The Capacity of Classical Summation over a Quantum MAC with Arbitrarily Replicated Inputs

Authors
Yao, Yuhang
Jafar, Syed A

Publication Date
2023-05-03

The Capacity of Classical Summation over a Quantum MAC with Arbitrarily Replicated Inputs

Yuhang Yao, Syed Jafar
Center for Pervasive Communications and Computing (CPCC)
University of California Irvine, Irvine, CA 92697
Emails: {*yuhangy5, syed*}*@uci.edu*

***Abstract*—The problem of entanglement-assisted summation over a quantum multiple access channel (Σ-QMAC) is introduced, involving S servers, K classical ($\mathbb{F}_d$) data streams that are replicated arbitrarily across various subsets of servers, and a receiver who wishes to compute the sum of the K data streams. Independent of the data, entangled quantum systems $\mathcal{Q}_1, \mathcal{Q}_2, \cdots, \mathcal{Q}_S$ are prepared in advance and distributed to the corresponding servers. Each server $s, s \in [S]$ locally manipulates its quantum system $\mathcal{Q}_s$ according to its classical data and sends $\mathcal{Q}_s$ to the receiver. The total communication cost is $\log_d |\mathcal{Q}_1| + \log_d |\mathcal{Q}_2| + \cdots + \log_d |\mathcal{Q}_S|$ qudits, where $|\mathcal{Q}_s|$ denotes the dimension of $\mathcal{Q}_s$. Based on a measurement of the composite system $\mathcal{Q}_1\mathcal{Q}_2 \cdots \mathcal{Q}_S$, the receiver must recover the desired sum. The rate thus achieved is defined as the number of dits ($\mathbb{F}_d$ symbols) of the desired sum computed by the receiver per qudit (d-dimsional quantum system) of download. The capacity C is the supremum of the set of all achievable rates. As the main result of this work, the precise capacity of Σ-QMAC is obtained, from which it follows that quantum entanglements allow a factor of 2 gain in capacity (superdense coding gain) relative to capacity with no entanglements, in all cases (any S, K, $\mathbb{F}_d$ and any data replication pattern) provided that the entanglement-assisted capacity does not exceed 1 dit/qudit (Holevo bound). Coding schemes based on a recent N-sum box abstraction are sufficient to achieve capacity.**

I. Introduction

We explore the information-theoretic capacity of an ideal (noise-free) quantum multiple-access channel (QMAC) with S transmitters (servers) and 1 receiver (Alice), used for the elementary distributed classical computation task of *summation* (Σ) of K classical data streams of $\mathbb{F}_d$ symbols (dits), when each data-stream is available to an arbitrary subset of transmitters. In short, we explore the capacity of a Σ-QMAC. To illustrate the problem with a toy example, consider a user, say Alice, who wants to compute the sum of $K = 4$ classical data streams $(\mathsf{A}, \mathsf{B}, \mathsf{C}, \mathsf{D})$, that are distributed among $S = 4$ servers as shown in Fig. 1 so that Servers $1, 2, 3, 4$ have data streams $(\mathsf{A}, \mathsf{B}), (\mathsf{A}, \mathsf{C}), (\mathsf{B}, \mathsf{C}), (\mathsf{D})$, respectively. Alice initially has no quantum resource available to her. Independent of the data-streams, (entangled) quantum systems $\mathcal{Q}_1, \mathcal{