between Alice and the data-servers. Essentially Server 0 does not exist in this case. However, entanglement is still allowed among the data-servers.

Corollary 1 ($\Delta_0 = 0$). *For $\Delta_0 = 0$,*

$$
C(0) = \max\left\{ \underbrace{\min\left\{ \frac{2(\alpha-\beta)}{S}, \frac{S-2\beta}{S} \right\}}_{R_{\mathrm{AME}}}, \underbrace{\frac{\alpha-\beta}{S}}_{R_{\mathrm{TQC}}} \right\}
\tag{11}
$$

$$
= \begin{cases} \frac{2(\alpha-\beta)}{S} = R_{\mathrm{AME}}, & S \geq 2\alpha \\ \frac{S-2\beta}{S} = R_{\mathrm{AME}}, & \alpha + \beta \leq S \leq 2\alpha \\ \frac{\alpha-\beta}{S} = R_{\mathrm{TQC}}, & S \leq \alpha + \beta \end{cases} .
\tag{12}
$$

R_{AME} that appears in (11) is defined as the maximal value of $(\Delta_1 + \cdots + \Delta_S)^{-1}$ (given $\Delta_0 = 0$) for $\boldsymbol{\Delta} \in \mathfrak{D}_{\mathrm{AME}}$. Thus, R_{AME} is achieved by our quantum coding scheme. Similarly, R_{TQC} is defined as the maximal value of $(\Delta_1 + \cdots + \Delta_S)^{-1}$ (given $\Delta_0 = 0$) for $\boldsymbol{\Delta} = (\Delta_0, \Delta_1, \cdots, \Delta_S) \in \mathfrak{D}_{\mathrm{TQC}}$. Thus, R_{TQC} is achieved by treating qudits as classical dits. It can be seen from (12) that when $S > \alpha + \beta$,

we have $R_{\text{AME}} > R_{\text{TQC}}$, i.e., the optimal scheme is our proposed scheme that is facilitated by the N-sum box abstraction and utilizes quantum entanglement, outperforming the classical scheme which does not require quantum entanglement.

Fig. 3 illustrates the capacity (and the rates $R_{\text{AME}}, R_{\text{TQC}}$) from Corollary 1 with $S = 8$ data-servers and erasure levels $\beta \in \{1, 2\}$ for various data replication levels α.

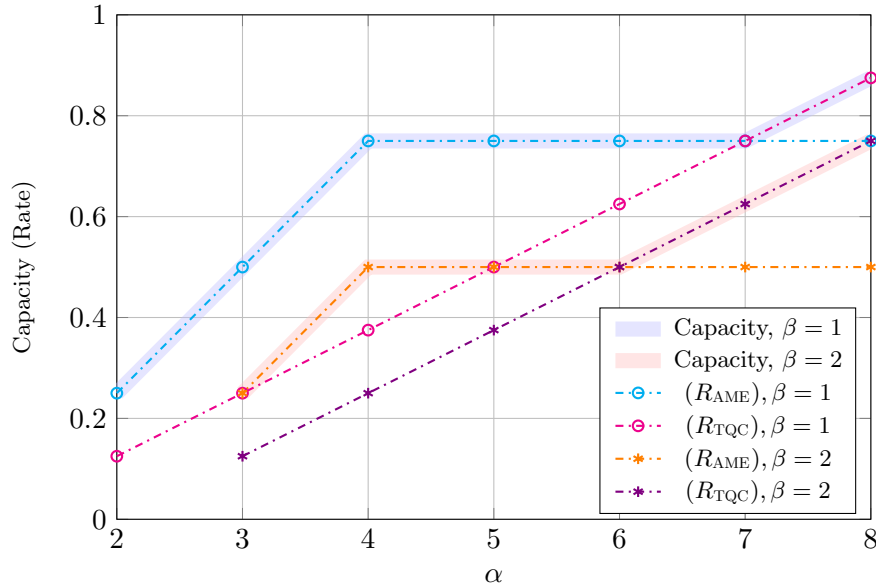Figure 3: The capacity (and rates R_{AME} and R_{TQC}) are shown for $S = 8$, $\beta \in \{1, 2\}$ versus α when the receiver Alice has no prior shared entanglement with the data-servers ($\Delta_0 = 0$). The data-servers are still allowed to be entangled. Note that R_{TQC} is the capacity of classical codes.

As Δ_0 is increased, i.e., as the amount of initially shared entanglement between Alice and the data-servers is increased, there appears a critical threshold beyond which the capacity saturates, i.e., additional entanglement does not improve the capacity of the Σ^s-QEMAC. This threshold is highlighted in the second corollary.

Corollary 2 (Saturation). $C(\Delta_0) = \frac{2(\alpha-\beta)}{S}$ *if* $\Delta_0 \geq \frac{2\alpha-S}{2(\alpha-\beta)}$.

Evidently, when Δ_0 is above the threshold[1] value $\frac{2\alpha-S}{2(\alpha-\beta)}$, then the capacity is equal to $\frac{2(\alpha-\beta)}{S}$ which is 2 times the classical capacity R_{TQC} that appears in (12). The factor of 2 represents a superdense coding gain [21, 41], and one might wonder if it can be achieved with only pairwise entanglements of each data-server with Server 0 based on the original superdense coding protocol [41]. Indeed, such a pairwise superdense coding strategy can achieve the rate $R = \frac{2(\alpha-\beta)}{S}$ but it requires $\Delta_0 \geq \frac{S}{2(\alpha-\beta)}$, i.e., more entanglement than the threshold in Corollary 2. This is explained as follows. The classical scheme achieves the cost tuple $(\Delta_1, \cdots, \Delta_S) = (\frac{1}{\alpha-\beta}, \cdots, \frac{1}{\alpha-\beta})$. Then using pairwise superdense coding, $\Delta_0 = \frac{S}{2(\alpha-\beta)}$ and $\Delta_1 = \cdots = \Delta_S = \frac{1}{2(\alpha-\beta)}$ is achievable.

Let us reiterate that the saturation threshold in Corollary 2 is *non-trivial* because this threshold is reached with strictly smaller Δ_0. Note that $S > \alpha$ when we have more than one data-stream, so $2\alpha - S < S$. Thus, pairwise superdense coding is not sufficient to achieve the capacity in Corollary

---

[1]If $\frac{2\alpha-S}{2(\alpha-\beta)} \leq 0$, then any $\Delta_0 \geq 0$ suffices.

2. Indeed, our achievable scheme utilizes entanglement across all servers, instead of merely pairwise entanglements.

Fig. 4 illustrates the functional form of $\Delta^*(\Delta_0)$ defined in (10) evaluated for $(S, \alpha, \beta) = (4, 3, 2)$.
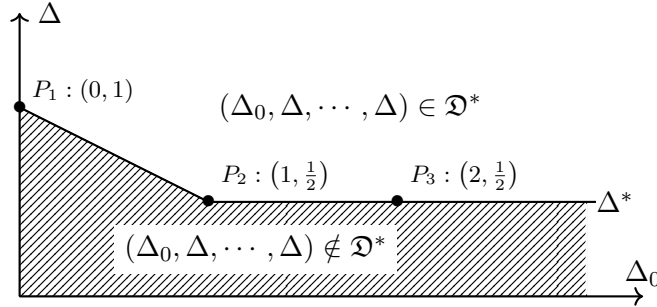

Figure 4: The functional form of $\Delta^*(\Delta_0)$ defined in (10) is illustrated for $(S, \alpha, \beta) = (4, 3, 2)$. P_1 is achieved by treating qudits as classical dits (TQC). (This follows from Corollary 1 since for this example $S \leq \alpha + \beta$. If $S > \alpha + \beta$, entanglement is still required to achieve Δ^* for $\Delta_0 = 0$). P_2 is achieved by our quantum coding scheme (AME). P_3 is achievable with the original superdense coding scheme based on pairwise entanglements.

5 Example

5.1 Converse bounds for symmetric $(S, \alpha, \beta) = (3, 2, 1)$

Let us show the insufficiency of the cut-set argument through an example of a Σ^s-QEMAC with $(S, \alpha, \beta) = (3, 2, 1)$. There are $K = \binom{3}{2} = 3$ data streams, denoted as $\mathsf{A}, \mathsf{B}, \mathsf{C}$. Without loss of generality, say Server 1 has (A, B), Server 2 has (A, C) and Server 3 has (B, C). To simplify the example further, let us set $\Delta_0 = 0$, so that Server 0 can be ignored. Say, $\beta = 1$, meaning that one of $\mathcal{Q}_1, \mathcal{Q}_2$ or $\mathcal{Q}_3$ may get erased.

Let us first apply the EACQ singleton bound with a cut-set argument to establish a baseline. For the cut-set argument, we need to separate the parties {Alice, Server 1, Server 2, Server 3} into 2 groups. The group that contains Alice will jointly act as a receiver while the other group jointly acts as a transmitter in the resulting communication problem. Consider the following cuts.

1. "A cut": We collect the parties that have the data-stream A, i.e., {Server 1, Server 2} into one group (transmitter) and {Server 3, Alice} into the other group (receiver). Suppose $\mathsf{B} = \mathsf{C} = 0$ (or any constant, that is known by the receiver). Then the receiver must be able to determine A, even if one of $\mathcal{Q}_1$ or $\mathcal{Q}_2$ gets erased. According to Theorem 2, with $\Delta_1 = \Delta_2 = \Delta_3 = \Delta$, we have the bound,

$$2\Delta \geq 1/2, \quad \text{and} \quad 3\Delta \geq 2 \implies \Delta \geq 2/3. \tag{13}$$

2. "AB cut": We collect the parties that have at least one of the data-streams A, B, i.e., {Server 1, Server 2, Server 3} into the transmitter group, leaving only {Alice} in the receiver group.
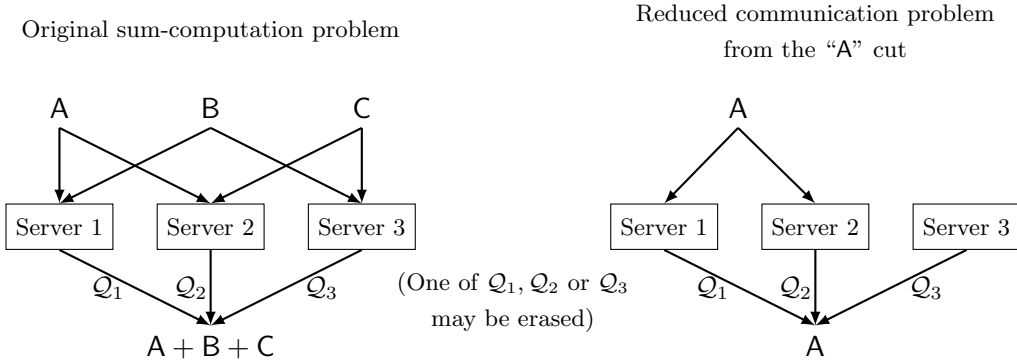
Figure 5: Original sum-computation problem and the reduced communication problem from the "A" cut.

Suppose $C = 0$. Then the receiver must be able to determine $A + B$ (which can be regarded as a single data stream). According to Theorem 2, we have

$$3\Delta \geq 1/2, \quad \text{and} \quad 3\Delta \geq 3/2 \implies \Delta \geq 1/2. \tag{14}$$

3. "ABC cut": The grouping can be also based on who has either (A or B or C), but this will yield the same partitioning and thus the same bound as the second case.

Other cuts also do not produce new bounds due to the symmetry of the problem, e.g., "B cut" produces the same bound as the "A cut", "BC cut" produces the same bound as the "AB cut", etc. Therefore, the cut-set and the EACQ singleton bound give us at best the converse bound $\Delta \geq 2/3$, which comes from the "A cut".

However, this bound $\Delta \geq 2/3$ is not tight for the Σ^s-QEMAC problem where Alice must recover the sum $A + B + C$. As shown by Theorem 3, the smallest Δ given $\Delta_0 = 0$ for $(S, \alpha, \beta) = (3, 2, 1)$ is equal to $\Delta^* = 1$.

One may wonder if this is because the EACQ bound implicitly assumes that $\mathcal{Q}_3$ cannot be erased. Taking into consideration that $\mathcal{Q}_3$ may also be erased, we prove in Appendix A that $\Delta = 3/4 < 1$ is still achievable for the communication problem reduced from the "A cut", based on superdense coding. This shows that such a cut-set argument *cannot* provide stronger bounds than $\Delta \geq 3/4$, establishing the insufficiency of the cut-set argument for the Σ^s-QEMAC. This observation shows an interesting distinction between the Σ-QEMAC, where erasures are allowed, and the original Σ-QMAC setting of [21], in which no erasure is considered. A cut-set argument combined with a tight communication bound suffices for the converse bounds for the Σ-QMAC in [21], but not for the Σ-QEMAC considered in this work.

In fact the property of *weak monotonicity*[2] of quantum entropy (see e.g., [39, 43]) plays an important role in proving a tight converse for the Σ^s-QEMAC. Intuitively, this is reminiscent of a result in [40] referred to as the exclusion principle in dense coding. However, since the Σ^s-QEMAC has distributed data streams and the information desired by Alice is a function (sum) of the data-streams rather the data-streams themselves, the connection to [40] is not straightforward.

To conclude this example, let us prove the bound $\Delta \geq 1$. Since a coding scheme must be correct for every realization of (A, B, C), it must be correct if A, B, C are independent random

---

[2]Weak monotonicity is regarded as equivalent to the strong subadditivity property of quantum entropies [42].

variables uniformly distributed in $\mathbb{F}_d^L$. Depending on the case of erasure, the measurement result is denoted as Y_1 (if $\mathcal{Q}_1$ gets erased); Y_2 (if $\mathcal{Q}_2$ gets erased) and Y_3 (if $\mathcal{Q}_3$ gets erased). Note that given any coding scheme, after the servers apply their encoding operations, the state of $\mathsf{ABC}\mathcal{Q}_1\mathcal{Q}_2\mathcal{Q}_3$ is determined, denoted as ρ. Let us consider the erasure of $\mathcal{Q}_1$ and conditioning on (B,C). In this case we have,

$$L = I(\mathsf{A},\mathsf{B},\mathsf{C};\mathsf{A}+\mathsf{B}+\mathsf{C}\mid \mathsf{B},\mathsf{C}) \tag{15}$$
$$= I(\mathsf{A},\mathsf{B},\mathsf{C};Y_1\mid \mathsf{B},\mathsf{C}) \tag{16}$$
$$= I(\mathsf{A};Y_1\mid \mathsf{B},\mathsf{C}) \tag{17}$$
$$\leq I(\mathsf{A};\mathcal{Q}_2,\mathcal{Q}_3\mid \mathsf{B},\mathsf{C})_\rho \tag{18}$$
$$= \underbrace{I(\mathsf{A};\mathcal{Q}_3\mid \mathsf{B},\mathsf{C})_\rho}_{=0} + I(\mathsf{A};\mathcal{Q}_2\mid \mathcal{Q}_3,\mathsf{B},\mathsf{C})_\rho \tag{19}$$
$$= I(\mathsf{A};\mathcal{Q}_2\mid \mathcal{Q}_3,\mathsf{B},\mathsf{C})_\rho \tag{20}$$
$$= H(\mathcal{Q}_2\mid \mathcal{Q}_3,\mathsf{B},\mathsf{C})_\rho - H(\mathcal{Q}_2\mid \mathcal{Q}_3,\mathsf{A},\mathsf{B},\mathsf{C})_\rho \tag{21}$$
$$\leq H(\mathcal{Q}_2)_\rho - H(\mathcal{Q}_2\mid \mathcal{Q}_3,\mathsf{A},\mathsf{B},\mathsf{C})_\rho \tag{22}$$

Step (18) is by Lemma 2 since Alice obtains Y_1 conditioned on any realization of (B,C) by measuring $\mathcal{Q}_2\mathcal{Q}_3$. Step (20) is by Lemma 1 conditioned on any realization of (B,C), since A is not available to Server 3. Step (22) is because conditioning does not increase entropy. By symmetry, one can similarly obtain,

$$L \leq H(\mathcal{Q}_2)_\rho - H(\mathcal{Q}_2\mid \mathcal{Q}_1,\mathsf{A},\mathsf{B},\mathsf{C})_\rho \tag{23}$$

by considering the erasure of $\mathcal{Q}_3$ and conditioning on (A,B). Adding (22) and (23), we have

$$2L \leq 2H(\mathcal{Q}_2)_\rho - \underbrace{\left(H(\mathcal{Q}_2\mid \mathcal{Q}_3,\mathsf{A},\mathsf{B},\mathsf{C})_\rho + H(\mathcal{Q}_2\mid \mathcal{Q}_1,\mathsf{A},\mathsf{B},\mathsf{C})_\rho\right)}_{\geq 0} \tag{24}$$
$$\leq 2H(\mathcal{Q}_2)_\rho \tag{25}$$

because of weak monotonicity,[3] conditioned on any realization of $(\mathsf{A},\mathsf{B},\mathsf{C})$. This shows that $\Delta_2 = \log_d \delta_2/L \geq H(\mathcal{Q}_2)_\rho/L \geq 1$. $\qquad\square$

5.2 N-sum box based coding scheme for the example in Fig. 1 with $\Delta_0 = 0$

Let us present the solution for the example in Fig. 1 for the case where Alice has no prior entanglement with the data-servers, i.e., $\Delta_0 = 0$ so Server 0 can be ignored. Let $\mathsf{A}_\ell,\mathsf{B}_\ell,\cdots,\mathsf{F}_\ell \in \mathbb{F}_5$ for all $\ell \in [L]$, and set $L = 2$ as the batch size of the coding scheme. Thus, the coding scheme must allow Alice to compute $\mathsf{A}_{[2]}+\mathsf{B}_{[2]}+\cdots+\mathsf{F}_{[2]}$, with each server transmitting a $\delta = 5$ dimensional quantum system, while tolerating the loss of the quantum subsystem from any one of the servers. The rate to be achieved is $R = 2/(4\log_5 5) = 1/2$. The scheme makes use of the N-sum box formulation in [29], which is summarized as a lemma below.

Lemma 3 (N-sum box [29]). *Given a field $\mathbb{F}_q$, a positive integer N, and an $N \times 2N$ matrix $\mathbf{M} = [\mathbf{M}_l,\mathbf{M}_r]$ where $\mathbf{M}_l,\mathbf{M}_r \in \mathbb{F}_q^{N\times N}$ satisfy the self-orthogonality constraint: $\mathbf{M}_r\mathbf{M}_l^\top = \mathbf{M}_l\mathbf{M}_r^\top$, there exists a set of orthogonal quantum states, denoted as $\{|\mathbf{a}\rangle_\mathbf{M}\}_{\mathbf{a}\in\mathbb{F}_q^{N\times 1}}$ on N q-dimensional*

---
[3]For a tripartite quantum system XYZ in the state ρ, $H(X|Y)_\rho + H(X|Z)_\rho \geq 0$.

quantum subsystems $Q_1, Q_2, \cdots, Q_N$, *such that applying* $\mathsf{X}(x_i)\mathsf{Z}(z_i)$ *to* Q_i *for all* $i \in [N]$, *the state of the composite quantum system* Q *changes from* $|\mathbf{a}\rangle_{\mathbf{M}}$ *to* $|\mathbf{a} + \mathbf{M}[\begin{smallmatrix}\mathbf{x}\\\mathbf{z}\end{smallmatrix}]\rangle_{\mathbf{M}}$ *(with global phases omitted), i.e.,* $\otimes_{i\in[N]}\mathsf{X}(x_i)\mathsf{Z}(z_i)|\mathbf{a}\rangle \equiv |\mathbf{a} + \mathbf{M}[\begin{smallmatrix}\mathbf{x}\\\mathbf{z}\end{smallmatrix}]\rangle_{\mathbf{M}}$, *where* $\mathbf{x} \triangleq [x_1, \cdots, x_N]^\top \in \mathbb{F}_q^{N\times 1}$ *and* $\mathbf{z} \triangleq [z_1, \cdots, z_N]^\top \in \mathbb{F}_q^{N\times 1}$. *We say that* $(\mathbb{F}_q, N, \mathbf{M}, \{|\mathbf{v}\rangle_{\mathbf{M}}\}_{\mathbf{a}\in\mathbb{F}_q^{N\times 1}})$ *is an* N-*sum box defined in* $\mathbb{F}_q$ *with transfer matrix* $\mathbf{M}$.

Suppose the 5-dimensional quantum subsystems available to the 4 servers are Q_1, Q_2, Q_3 and Q_4, respectively. Let us construct an $N = 4$-sum box defined in $\mathbb{F}_5$ with transfer matrix

$$\mathbf{M} = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 2 & 3 & 4 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 & 3 & 4 \\ 0 & 0 & 0 & 0 & 1 & 4 & 4 & 1 \end{bmatrix} \tag{26}$$

$$= [\mathbf{m}_{1x}, \cdots, \mathbf{m}_{4x}, \mathbf{m}_{1z}, \cdots, \mathbf{m}_{4z}] \tag{27}$$

where $\mathbf{m}_{ix}, \mathbf{m}_{iz}$ are the ith, $(i+4)^{th}$ columns of $\mathbf{M}$ for $i \in [4]$. One can verify that this $\mathbf{M}$ satisfies the self-orthogonality constraint required by Lemma 3. Moreover, this $\mathbf{M}$ has the following property.

Property P1: Given any subset $\mathcal{I} \subseteq [4]$, the submatrix of $\mathbf{M}$ with columns $\mathbf{m}_{ix}, \mathbf{m}_{iz}$ for $i \in \mathcal{I}$ has full rank, equal to $\min\{4, 2|\mathcal{I}|\}$.

For $s \in [4]$, Server s applies $\mathsf{X}(x_s)\mathsf{Z}(z_s)$ to its quantum subsystem, so that $[x_s, z_s]^\top$ is a linear function of the data that is available to Server s. Generally, we can write $[x_s, z_s]^\top$ as,

$$\begin{bmatrix} x_1 \\ z_1 \end{bmatrix} = V_{1a}\begin{bmatrix} \mathsf{A}_1 \\ \mathsf{A}_2 \end{bmatrix} + V_{1b}\begin{bmatrix} \mathsf{B}_1 \\ \mathsf{B}_2 \end{bmatrix} + V_{1c}\begin{bmatrix} \mathsf{C}_1 \\ \mathsf{C}_2 \end{bmatrix} \tag{28}$$

$$\begin{bmatrix} x_2 \\ z_2 \end{bmatrix} = V_{2a}\begin{bmatrix} \mathsf{A}_1 \\ \mathsf{A}_2 \end{bmatrix} + V_{2d}\begin{bmatrix} \mathsf{D}_1 \\ \mathsf{D}_2 \end{bmatrix} + V_{2e}\begin{bmatrix} \mathsf{E}_1 \\ \mathsf{E}_2 \end{bmatrix} \tag{29}$$

$$\begin{bmatrix} x_3 \\ z_3 \end{bmatrix} = V_{3b}\begin{bmatrix} \mathsf{B}_1 \\ \mathsf{B}_2 \end{bmatrix} + V_{3d}\begin{bmatrix} \mathsf{D}_1 \\ \mathsf{D}_2 \end{bmatrix} + V_{3f}\begin{bmatrix} \mathsf{F}_1 \\ \mathsf{F}_2 \end{bmatrix} \tag{30}$$

$$\begin{bmatrix} x_4 \\ z_4 \end{bmatrix} = V_{4c}\begin{bmatrix} \mathsf{C}_1 \\ \mathsf{C}_2 \end{bmatrix} + V_{4e}\begin{bmatrix} \mathsf{E}_1 \\ \mathsf{E}_2 \end{bmatrix} + V_{4f}\begin{bmatrix} \mathsf{F}_1 \\ \mathsf{F}_2 \end{bmatrix} \tag{31}$$

where V_{s*} is a 2×2 matrix with elements free to be chosen in $\mathbb{F}_5$, for all $s \in [4], * \in \{a, b, c, d, e, f\}$. According to Lemma 3, if the initial state of the composite quantum system Q is $|\mathbf{0}\rangle_{\mathbf{M}}$, then after the operations, the state becomes $|Y\rangle_{\mathbf{M}}$ and

$$Y = \begin{bmatrix} \mathbf{m}_{1x} & \mathbf{m}_{1z} & \mathbf{m}_{2x} & \mathbf{m}_{2z} \end{bmatrix}\begin{bmatrix} V_{1a} \\ V_{2a} \end{bmatrix}\begin{bmatrix} \mathsf{A}_1 \\ \mathsf{A}_2 \end{bmatrix}$$

$$+ \begin{bmatrix} \mathbf{m}_{1x} & \mathbf{m}_{1z} & \mathbf{m}_{3x} & \mathbf{m}_{3z} \end{bmatrix}\begin{bmatrix} V_{1b} \\ V_{3b} \end{bmatrix}\begin{bmatrix} \mathsf{B}_1 \\ \mathsf{B}_2 \end{bmatrix}$$

$$+ \begin{bmatrix} \mathbf{m}_{1x} & \mathbf{m}_{1z} & \mathbf{m}_{4x} & \mathbf{m}_{4z} \end{bmatrix}\begin{bmatrix} V_{1c} \\ V_{4c} \end{bmatrix}\begin{bmatrix} \mathsf{C}_1 \\ \mathsf{C}_2 \end{bmatrix}$$

$$+ \begin{bmatrix} \mathbf{m}_{2x} & \mathbf{m}_{2z} & \mathbf{m}_{3x} & \mathbf{m}_{3z} \end{bmatrix}\begin{bmatrix} V_{2d} \\ V_{3d} \end{bmatrix}\begin{bmatrix} \mathsf{D}_1 \\ \mathsf{D}_2 \end{bmatrix}$$

$$+ \begin{bmatrix} \mathbf{m}_{2x} & \mathbf{m}_{2z} & \mathbf{m}_{4x} & \mathbf{m}_{4z} \end{bmatrix}\begin{bmatrix} V_{2e} \\ V_{4e} \end{bmatrix}\begin{bmatrix} \mathsf{E}_1 \\ \mathsf{E}_2 \end{bmatrix}$$

$$+ \begin{bmatrix} \mathbf{m}_{3x} & \mathbf{m}_{3z} & \mathbf{m}_{4x} & \mathbf{m}_{4z} \end{bmatrix}\begin{bmatrix} V_{3f} \\ V_{4f} \end{bmatrix}\begin{bmatrix} \mathsf{F}_1 \\ \mathsf{F}_2 \end{bmatrix} \tag{32}$$

$$\triangleq \mathbf{M}_a\mathbf{V}_a\begin{bmatrix} \mathsf{A}_1 \\ \mathsf{A}_2 \end{bmatrix} + \cdots + \mathbf{M}_f\mathbf{V}_f\begin{bmatrix} \mathsf{F}_1 \\ \mathsf{F}_2 \end{bmatrix} \tag{33}$$

where in the last equation (33) we define the compact notations $\mathbf{M}_*, \mathbf{V}_*$ for $* \in \{a, b, c, d, e, f\}$. The matrix $\mathbf{V}_*$ is 4×2 with elements in $\mathbb{F}_5$ yet to be determined. It remains to specify $\mathbf{V}_*$. Let us first define a matrix,

$$\mathbf{U} = \begin{bmatrix} 4 & 3 \\ 1 & 1 \\ 2 & 2 \\ 1 & 3 \end{bmatrix}. \tag{34}$$

There is nothing too special about this choice of $\mathbf{U}$, except that we need it to satisfy the following property.

Property P2: $\mathrm{rk}([\mathbf{U}, \mathbf{m}_{tx}, \mathbf{m}_{tz}]) = 4$, i.e., $[\mathbf{U}, \mathbf{m}_{tx}, \mathbf{m}_{tz}]$ is invertible for $t \in [4]$.

By Property **P1**, for $* \in \{a, b, c, d, e, f\}$, the matrix $\mathbf{M}_*$ has full rank 4 and is invertible. Now we can specify $\mathbf{V}_*$ such that

$$Y = \mathbf{U}\begin{bmatrix} \mathsf{A}_1 \\ \mathsf{A}_2 \end{bmatrix} + \mathbf{U}\begin{bmatrix} \mathsf{B}_1 \\ \mathsf{B}_2 \end{bmatrix} + \cdots + \mathbf{U}\begin{bmatrix} \mathsf{F}_1 \\ \mathsf{F}_2 \end{bmatrix} \tag{35}$$

$$= \mathbf{U}\left(\begin{bmatrix} \mathsf{A}_1 \\ \mathsf{A}_2 \end{bmatrix} + \begin{bmatrix} \mathsf{B}_1 \\ \mathsf{B}_2 \end{bmatrix} + \cdots + \begin{bmatrix} \mathsf{F}_1 \\ \mathsf{F}_2 \end{bmatrix} \right) \tag{36}$$

by letting $\mathbf{V}_* = \mathbf{M}_*^{-1}\mathbf{U}$ for $* \in \{a, b, c, d, e, f\}$.

The next step is to consider the transmission of the quantum subsystems. Suppose during the transmission, there exists one $t \in [4]$ such that Q_t is subjected to another operation $\mathsf{X}(\tilde{x})\mathsf{Z}(\tilde{z})$ where $\tilde{x}, \tilde{z}$ are unknown. The state of the composite system now becomes $|Y'\rangle_{\mathbf{M}}$ and

$$Y' = \mathbf{U}\left(\begin{bmatrix} \mathsf{A}_1 \\ \mathsf{A}_2 \end{bmatrix} + \begin{bmatrix} \mathsf{B}_1 \\ \mathsf{B}_2 \end{bmatrix} + \cdots + \begin{bmatrix} \mathsf{F}_1 \\ \mathsf{F}_2 \end{bmatrix} \right) + [\, \mathbf{m}_{tx}, \mathbf{m}_{tz} \,]\begin{bmatrix} \tilde{x} \\ \tilde{z} \end{bmatrix}. \tag{37}$$

After receiving the composite system, Alice obtains Y' as the result of her measurement with certainty. By Property **P2**, if Alice knows t, then she can retrieve

$$\begin{bmatrix} \mathsf{A}_1 \\ \mathsf{A}_2 \end{bmatrix} + \begin{bmatrix} \mathsf{B}_1 \\ \mathsf{B}_2 \end{bmatrix} + \cdots + \begin{bmatrix} \mathsf{F}_1 \\ \mathsf{F}_2 \end{bmatrix} \tag{38}$$

by multiplying $[\mathbf{U}, \mathbf{m}_{tx}, \mathbf{m}_{tz}]^{-1}$ to Y' and taking the top 2 elements. Note that the scheme works no matter which quantum subsystem Q_t is subjected to the unknown operations $\mathsf{X}(\tilde{x})\mathsf{Z}(\tilde{z})$. In addition, $\tilde{x}, \tilde{z}$ can be any value in $\mathbb{F}_5$. Therefore, the scheme also works if $\tilde{x}, \tilde{z}$ are independent and uniformly drawn in $\mathbb{F}_5$. But if Q_t is subjected to the operation $\mathsf{X}(\tilde{x})\mathsf{Z}(\tilde{z})$ with independent $\tilde{x}, \tilde{z}$ chosen uniformly in $\mathbb{F}_5$, then it puts Q_t in the maximally mixed state and makes it *independent* of (and unentangled with) the rest of the quantum subsystems (Lemma 4). In other words, Alice is able to recover the desired sum even if any one of the 4 quantum systems (Alice knows which one) is subjected to random $\mathsf{X}(\tilde{x})\mathsf{Z}(\tilde{z})$ operations that make it independent of the rest of the quantum systems. Recall that positions of erasures are by definition known to the receiver.

What this implies is that even if Q_t is lost, i.e., not received by Alice, the scheme still works [44] if Alice simply replaces the missing $\mathcal{Q}_t$ by an ancillary 5-dimensional quantum subsystem $\widehat{Q}$ that is in the maximally mixed state described by the density operator $\rho_{\widehat{Q}} = \mathbf{I}_5/5$, where $\mathbf{I}_5$ denotes the 5×5 identity matrix, and $\widehat{Q}$ is independent of the quantum system Q (with density operator ρ_Q) composed of Q_1, Q_2, Q_3, Q_4, i.e., the joint state of Q and $\widehat{Q}$ is $\rho_{Q\widehat{Q}} = \rho_Q \otimes \rho_{\widehat{Q}}$.

Lemma 4. *Let A, B denote two quantum subsystems in the joint state ρ_{AB} where B has dimension $d = p^r$ with d being a power of a prime. Suppose B is subjected to a random operation $\mathsf{X}(\tilde{x})\mathsf{Z}(\tilde{z})$ with independent $\tilde{x}, \tilde{z}$ drawn uniformly in $\mathbb{F}_d$. Denote the joint state, the partial state of A, and the partial state of B after the random operation as ρ'_{AB}, ρ_A and ρ'_B, respectively. Then $\rho'_{AB} = \rho_A \otimes \rho'_B$ and $\rho'_B = \mathbf{I}_d/d$, where $\mathbf{I}_d$ denotes the $d \times d$ identity matrix.*

The argument in the lemma is standard in quantum literature [44], [32, Exercise 4.7.6 (Qudit Twirl)]. A proof is provided in Appendix B.

16

6   Proof of Theorem 1

6.1   Scheme with download cost tuple in $\mathfrak{D}_{\text{AME}}$

Let us design a scheme which allows Alice to compute $L = \lambda l$ instances of the sum $\sum_{k \in [K]} \mathsf{W}_k^{[L]} \in \mathbb{F}_d^{L \times 1}$. To do so, let the $S+1$ servers prepare $N = N_0 + N_1 + N_2 + \cdots + N_S$ q-dimensional quantum subsystems, $Q_0, Q_1, Q_2, \cdots Q_N$, with $q = d^\lambda$. For $s \in \mathcal{S} = \{0, 1, \cdots, S\}$, Server s possesses N_s of these quantum subsystems indexed by $\mathcal{I}_s \subseteq [N]$. Let $\mathbf{M} \in \mathbb{F}_q^{N \times 2N}$ be the transfer matrix of an N-sum box where $N = \sum_{s \in \mathcal{S}} N_s$. By definition, an element of $\mathbb{F}_q$ is equivalent to a λ-length vector in $\mathbb{F}_d$. Thus, let $\mathbf{W}_k \in \mathbb{F}_q^{l \times 1}$ denote $\mathsf{W}_k^{[L]}$ written in $\mathbb{F}_q$ for $k \in [K]$. Recall that Server s possesses the N_s q-dimensional quantum subsystems Q_i for $i \in \mathcal{I}_s$.

Define $x_i = 0, z_i = 0$, for all $i \in \mathcal{I}_0$, since the auxiliary server has no data inputs. Let Server $s \in \mathcal{S}$ apply the operation $\mathsf{X}(x_i)\mathsf{Z}(z_i)$ to Q_i for $i \in \mathcal{I}_s$. Suppose that each x_i, z_i is equal to the output of a linear function of the data available to the server. If the initial state of the composite system is $|\mathbf{0}\rangle_{\mathbf{M}}$, then after each server applies the operations, the output state can be written as

$$|\mathbf{M}[\begin{smallmatrix} \mathbf{x} \\ \mathbf{z} \end{smallmatrix}]\rangle_{\mathbf{M}} = \left| \sum_{k \in [K]} \mathbf{M}_k \mathbf{V}_k \mathbf{W}_k \right\rangle_{\mathbf{M}}, \tag{39}$$

where for $k \in [K]$, $\mathbf{V}_k$ is a $\sum_{s \in \mathcal{W}(k)} 2N_s \times l$ matrix with elements freely chosen in $\mathbb{F}_q$, and $\mathbf{M}_k$ is the submatrix composed of the columns of $\mathbf{M}$ 'controlled' by Servers $s \in \mathcal{W}(k)$. Specifically, for $k \in [K]$, $\mathbf{M}_k$ contains the ith and $(i + N)^{th}$ columns of $\mathbf{M}$ for $i \in \cup_{s \in \mathcal{W}(k)} \mathcal{I}_s$ and thus $\mathbf{M}_k$ has size $N \times \sum_{s \in \mathcal{W}(k)} 2N_s$. It is proved in [21] that if $q \geq N$, then there exists an $\mathbf{M}$ (as the transfer matrix of an N-sum box) such that $\text{rk}(\mathbf{M}_k) = \min\{N, \sum_{s \in \mathcal{W}(k)} 2N_s\}$ for all $k \in [K]$.

Recall that during the transmission, the quantum subsystems possessed by Servers $s \in \mathcal{E}(t)$ may be erased for any $t \in [T]$. To tolerate this erasure, let us find a matrix $\mathbf{U} \in \mathbb{F}_q^{N \times u}$ with $u = N - \max_{t \in [T]} \sum_{s \in \mathcal{E}(t)} 2N_s$ that has full column rank u. Here, we require that $N \geq \max_{t \in [T]} \sum_{s \in \mathcal{E}(t)} 2N_s$ for the scheme to work. Further, for $t \in [T]$, define $\mathbf{E}_t$ as the submatrix of $\mathbf{M}$ composed by the columns indexed by $i, i + N$ for $i \in \cup_{s \in \mathcal{E}(t)} \mathcal{I}_s$. We require that $[\mathbf{U}, \mathbf{E}_t]$ must have full rank $u + \sum_{s \in \mathcal{E}(t)} 2N_s$ for all $t \in [T]$. The existence of such a $\mathbf{U}$ is guaranteed if $q > TN$ (proof provided in Appendix C). In the following, let $\langle \mathbf{A} \rangle$ denote the linear subspace spanned by the columns of $\mathbf{A}$ with coefficients chosen in $\mathbb{F}_q$. For $k \in [K]$, denote $\mathbf{U}_k$ as a basis of the linear subspace spanned by the intersection of $\langle \mathbf{U} \rangle$ and $\langle \mathbf{M}_k \rangle$. Since $\langle \mathbf{U}_k \rangle \subseteq \langle \mathbf{M}_k \rangle$ for all $k \in [K]$, we can specify $\mathbf{V}_{[K]}$ such that the output state (39) of the composite quantum system becomes

$$\left| \sum_{k \in [K]} \mathbf{U}_k \mathbf{V}'_k \mathbf{W}_k \right\rangle_{\mathbf{M}}, \tag{40}$$

where $\mathbf{V}'_k \in \mathbb{F}_q^{\text{rk}(\mathbf{U}_k) \times l}$ has full column rank, equal to $\text{rk}(\mathbf{U}_k)$ if $l \leq \text{rk}(\mathbf{U}_k), \forall k \in [K]$. By the dimension law for linear subspaces,

$$\text{rk}(\mathbf{U}_k) = \text{rk}(\mathbf{U}) + \text{rk}(\mathbf{M}_k) - \text{rk}([\mathbf{U}, \mathbf{M}_k]) \tag{41}$$

$$\geq u + \min\{N, \sum_{s \in \mathcal{W}(k)} 2N_s\} - N \tag{42}$$

$$= \min\{N, \sum_{s \in \mathcal{W}(k)} 2N_s\} - \max_{t \in \mathcal{E}(t)} \sum_{s \in \mathcal{E}(t)} 2N_s \tag{43}$$

17

for all $k \in [K]$. After the servers apply the operations to their quantum subsystems, suppose in the transmission, the operations $\mathsf{X}(\tilde{x}_i)\mathsf{Z}(\tilde{z}_i)$ are applied to the ith quantum subsystem, with unknown $\tilde{x}_i, \tilde{z}_i$ for $i \in \cup_{s \in \mathcal{E}(t)}$. The state received by Alice becomes

$$\left| \sum_{k \in [K]} \mathbf{U}_k \mathbf{V}'_k \mathbf{W}_k + \mathbf{E}_t \begin{bmatrix} \tilde{x}_{i_1} \\ \vdots \\ \tilde{x}_{i_n} \\ \tilde{z}_{i_1} \\ \vdots \\ \tilde{z}_{i_n} \end{bmatrix} \right\rangle_{\mathbf{M}} \tag{44}$$

where $\{i_1, \cdots, i_n\} = \cup_{s \in \mathcal{E}(t)} \mathcal{I}_s$. Alice can now measure the result

$$Y = \sum_{k \in [K]} \mathbf{U}_k \mathbf{V}'_k \mathbf{W}_k + \mathbf{E}_t \begin{bmatrix} \tilde{x}_{i_1} \\ \vdots \\ \tilde{x}_{i_n} \\ \tilde{z}_{i_1} \\ \vdots \\ \tilde{z}_{i_n} \end{bmatrix} \tag{45}$$

with certainty given any $t \in [T]$. Since for any $t \in [T]$, $[\mathbf{U}, \mathbf{E}_t]$ has full column rank, and $\langle \mathbf{U}_k \rangle \subseteq \langle \mathbf{U} \rangle$ for all $k \in [K]$, Alice is then able to retrieve

$$\sum_{k \in [K]} \mathbf{U}_k \mathbf{V}'_k \mathbf{W}_k \in \mathbb{F}_q^{N \times 1} \tag{46}$$

and further compute

$$\mathbf{V}_{\mathrm{dec}} \sum_{k \in [K]} \mathbf{U}_k \mathbf{V}'_k \mathbf{W}_k = \sum_{k \in [K]} \mathbf{R}_k \mathbf{W}_k \in \mathbb{F}_q^{l \times 1} \tag{47}$$

where $\mathbf{R}_k$ is an $l \times l$ invertible square matrix for $k \in [K]$. The existence of the $\mathbf{V}_{\mathrm{dec}}$ is guaranteed if $q > Kl$ (proof provided in Appendix C). Since $\mathbf{R}_k$ is invertible for all $k \in [K]$, the servers can simply treat $\mathbf{W}_k$ as $\mathbf{R}^{-1} \mathbf{W}_k$ when coding so that Alice is able to compute the desired sum $\sum_{k \in [K]} \mathbf{W}_k$ in the end.

6.2 Extend the scheme to tolerate erasures

In the analysis of the scheme, we assumed that the quantum subsystems for Servers $s \in \mathcal{E}(t)$ are subjected to unknown X and Z operations during the transmission. If these quantum subsystems are lost during the transmission, a simple solution is to replace the lost quantum systems with ancillary quantum subsystems generated locally by Alice, which are independent of the quantum systems sent from the servers. The reasoning follows from Lemma 4. Thus, the scheme in Section 6.1 now tolerates erasures. Note that such a scheme exists if

$$\begin{cases} l \in \mathbb{N}, \\ \Delta_s = N_s/l, \forall s \in [S], \\ \min\{N, \sum_{s \in \mathcal{W}(k)} 2N_s\} - \max_{t \in \mathcal{E}(t)} \sum_{s \in \mathcal{E}(t)} 2N_s \geq l, \forall k, t \in [T]. \end{cases} \tag{48}$$

Then by definition,

$$\mathrm{closure} \left\{ \boldsymbol{\Delta} \in \mathbb{R}_+^S \;\middle|\; \begin{array}{l} l \in \mathbb{N}, \\ \Delta_s = N_s/l, \forall s \in [S], \\ \min\{N, \sum_{s \in \mathcal{W}(k)} 2N_s\} - \max_{t \in \mathcal{E}(t)} \sum_{s \in \mathcal{E}(t)} 2N_s \geq l, \forall k, t \in [T] \end{array} \right\} \subseteq \mathfrak{D}^*. \tag{49}$$

Note that the LHS of (49) is equal to $\mathfrak{D}_{\text{AME}}$. Therefore, $\mathfrak{D}_{\text{AME}} \subseteq \mathfrak{D}^*$. It then follows that $\mathfrak{D}_{\text{AME}}^+ \subseteq \mathfrak{D}^*$ as one can always send extra unentangled quantum resource.

6.3 Treating Qudits as Classical-dits (TQC)

Let us show that $\mathfrak{D}_{\text{TQC}} \subseteq \mathfrak{D}^*$. Suppose for $s \in \mathcal{S}$, Server s sends N_s q-dimensional quantum subsystems by treating them as classical q-ary symbols, where $q = d^\lambda$. Denote $N \triangleq N_0 + N_1 + \cdots + N_S$. During the transmission, the quantum subsystems (now regarded as classcial q-ary symbols) from servers $s \in \mathcal{E}(t)$ may be lost. Alice should be able to compute l instances of the sum, written in $\mathbb{F}_q$ as $\sum_{k \in [K]} \mathbf{W}_k$, where $\mathbf{W}_k \in \mathbb{F}_q^{l \times 1}$. Let us restate the result of [27] in the following lemma.

Lemma 5 (Restatement of [27]). *The classical scheme exists if $q > N$, and*

$$\max_{t \in [T]} \sum_{s \in \mathcal{E}(t)} N_s \leq \min_{k \in [K]} \sum_{s \in \mathcal{W}(k)} N_s - l. \tag{50}$$

Since $q > N$ can always be satisfied by choosing large enough λ, we have by definition,

$$\text{closure} \left\{ \boldsymbol{\Delta} \in \mathbb{R}_+^S \;\middle|\; \begin{array}{l} l \in \mathbb{N}, \\ \Delta_s = N_s/l, \forall s \in [S], \\ \max_{t \in [T]} \sum_{s \in \mathcal{E}(t)} N_s \leq \min_{k \in [K]} \sum_{s \in \mathcal{W}(k)} N_s - l \end{array} \right\} \subseteq \mathfrak{D}^*. \tag{51}$$

Note that the LHS of (51) is equal to $\mathfrak{D}_{\text{TQC}}$. Therefore, $\mathfrak{D}_{\text{TQC}} \subseteq \mathfrak{D}^*$. It then follows that $\mathfrak{D}_{\text{TQC}}^+ \subseteq \mathfrak{D}^*$ as one can always send extra unentangled quantum resource. Finally, by a time-sharing argument, any convex combination of the tuples in $\mathfrak{D}_{\text{AME}}^+ \cup \mathfrak{D}_{\text{TQC}}^+ \subseteq \mathfrak{D}^*$. This concludes the proof of Theorem 1. $\qquad\square$

7 Proof of Theorem 3

7.1 Achievability

Apply Theorem 1 to the Σ^s-QEMAC setting, with the cost tuple in the form $\boldsymbol{\Delta} = (\Delta_0, \Delta, \cdots, \Delta)$. From (6) we have $\boldsymbol{\Delta} \in \mathfrak{D}_{\text{AME}}$ if

$$\min\{\Delta_0 + S\Delta, 2\alpha\Delta\} - 2\beta\Delta \geq 1. \tag{52}$$

Similarly (7) implies that $\boldsymbol{\Delta} \in \mathfrak{D}_{\text{TQC}}$ if

$$(\alpha - \beta)\Delta \geq 1. \tag{53}$$

Consider two cases.

Case 1: $S \geq \alpha + \beta$. It follows from $\alpha > \beta$ that $S - 2\beta > 0$ and from (52) that for any $\Delta_0 \in \mathbb{R}_+$ and $\Delta = \max\{\frac{1}{2(\alpha-\beta)}, \frac{1-\Delta_0}{S-2\beta}\}$, we have $(\Delta_0, \Delta, \cdots, \Delta) \in \mathfrak{D}_{\text{AME}} \subseteq \mathfrak{D}^*$.

Case 2: $S < \alpha + \beta$. It follows from (52) that for $\left(\Delta_0 = \frac{2\alpha - S}{2(\alpha-\beta)}, \Delta = \frac{1}{2(\alpha-\beta)}\right)$ the cost tuple $(\Delta_0, \Delta, \cdots, \Delta) \in \mathfrak{D}_{\text{AME}}$. Also (53) implies that for $\left(\Delta_0 = 0, \Delta = \frac{1}{\alpha-\beta}\right)$ the cost tuple $(\Delta_0, \Delta, \cdots, \Delta) \in \mathfrak{D}_{\text{TQC}}$. It can be verified that the equation for the straight line connecting these two points is $\Delta = \frac{1}{\alpha-\beta} - \frac{\Delta_0}{2\alpha-S}$. It thus follows that for any $\Delta_0 \in \mathbb{R}_+$ and $\Delta = \max\{\frac{1}{2(\alpha-\beta)}, \frac{1}{\alpha-\beta} - \frac{\Delta_0}{2\alpha-S}\}$, we have $(\Delta_0, \Delta, \cdots, \Delta) \in \text{conv}(\mathfrak{D}_{\text{AME}}^+ \cup \mathfrak{D}_{\text{TQC}}^+) \subseteq \mathfrak{D}^*$.

Given $\Delta_0 \in \mathbb{R}_+$, by definition, $C(\Delta_0) \geq (S\Delta)^{-1}$ if $(\Delta_0, \Delta, \cdots, \Delta) \in \mathfrak{D}^*$. Thus, $C(\Delta_0) \geq (S\Delta^*)^{-1}$ with the Δ^* defined in (10). $\qquad\square$

7.2 Converse

Recall that the Σ^s-QEMAC contains $K = \binom{S}{\alpha}$ data streams and $S + 1$ servers. There are $T = \binom{S}{\beta}$ possible cases of erasure, each corresponding to a unique β subset of the answers from the S data-servers being erased. For any scheme with batch size L, since the decoding must be correct for all data realization $w = (w_1, w_2, \cdots, w_K) \in \mathbb{F}_d^{KL}$, it must be correct if the K data streams are uniformly distributed over $\mathbb{F}_d^{KL}$. Therefore, for the purpose of proving a converse, it will not hurt to assume that the data is uniformly distributed over $\mathbb{F}_d^{KL}$, and let $(\mathsf{W}_1, \mathsf{W}_2, \cdots, \mathsf{W}_K)$ denote these K random variables, one for each data stream. This facilitates entropic proofs. After the coding operations applied by the servers, the classical-quantum system of interest

$$\mathsf{W}_1 \cdots \mathsf{W}_K \mathcal{Q}_0 \mathcal{Q}_1 \cdots \mathcal{Q}_S$$

is in the state

$$\rho_{\mathsf{W}_1 \cdots \mathsf{W}_K \mathcal{Q}_0 \mathcal{Q}_1 \cdots \mathcal{Q}_S} = \sum_{w \in \mathbb{F}_d^{KL}} \frac{1}{d^{KL}} \rho_{\mathcal{Q}_0 \mathcal{Q}_1 \cdots \mathcal{Q}_S}^{(w)}. \tag{54}$$

Also recall that for the case of erasure indexed by $t \in [T]$, the measurement result is a random variable, denoted as Y_t such that

$$\mathsf{Pr}(Y_t = y \mid \mathsf{W}_{[K]} = w) = \mathsf{Tr}(\Lambda_t^{(y)} \rho_{\mathcal{Q}_0 \mathcal{Q}_{[S] \setminus \mathcal{E}(t)}}), \tag{55}$$

where $\{\Lambda_t^{(y)}\}_y$ is the set of POVM matrices associated with the measurement Ψ_t. The joint distribution of $\mathsf{W}_1 \cdots \mathsf{W}_K Y_t$ is thus determined. According to the definition (3), the scheme must have $\mathsf{Pr}\left(Y_t = \sum_{k \in [K]} \mathsf{W}_k\right) = 1$ for $t \in [T]$. For $s \in \mathcal{S} = \{0, 1, \cdots, S\}$, the dimension of $\mathcal{Q}_s$ is δ_s and due to symmetry there is no loss of generality in considering schemes with $\delta_1 = \delta_2 = \cdots = \delta_S = \delta$.

The proof proceeds as follows. We shall show that for any $\Delta_0 \in \mathbb{R}_+$, if $(\Delta_0, \Delta, \cdots, \Delta) \in \mathfrak{D}^*$, then

$$\Delta \geq \frac{1}{2(\alpha - \beta)} \tag{56}$$

and in addition,

$$\Delta \geq \frac{1 - \Delta_0}{S - 2\beta}, \quad \text{if } S \geq \alpha + \beta, \tag{57}$$

$$\Delta \geq \frac{1}{\alpha - \beta} - \frac{\Delta_0}{2\alpha - S}, \quad \text{if } S < \alpha + \beta. \tag{58}$$

First, consider any data stream (say W_1), and condition on any realization of $\mathsf{W}_{[K] \setminus \{1\}}$, the problem reduces to a communication problem with one data stream W_1, such that α servers (Servers $s \in \mathcal{W}(1)$) know the data stream, while the rest of the servers merely provide entanglement to Alice. Theorem 2 (Eq. (8)) then implies that $(\alpha - \beta)\Delta \geq 1/2 \implies \Delta \geq \frac{1}{2(\alpha - \beta)}$ (by substituting S by α).

Now, consider the following cases.

Case 1: $S \geq \alpha + \beta$. Partition $[S] = \{1, 2, \cdots, S\}$ such that

$$[S] = \underbrace{\{1, 2, \cdots, \beta\}}_{\mathcal{I}_1 \ (\beta)} \cup \underbrace{\{\beta + 1, \cdots, 2\beta\}}_{\mathcal{I}_2 \ (\beta)} \cup \underbrace{\{2\beta + 1, \cdots, \alpha + \beta\}}_{\mathcal{I}_3 \ (\alpha - \beta)} \cup \underbrace{\{\alpha + \beta + 1, \cdots, S\}}_{\mathcal{I}_4 \ (S - \alpha - \beta)}. \tag{59}$$

Identify indices k_1, k_2, t_1, t_2 such that

$$\mathcal{W}(k_1) = \underbrace{\mathcal{I}_1 \cup \mathcal{I}_3}_{(\alpha)}, \tag{60}$$

$$\mathcal{W}(k_2) = \underbrace{\mathcal{I}_2 \cup \mathcal{I}_3}_{(\alpha)}, \tag{61}$$

$$\mathcal{E}(t_1) = \underbrace{\mathcal{I}_1}_{(\beta)}, \tag{62}$$

$$\mathcal{E}(t_2) = \underbrace{\mathcal{I}_2}_{(\beta)}. \tag{63}$$

For the case of erasure indexed by t_1, i.e., when $\mathcal{Q}_{\mathcal{I}_1}$ is erased, we have

$$L = I\left(\mathsf{W}_{[K]}; \sum_{k \in [K]} \mathsf{W}_k \mid \mathsf{W}_{[K] \setminus \{k_1\}}\right) \tag{64}$$

$$\leq I\left(\mathsf{W}_{[K]}; Y_{t_1} \mid \mathsf{W}_{[K] \setminus \{k_1\}}\right) \tag{65}$$

$$\leq I\left(\mathsf{W}_{k_1}; \mathcal{Q}_0 \mathcal{Q}_{\mathcal{I}_2} \mathcal{Q}_{\mathcal{I}_3} \mathcal{Q}_{\mathcal{I}_4} \mid \mathsf{W}_{[K] \setminus \{k_1\}}\right)_{\rho_{\mathsf{W}_1 \cdots \mathsf{W}_K \mathcal{Q}_0 \mathcal{Q}_1 \cdots \mathcal{Q}_S}} \tag{66}$$

$$= \underbrace{I\left(\mathsf{W}_{k_1}; \mathcal{Q}_{\mathcal{I}_2} \mid \mathsf{W}_{[K] \setminus \{k_1\}}\right)}_{=0} + I\left(\mathsf{W}_{k_1}; \mathcal{Q}_0 \mathcal{Q}_{\mathcal{I}_3} \mathcal{Q}_{\mathcal{I}_4} \mid \mathcal{Q}_{\mathcal{I}_2}, \mathsf{W}_{[K] \setminus \{k_1\}}\right) \tag{67}$$

$$= I\left(\mathsf{W}_{k_1}; \mathcal{Q}_0 \mathcal{Q}_{\mathcal{I}_3} \mathcal{Q}_{\mathcal{I}_4} \mid \mathcal{Q}_{\mathcal{I}_2}, \mathsf{W}_{[K] \setminus \{k_1\}}\right) \tag{68}$$

$$= H\left(\mathcal{Q}_0 \mathcal{Q}_{\mathcal{I}_3} \mathcal{Q}_{\mathcal{I}_4} \mid \mathcal{Q}_{\mathcal{I}_2}, \mathsf{W}_{[K] \setminus \{k_1\}}\right) - H\left(\mathcal{Q}_0 \mathcal{Q}_{\mathcal{I}_3} \mathcal{Q}_{\mathcal{I}_4} \mid \mathcal{Q}_{\mathcal{I}_2}, \mathsf{W}_{[K]}\right) \tag{69}$$

$$\leq H(\mathcal{Q}_0 \mathcal{Q}_{\mathcal{I}_3} \mathcal{Q}_{\mathcal{I}_4}) - H\left(\mathcal{Q}_0 \mathcal{Q}_{\mathcal{I}_3} \mathcal{Q}_{\mathcal{I}_4} \mid \mathcal{Q}_{\mathcal{I}_2}, \mathsf{W}_{[K]}\right) \tag{70}$$

$$\leq \log_d \delta_0 + (S - 2\beta) \log_d \delta - H\left(\mathcal{Q}_0 \mathcal{Q}_{\mathcal{I}_3} \mathcal{Q}_{\mathcal{I}_4} \mid \mathcal{Q}_{\mathcal{I}_2}, \mathsf{W}_{[K]}\right) \tag{71}$$

Information measures on and after Step (66) are with respect to the state $\rho_{\mathsf{W}_1 \cdots \mathsf{W}_K \mathcal{Q}_0 \mathcal{Q}_1 \cdots \mathcal{Q}_S}$.
Step (66) is by Lemma 2 since Alice obtains Y_{t_1} conditioned on any realization of $\mathsf{W}_{[K] \setminus \{k_1\}}$
by measuring $\mathcal{Q}_0 \mathcal{Q}_{\mathcal{I}_2} \mathcal{Q}_{\mathcal{I}_3} \mathcal{Q}_{\mathcal{I}_4}$. Step (68) is by Lemma 1 conditioned on any realization of
$\mathsf{W}_{[K] \setminus \{k_1\}}$, since W_{k_1} is not available to any server in $\mathcal{I}_2$. Step (71) is because conditioning
does not increase entropy [32, Thm. 11.4.1].

For the case of erasure indexed by t_2, by the same reasoning, we similarly have ($\mathcal{I}_2$ replaced
by $\mathcal{I}_1$),

$$L \leq \log_d \delta_0 + (S - 2\beta) \log_d \delta - H\left(\mathcal{Q}_0 \mathcal{Q}_{\mathcal{I}_3} \mathcal{Q}_{\mathcal{I}_4} \mid \mathcal{Q}_{\mathcal{I}_1}, \mathsf{W}_{[K]}\right). \tag{72}$$

Adding (71) and (72), we have

$$2L \leq 2\left(\log_d \delta_0 + (S - 2\beta) \log_d \delta\right)$$
$$- \underbrace{\left(H\left(\mathcal{Q}_0 \mathcal{Q}_{\mathcal{I}_3} \mathcal{Q}_{\mathcal{I}_4} \mid \mathcal{Q}_{\mathcal{I}_2}, \mathsf{W}_{[K]}\right) + H\left(\mathcal{Q}_0 \mathcal{Q}_{\mathcal{I}_3} \mathcal{Q}_{\mathcal{I}_4} \mid \mathcal{Q}_{\mathcal{I}_1}, \mathsf{W}_{[K]}\right)\right)}_{\geq 0} \tag{73}$$

21

$$\leq 2\big(\log_d \delta_0 + (S - 2\beta)\log_d \delta\big) \tag{74}$$

$$\implies \Delta_0 + (S - 2\beta)\Delta \geq 1 \tag{75}$$

$$\implies \Delta \geq \frac{1 - \Delta_0}{S - 2\beta}. \tag{76}$$

Step (74) follows from weak monotonicity[4] [39,43] conditioned on $\mathsf{W}_{[K]} = w$ for any $w \in \mathbb{F}_d^{KL}$. Step (75) is by dividing by $2L$ on both sides and using the definition $\Delta_0 = \log_d \delta_0/L$, $\Delta = \log_d \delta/L$.

Case 2: $S < \alpha + \beta$. The idea is similar but the proof requires a few more steps. Partition $[S]$ such that,

$$[S] = \underbrace{\{1, 2, \cdots, 2\alpha - S\}}_{\mathcal{I}_1 \ (2\alpha - S)} \cup \underbrace{\{2\alpha - S, \cdots, \alpha\}}_{\mathcal{I}_2 \ (S - \alpha)} \cup \underbrace{\{\alpha + 1, \cdots, S\}}_{\mathcal{I}_3 \ (S - \alpha)}. \tag{77}$$

Note that since $S < \alpha + \beta$, we have $2\alpha - S > \alpha - \beta$. Let $\mathcal{J} \in \binom{[2\alpha - S]}{\alpha - \beta}$ be any subset of $\mathcal{I}_1$ with cardinality equal to $\alpha - \beta$. Identify indices k, t such that

$$\mathcal{W}(k) = \underbrace{\mathcal{I}_1 \cup \mathcal{I}_3}_{(\alpha)}, \tag{78}$$

$$\mathcal{E}(t) = \underbrace{(\mathcal{I}_1 \setminus \mathcal{J}) \cup \mathcal{I}_3}_{(\beta)}. \tag{79}$$

We have

$$L = I\big(\mathsf{W}_{[K]}; \sum_{k \in [K]} \mathsf{W}_k \mid \mathsf{W}_{[K]\setminus\{k\}}\big) \tag{80}$$

$$\leq I\big(\mathsf{W}_{[K]}; Y_t \mid \mathsf{W}_{[K]\setminus\{k\}}\big) \tag{81}$$

$$\leq I\big(\mathsf{W}_k; \mathcal{Q}_0 \mathcal{Q}_{\mathcal{J}} \mathcal{Q}_{\mathcal{I}_2} \mid \mathsf{W}_{[K]\setminus\{k\}}\big)_{\rho_{\mathsf{W}_1 \cdots \mathsf{W}_K \mathcal{Q}_0 \mathcal{Q}_1 \cdots \mathcal{Q}_S}} \tag{82}$$

$$= \underbrace{I\big(\mathsf{W}_k; \mathcal{Q}_0 \mathcal{Q}_{\mathcal{I}_2} \mid \mathsf{W}_{[K]\setminus\{k\}}\big)}_{=0} + I\big(\mathsf{W}_k; \mathcal{Q}_{\mathcal{J}} \mid \mathcal{Q}_0 \mathcal{Q}_{\mathcal{I}_2}, \mathsf{W}_{[K]\setminus\{k\}}\big) \tag{83}$$

$$= I\big(\mathsf{W}_k; \mathcal{Q}_{\mathcal{J}} \mid \mathcal{Q}_0 \mathcal{Q}_{\mathcal{I}_2}, \mathsf{W}_{[K]\setminus\{k\}}\big) \tag{84}$$

$$\leq H(\mathcal{Q}_{\mathcal{J}}) - H(\mathcal{Q}_{\mathcal{J}} \mid \mathcal{Q}_0 \mathcal{Q}_{\mathcal{J}_2}, \mathsf{W}_{[K]}) \tag{85}$$

$$\leq (\alpha - \beta)\log_d \delta - H(\mathcal{Q}_{\mathcal{J}} \mid \mathcal{Q}_0 \mathcal{Q}_{\mathcal{J}_2}, \mathsf{W}_{[K]}) \tag{86}$$

Information measures on and after Step (82) are with respect to the state $\rho_{\mathsf{W}_1 \cdots \mathsf{W}_K \mathcal{Q}_0 \mathcal{Q}_1 \cdots \mathcal{Q}_S}$. Step (82) is by Lemma 2 since Alice obtains Y_t conditioned on any realization of $\mathsf{W}_{[K]\setminus\{k\}}$ by measuring $\mathcal{Q}_0 \mathcal{Q}_{\mathcal{J}} \mathcal{Q}_{\mathcal{I}_2}$. Step (84) is by Lemma 1 conditioned on any realization of $\mathsf{W}_{[K]\setminus\{k\}}$, since W_k is not available to any server in $\{0\} \cup \mathcal{I}_2$. Step (85) is because conditioning does not increase entropy.

By symmetry, (86) holds for any $\mathcal{J} \in \binom{[2\alpha - S]}{\alpha - \beta}$. Taking the sum over all $\mathcal{J} \in \binom{[2\alpha - S]}{\alpha - \beta}$ (in total $\binom{2\alpha - S}{\alpha - \beta}$ terms), we have

$$\binom{2\alpha - S}{\alpha - \beta} L \leq \binom{2\alpha - S}{\alpha - \beta}(\alpha - \beta)\log_d \delta - \sum_{\mathcal{J}} H(\mathcal{Q}_{\mathcal{J}} \mid \mathcal{Q}_0 \mathcal{Q}_{\mathcal{I}_2}, \mathsf{W}_{[K]}) \tag{87}$$

---

[4]For a tripartite quantum system ABC in the state ρ, $H(A|B)_\rho + H(A|C)_\rho \geq 0$.

$$\leq \binom{2\alpha - S}{\alpha - \beta}(\alpha - \beta)\log_d \delta - \binom{2\alpha - S - 1}{\alpha - \beta - 1}H(\mathcal{Q}_{[2\alpha - S]} \mid \mathcal{Q}_0\mathcal{Q}_{\mathcal{I}_2}, \mathsf{W}_{[K]}) \quad (88)$$

$$\implies L \leq (\alpha - \beta)\log_d \delta - \frac{\alpha - \beta}{2\alpha - S}H(\mathcal{Q}_{[2\alpha - S]} \mid \mathcal{Q}_0\mathcal{Q}_{\mathcal{I}_2}, \mathsf{W}_{[K]}) \quad (89)$$

$$= (\alpha - \beta)\log_d \delta - \frac{\alpha - \beta}{2\alpha - S}H(\mathcal{Q}_{[2\alpha - S]}\mathcal{Q}_0 \mid \mathcal{Q}_{\mathcal{I}_2}, \mathsf{W}_{[K]}) + \frac{\alpha - \beta}{2\alpha - S}H(\mathcal{Q}_0 \mid \mathcal{Q}_{\mathcal{I}_2}, \mathsf{W}_{[K]}) \quad (90)$$

Step (88) follows from [30, Lemma 3] (which may be viewed as the quantum conditional version of Han's inequality). By similar reasoning, we have ($\mathcal{I}_2$ replaced by $\mathcal{I}_3$),

$$L \leq (\alpha - \beta)\log_d \delta - \frac{\alpha - \beta}{2\alpha - S}H(\mathcal{Q}_{[2\alpha - S]}\mathcal{Q}_0 \mid \mathcal{Q}_{\mathcal{I}_3}, \mathsf{W}_{[K]}) + \frac{\alpha - \beta}{2\alpha - S}H(\mathcal{Q}_0 \mid \mathcal{Q}_{\mathcal{I}_3}, \mathsf{W}_{[K]}). \quad (91)$$

Adding (90) and (91), and noting that,

$$H(\mathcal{Q}_{[2\alpha - S]}\mathcal{Q}_0 \mid \mathcal{Q}_{\mathcal{I}_2}, \mathsf{W}_{[K]}) + H(\mathcal{Q}_{[2\alpha - S]}\mathcal{Q}_0 \mid \mathcal{Q}_{\mathcal{I}_3}, \mathsf{W}_{[K]}) \geq 0, \quad (92)$$

because of weak monotonicity conditioned on $\mathsf{W}_{[K]} = w$ for any $w \in \mathbb{F}_d^{KL}$, we have

$$2L \leq 2(\alpha - \beta)\log_d \delta + \frac{2(\alpha - \beta)}{2\alpha - S}\log_d \delta_0 \quad (93)$$

$$\implies 1 \leq (\alpha - \beta)\Delta + \frac{\alpha - \beta}{2\alpha - S}\Delta_0 \quad (94)$$

$$\implies \Delta \geq \frac{1}{\alpha - \beta} - \frac{\Delta_0}{2\alpha - S} \quad (95)$$

In Step (94) we divide both sides by $2L$ and apply the definitions $\Delta_0 = \log_d \delta_0/L, \Delta = \log_d \delta/L$.

This concludes the proof of the converse. $\qquad\square$

8 Conclusion

Generalizing the Σ-QMAC model to Σ-QEMAC, which allows erasures, we construct a coding scheme to show that the communication efficiency gains that are enabled by quantum multiparty entanglement are not dominated in general by the higher cost of quantum erasure correction. The advantage provided by quantum entanglement is evident, e.g., from Corollaries 1 and 2. For the symmetric setting we also show by quantum entropic analysis that the proposed coding scheme, in combination with the simple idea of treating qudits as classical dits, is exactly optimal in communication efficiency for the Σ^s-QEMAC, for any given level of prior entanglement between the data-servers and the receiver. In other words, we characterize the precise capacity of the Σ^s-QEMAC for arbitrary levels of receiver entanglement. A natural next step would be to find the capacity of the asymmetric Σ-QEMAC. Additional insights are needed to overcome the combinatorial complexity of asymmetric settings. This is left as an open problem for future work.

A Proof of achievability of $\Delta = 3/4$

Let us first formulate the problem. The reduced communication problem contains 3 servers, referred to as Server 1, Server 2 and Server 3. The answer from one of them can get erased. The data stream A is only known to Server 1 and Server 2. The receiver must be able to recover A. Now, let us prove that $\Delta = 3/4$ is achievable for the communication problem reduced from the "A cut" from Section 5. Let $[A_1, A_2, A_3, A_4]$ be symbols from $\mathbb{F}_{d^z}$ that constitute $4z$ instances of the data stream A. Let

$$\begin{bmatrix} A_1' & A_2' & \cdots & A_8' \end{bmatrix} = \begin{bmatrix} A_1 & A_2 & A_3 & A_4 \end{bmatrix} \mathbf{M}^{4 \times 8} \tag{96}$$

where $\mathbf{M} \in \mathbb{F}_{d^z}^{4 \times 8}$ is the generator matrix of a $(k = 4, n = 8)$ MDS linear code defined in $\mathbb{F}_{d^z}$. z is allowed to be chosen freely to allow the existence of $\mathbf{M}$. Let $Q_1, Q_2, \cdots, Q_8$ be d^z-dimensional quantum systems, distributed to Server 1, Server 2 and Server 3 such that

1. Server 1 has Q_1, Q_2, Q_3;

2. Server 2 has Q_4, Q_5, Q_6;

3. Server 3 has Q_7, Q_8.

Let (Q_1, Q_7) and (Q_4, Q_8) be initially prepared in the entangled state for superdense coding. Recall that only Server 1 and Server 2 know $(A_1', \cdots, A_8')$. Server 1 and Server 2 perform the encoding operations as follows.

1. Server 1 encodes (A_1', A_2') into Q_1 using superdense coding, and encodes A_3' into Q_2, A_4' into Q_3 classically.

2. Server 2 encodes (A_5', A_6') into Q_4 using superdense coding, and encodes A_7' into Q_5, A_8' into Q_6 classically.

Depending on different cases of erasure, the receiver applies one of the following decoding options.

1. In the case that the answer from Server 1 gets erased (this also ruins Q_7), Alice is able to measure Q_4, Q_5, Q_6, Q_8 to obtain (A_5', A_6', A_7', A_8') and recover (A_1, A_2, A_3, A_4) by the property of the MDS code.

2. In the case that the answer from Server 2 gets erased (this also ruins Q_8), Alice is able to measure Q_1, Q_2, Q_3, Q_7 to obtain (A_1', A_2', A_3', A_4') and recover (A_1, A_2, A_3, A_4) by the property of the MDS code..

3. In the case that the answer from Server 3 gets erased (this also ruins Q_1, Q_4), Alice is able to measure (Q_2, Q_3, Q_5, Q_6) to obtain (A_3', A_4', A_7', A_8') and recover (A_1, A_2, A_3, A_4) by the property of the MDS code..

Therefore, Alice gets $4z$ instances of the data stream A by downloading at most $3z$ qudits from each of the servers. We thus conclude that $\Delta = 3/4$ is achievable for the communication problem.

B Proof of Lemma 4

Let $\mathcal{H}_A, \mathcal{H}_B$ denote the Hilbert spaces related to System A and System B. It suffices to prove for pure state $\rho_{AB} = |\psi\rangle_{AB} \langle\psi|_{AB}$. Let us first show the case for $d = p$ being a prime. Without loss of generality, we write

$$|\psi\rangle_{AB} = \sum_{i=0}^{p-1} |\phi_i\rangle_A |i\rangle_B \tag{97}$$

for a set of vectors $\{|\psi_i\rangle_A\}_{i=1}^{p-1}$ defined in $\mathcal{H}_A$, and $\{|i\rangle_B\}_{i=0}^{p-1}$ is the computational basis for $\mathcal{H}_B$.

After the random $\mathsf{X}(\tilde{x})\mathsf{Z}(\tilde{z})$ operation is applied to System B, the state becomes a mixed state with density operator

$$\rho'_{AB} = \frac{1}{p^2} \sum_{\tilde{x}=0}^{p-1} \sum_{\tilde{z}=0}^{p-1} \underbrace{\left(\mathbf{I} \otimes \mathsf{X}(\tilde{x})\mathsf{Z}(\tilde{z})\right)}_{U_{\tilde{x}\tilde{z}}} |\psi\rangle_{AB} \langle\psi|_{AB} U_{\tilde{x}\tilde{z}}^\dagger. \tag{98}$$

By (97),

$$U_{\tilde{x}\tilde{z}} |\phi\rangle_{AB} \langle\phi|_{AB} U_{\tilde{x}\tilde{z}}^\dagger$$
$$= \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} \omega^{\tilde{z}(i-j)} |\phi_i\rangle_A \langle\phi_j|_A |i+\tilde{x}\rangle_B \langle j+\tilde{x}|_B. \tag{99}$$

Therefore, (98) is equal to (the subscripts A, B are omitted for simplicity)

$$\frac{1}{p^2} \sum_{\tilde{x}=0}^{p-1} \sum_{\tilde{z}=0}^{p-1} \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} \omega^{\tilde{z}(i-j)} |\phi_i\rangle \langle\phi_j| |i+\tilde{x}\rangle \langle j+\tilde{x}| \tag{100}$$

$$= \frac{1}{p^2} \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} |\phi_i\rangle \langle\phi_j| \sum_{\tilde{x}=0}^{p-1} \sum_{\tilde{z}=0}^{p-1} \omega^{\tilde{z}(i-j)} |i+\tilde{x}\rangle \langle j+\tilde{x}| \tag{101}$$

$$= \frac{1}{p^2} \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} |\phi_i\rangle \langle\phi_j| \underbrace{\sum_{\tilde{z}=0}^{p-1} \omega^{\tilde{z}(i-j)}}_{p\delta(i-j)} \sum_{\tilde{x}=0}^{p-1} |\tilde{x}\rangle \langle\tilde{x}| \tag{102}$$

$$= \frac{1}{p} \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} |\phi_i\rangle \langle\phi_j| \mathbf{I}_p \delta(i-j) \tag{103}$$

$$= \left(\sum_{i=0}^{p-1} |\phi_i\rangle \langle\phi_i| \right) \otimes \left(\frac{\mathbf{I}_p}{p} \right) \tag{104}$$

where $\delta(x) \triangleq 1$ if $x = 0$ and $\delta(x) \triangleq 0$ otherwise.

This shows that B is independent of A and is in the maximally mixed state. To generalize the argument to general $d = p^r$, it is important to note that applying a random $\mathsf{X}(\tilde{x})\mathsf{Z}(\tilde{z})$ operation to a qudit is equivalent to applying a random $\mathsf{X}(\tilde{x}_i)\mathsf{Z}(\tilde{x}_i)$ operation to the ith p-dimensional subsystem for all $i \in [r]$, where $\tilde{x}_i, \tilde{z}_i \in \mathbb{F}_p$. Therefore, the argument generalizes to $d = p^r$.

C Proofs of claims in Section 6

C.1 The existence of U

Recall that we are given $\mathbf{E}_t \in \mathbb{F}_q^{N \times \sum_{s \in \mathcal{E}(t)} 2N_s}$ that has full column rank for $t \in [T]$. We will prove the existence of the matrix $\mathbf{U} \in \mathbb{F}_q^{N \times u}$, where $u = N - \max_{t \in [T]} \sum_{s \in \mathcal{E}(t)} N_s$, such that $[\mathbf{U}, \mathbf{E}_t]$ has full column rank for all $t \in [T]$. For $t \in [T]$, there exists a realization of $\mathbf{U} \in \mathbb{F}_q^{N \times u}$ and a deterministic matrix $\mathbf{Z}_t \in \mathbb{F}_q^{N \times (N - u - \sum_{s \in \mathcal{E}(t)} 2N_s)}$ such that $[\mathbf{U}, \mathbf{E}_t, \mathbf{Z}_t]$ is invertible. Therefore, $P_t \triangleq \det([\mathbf{U}, \mathbf{E}_t, \mathbf{Z}_t])$ is a non-zero polynomial in the elements of $\mathbf{U}$, with degree more than N for all $t \in [T]$. Consider the polynomial $P = \prod_{t=1}^{T} P_t$, which is a non-zero polynomial with degree not more than TN. By Schwartz-Zippel Lemma, if the element of $\mathbf{U}$ is chosen i.i.d. uniformly in $\mathbb{F}_q$, then the probability of P evaluating to 0 is not more than $\frac{TN}{q}$, which is strictly less than 1 if $q > TN$. Therefore, if $q > TN$, there exists $\mathbf{U}$ such that $[\mathbf{U}, \mathbf{E}_t]$ has full column rank for all $t \in [T]$.

C.2 The existence of $\mathbf{V}_{\text{dec}}$

Recall that we are given $\mathbf{U}_k \in \mathbb{F}_q^{N \times \text{rk}(\mathbf{U}_k)}$, $\mathbf{V}_k' \in \mathbb{F}_q^{\text{rk}(\mathbf{U}_k) \times l}$ that has full column rank for $k \in [K]$. We will prove the existence of the matrix $\mathbf{V}_{\text{dec}} \in \mathbb{F}_q^{l \times N}$ such that $\mathbf{V}_{\text{dec}} \mathbf{U}_k \mathbf{V}_k'$ is an $l \times l$ invertible matrix $\mathbf{R}_k$ for all $k \in [K]$. The proof is as follows. By definition, there exists a realization of $\mathbf{V}_{\text{dec}} \in \mathbb{F}_q^{l \times N}$ such that $\mathbf{V}_{\text{dec}} \mathbf{U}_k \mathbf{V}_k'$ is invertible. Therefore, $P_k \triangleq \det(\mathbf{V}_{\text{dec}} \mathbf{U}_k \mathbf{V}_k')$ is a non-zero polynomial in the elements of $\mathbf{V}_{\text{dec}}$, with degree not more than l for all $k \in [K]$. Consider the polynomial $P = \prod_{k=1}^{K} P_K$, which is a non-zero polynomial with degree not more than Kl. By Schwartz-Zippel Lemma, if the element of $\mathbf{V}_{\text{dec}}$ is chosen i.i.d. uniformly in $\mathbb{F}_q$, then the probability of P evaluating to 0 is not more than $\frac{Kl}{q}$, which is strictly less than 1 if $q > Kl$. Therefore, if $q > Kl$, there exists $\mathbf{V}_{\text{dec}}$ such that $\mathbf{V}_{\text{dec}} \mathbf{U}_k \mathbf{V}_k'$ is invertible for all $k \in [K]$.

D Proof of Theorem 2

We continue to use the notations as defined in Section 7.2. After the coding operations done by the servers, the classical-quantum system of interest $\mathsf{W}\mathcal{Q}_0\mathcal{Q}_1 \cdots \mathcal{Q}_S$ is in the state,

$$\rho_{\mathsf{W}\mathcal{Q}_0\mathcal{Q}_1 \cdots \mathcal{Q}_S} = \sum_{w \in \mathbb{F}_d^L} \frac{1}{d^L} \rho_{\mathcal{Q}_0\mathcal{Q}_1 \cdots \mathcal{Q}_S}^{(w)}. \tag{105}$$

For $t \in [T]$, Alice measures $\mathcal{Q}_0\mathcal{Q}_{[S] \setminus \mathcal{E}(t)}$ to obtain Y_t such that $\Pr(Y_t = \mathsf{W}) = 1$. Recall that in this theorem $\{\mathcal{E}(1), \mathcal{E}(2), \cdots, \mathcal{E}(T)\}$ constitute the collection of all cardinality-β subsets of $\{1, 2, \cdots, S\}$. Denote $\mathcal{I}_t \triangleq [S] \setminus \mathcal{E}(t)$. We have, for all $t \in [T]$,

$$L = H(\mathsf{W}) = I(\mathsf{W}; Y_t) \tag{106}$$

$$\leq I(\mathsf{W}; \mathcal{Q}_0 \mathcal{Q}_{\mathcal{I}_t})_{\rho_{\mathsf{W}\mathcal{Q}_0\mathcal{Q}_1 \cdots \mathcal{Q}_S}} \tag{107}$$

$$= \underbrace{I(\mathsf{W}; \mathcal{Q}_0)}_{=0} + I(\mathsf{W}; \mathcal{Q}_{\mathcal{I}_t} \mid \mathcal{Q}_0) \tag{108}$$

$$= I(\mathsf{W}; \mathcal{Q}_{\mathcal{I}_t} \mid \mathcal{Q}_0) \tag{109}$$

$$= H(\mathcal{Q}_{\mathcal{I}_t} \mid \mathcal{Q}_0) - H(\mathcal{Q}_{\mathcal{I}_t} \mid \mathcal{Q}_0, \mathsf{W}) \tag{110}$$

$$\leq H(\mathcal{Q}_{\mathcal{I}_t}) - H(\mathcal{Q}_{\mathcal{I}_t} \mid \mathcal{Q}_0, \mathsf{W}) \tag{111}$$

$$\leq H(\mathcal{Q}_{\mathcal{I}_t}) + H(\mathcal{Q}_{\mathcal{I}_t}) \tag{112}$$

$$\leq 2 \log_d \sum_{s \in \mathcal{I}_t} \delta_s \tag{113}$$

$$\implies \sum_{s \in \mathcal{I}} \Delta_s \geq 1/2, \quad \forall \mathcal{I} \in \binom{[S]}{S-\beta} \tag{114}$$

Information measures on and after Step (107) are with respect to the state $\rho_{\mathsf{W}\mathcal{Q}_0\mathcal{Q}_1\cdots\mathcal{Q}_S}$. Step (107) is by Holevo bound (Lemma 2). Step (108) is by Lemma 1 since Server 0 does not know W. Step (111) is because conditioning does not increase entropy. (112) is from the Ariki-Lieb triangle inequality[5]. This proves (8). We next show (9). From (111), we have,

$$L \leq H(\mathcal{Q}_{\mathcal{I}}) - H(\mathcal{Q}_{\mathcal{I}} \mid \mathcal{Q}_0, \mathsf{W}), \quad \forall \mathcal{I} \in \binom{[S]}{S-\beta}. \tag{115}$$

Taking the sum over all $\mathcal{I} \in \binom{[S]}{S-\beta}$ (in total $\binom{S}{\beta}$ terms), we have

$$\binom{S}{\beta} L \leq \sum_{\mathcal{I} \in \binom{[S]}{S-\beta}} H(\mathcal{Q}_{\mathcal{I}}) - \sum_{\mathcal{I} \in \binom{[S]}{S-\beta}} H(\mathcal{Q}_{\mathcal{I}} \mid \mathcal{Q}_0, \mathsf{W}) \tag{116}$$

$$\leq \binom{S-1}{\beta} \sum_{s \in [S]} \log_d \delta_s - \sum_{\mathcal{I} \in \binom{[S]}{S-\beta}} H(\mathcal{Q}_{\mathcal{I}} \mid \mathcal{Q}_0, \mathsf{W}) \tag{117}$$

$$\leq \binom{S-1}{\beta} \sum_{s \in [S]} \log_d \delta_s - \binom{S-1}{\beta} H(\mathcal{Q}_{[S]} \mid \mathcal{Q}_0, \mathsf{W}) \tag{118}$$

$$\leq \binom{S-1}{\beta} \sum_{s \in [S]} \log_d \delta_s + \binom{S-1}{\beta} H(\mathcal{Q}_0) \tag{119}$$

$$\leq \binom{S-1}{\beta} \Big(\sum_{s \in [S]} \Delta_s + \Delta_0 \Big) \tag{120}$$

$$\implies \Delta_0 + \Delta_1 + \cdots + \Delta_S \geq \frac{S}{S-\beta} \tag{121}$$

Step (118) follows from [30, Lemma 3]. Step (119) is due to non-negativity of entropy and the fact that conditioning does not increase entropy. This concludes the proof of Theorem 2.

References

[1] E. Schrodinger, "Discussion of probability relations between separated systems," *Proceedings of the Cambridge Philosophical Society*, p. 31: 555–563; 32 (1936): 446–451, 1936.

[2] J. Korner and K. Marton, "How to encode the modulo-two sum of binary sources (corresp.)," *IEEE Transactions on Information Theory*, vol. 25, no. 2, pp. 219–221, 1979.

[3] B. K. Rai and B. K. Dey, "On network coding for sum-networks," *IEEE Transactions on Information Theory*, vol. 58, no. 1, pp. 50–63, 2012.

---

[5]For a bipartite quantum system AB in the state ρ, $|H(A)_\rho - H(B)_\rho| \leq H(AB)_\rho$.

[4] A. Ramamoorthy and M. Langberg, "Communicating the sum of sources over a network," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 4, pp. 655–665, 2013.

[5] R. Appuswamy, M. Franceschetti, N. Karamchandani, and K. Zeger, "Network coding for computing: Cut-set bounds," *IEEE Transactions on Information Theory*, vol. 57, no. 2, pp. 1015–1030, Feb. 2011.

[6] H. Kowshik and P. R. Kumar, "Optimal function computation in directed and undirected graphs," *IEEE Transactions on Information Theory*, vol. 58, no. 6, pp. 3407–3418, 2012.

[7] X. Guang, Y. Bai, and R. W. Yeung, "Secure network function computation for linear functions – part i: Source security," 2022.

[8] X. Guang, R. W. Yeung, S. Yang, and C. Li, "Improved upper bound on the network function computing capacity," *IEEE Transactions on Information Theory*, vol. 65, no. 6, pp. 3790–3811, Jun. 2019.

[9] A. Şahin and R. Yang, "A survey on over-the-air computation," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 3, pp. 1877–1908, 2023.

[10] V. Giovannetti, S. Lloyd, and L. Maccone, "Quantum-enhanced measurements: Beating the standard quantum limit," *Science*, vol. 306, no. 5700, pp. 1330–1336, 2004. [Online]. Available: https://www.science.org/doi/abs/10.1126/science.1104149

[11] T. J. Proctor, P. A. Knott, and J. A. Dunningham, "Multiparameter estimation in networked quantum sensors," *Phys. Rev. Lett.*, vol. 120, p. 080501, Feb 2018. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.120.080501

[12] Y. Cao and X. Wu, "Distributed quantum sensing network with geographically constrained measurement strategies," in *Proc. 2023 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2023, pp. 1–5. [Online]. Available: https://api.semanticscholar.org/CorpusID:258532409

[13] Z. Ren, W. Li, A. Smerzi, and M. Gessner, "Metrological detection of multipartite entanglement from young diagrams," *Phys. Rev. Lett.*, vol. 126, p. 080502, Feb 2021. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.126.080502

[14] H. Buhrman, R. Cleve, and A. Wigderson, "Quantum vs. classical communication and computation," in *Proceedings of the thirtieth annual ACM symposium on Theory of computing*, 1998, pp. 63–68.

[15] D. Gavinsky, "Quantum versus classical simultaneity in communication complexity," *IEEE Transactions on Information Theory*, vol. 65, no. 10, pp. 6466–6483, 2019.

[16] A. Kawachi and H. Nishimura, "Communication complexity of private simultaneous quantum messages protocols," 2021. [Online]. Available: https://arxiv.org/abs/2105.07120

[17] S. Song and M. Hayashi, "Capacity of quantum private information retrieval with multiple servers," *IEEE Transactions on Information Theory*, vol. 67, no. 1, pp. 452–463, 2020.

[18] ——, "Capacity of quantum private information retrieval with colluding servers," *IEEE Transactions on Information Theory*, vol. 67, no. 8, pp. 5491–5508, 2021.

[19] M. Allaix, S. Song, L. Holzbaur, T. Pllaha, M. Hayashi, and C. Hollanti, "On the capacity of quantum private information retrieval from MDS-coded and colluding servers," *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 3, pp. 885–898, 2022.

[20] M. Hayashi and Á. Vázquez-Castro, "Computation-aided classical-quantum multiple access to boost network communication speeds," *Physical Review Applied*, vol. 16, no. 5, p. 054021, 2021.

[21] Y. Yao and S. A. Jafar, "The capacity of classical summation over a quantum MAC with arbitrarily distributed inputs and entanglements," *IEEE Transactions on Information Theory (Early Access)*, 2024.

[22] A. Aytekin, M. Nomeir, S. Vithana, and S. Ulukus, "Quantum symmetric private information retrieval with secure storage and eavesdroppers," 2023. [Online]. Available: https://arxiv.org/abs/2308.10883

[23] J. Yard, P. Hayden, and I. Devetak, "Capacity theorems for quantum multiple-access channels: Classical-quantum and quantum-quantum capacity regions," *IEEE Transactions on Information Theory*, vol. 54, no. 7, pp. 3091–3113, 2008.

[24] M.-H. Hsieh, I. Devetak, and A. Winter, "Entanglement-assisted capacity of quantum multiple-access channels," *IEEE Transactions on Information Theory*, vol. 54, no. 7, pp. 3078–3090, 2008.

[25] S. Jafar, "Interference alignment: A new look at signal dimensions in a communication network," in *Foundations and Trends in Communication and Information Theory*, 2011, pp. 1–136.

[26] R. Ahlswede, N. Cai, S.-Y. Li, and R. Yeung, "Network information flow," *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1204–1216, 2000.

[27] H. Wei, M. Xu, and G. Ge, "Robust network function computation," *IEEE Transactions on Information Theory*, vol. 69, no. 11, pp. 7070–7081, 2023.

[28] R. F. Werner, "All teleportation and dense coding schemes," *Journal of Physics A: Mathematical and General*, vol. 34, no. 35, p. 7081, 2001.

[29] M. Allaix, Y. Lu, Y. Yao, T. Pllaha, C. Hollanti, and S. Jafar, "N-sum box: An abstraction for linear computation over many-to-one quantum networks," 2023. [Online]. Available: https://arxiv.org/abs/2304.07561

[30] M. Grassl, F. Huber, and A. Winter, "Entropic proofs of singleton bounds for quantum error-correcting codes," *IEEE Transactions on Information Theory*, vol. 68, no. 6, pp. 3942–3950, 2022.

[31] M. Mamindlapally and A. Winter, "Singleton bounds for entanglement-assisted classical and quantum error correcting codes," *IEEE Transactions on Information Theory*, vol. 69, no. 9, pp. 5857–5868, 2023.

[32] M. Wilde, *From Classical to Quantum Shannon Theory.* Cambridge University Press, Nov. 2016, [Online draft at ArXiv:1106.1445].

[33] A. Peres and D. R. Terno, "Quantum information and relativity theory," *Rev. Mod. Phys.*, vol. 76, pp. 93–123, Jan 2004. [Online]. Available: https://link.aps.org/doi/10.1103/RevModPhys.76.93

[34] Wikipedia, "No-communication theorem — Wikipedia, the free encyclopedia," http://en.wikipedia.org/w/index.php?title=No-communication%20theorem&oldid=1127027017, 2024, [Online; accessed 11-May-2024].

[35] A. S. Holevo, "Bounds for the quantity of information transmitted by a quantum communication channel," *Problemy Peredachi Informatsii*, vol. 9, no. 3, pp. 3–11, 1973.

[36] W. Helwig, W. Cui, J. I. Latorre, A. Riera, and H.-K. Lo, "Absolute maximal entanglement and quantum secret sharing," *Physical Review A*, vol. 86, no. 5, p. 052335, 2012.

[37] M. Huber and J. I. De Vicente, "Structure of multidimensional entanglement in multipartite systems," *Physical review letters*, vol. 110, no. 3, p. 030501, 2013.

[38] D. Goyeneche, D. Alsina, J. I. Latorre, A. Riera, and K. Życzkowski, "Absolutely maximally entangled states, combinatorial designs, and multiunitary matrices," *Physical Review A*, vol. 92, no. 3, p. 032316, 2015.

[39] N. Linden and A. Winter, "A new inequality for the von neumann entropy," *Communications in mathematical physics*, vol. 259, pp. 129–138, 2005.

[40] R. Prabhu, A. K. Pati, A. Sen, U. Sen *et al.*, "Exclusion principle for quantum dense coding," *Physical Review A*, vol. 87, no. 5, p. 052319, 2013.

[41] C. H. Bennett and S. J. Wiesner, "Communication via one- and two-particle operators on einstein-podolsky-rosen states," *Phys. Rev. Lett.*, vol. 69, pp. 2881–2884, Nov 1992. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.69.2881

[42] H. Araki and E. H. Lieb, "Entropy inequalities," *Communications in Mathematical Physics*, vol. 18, no. 2, pp. 160–170, 1970.

[43] N. Pippenger, "The inequalities of quantum information theory," *IEEE Transactions on Information Theory*, vol. 49, no. 4, pp. 773–789, 2003.

[44] B. M. Terhal, "Quantum error correction for quantum memories," *Rev. Mod. Phys.*, vol. 87, pp. 307–346, Apr 2015. [Online]. Available: https://link.aps.org/doi/10.1103/RevModPhys.87.307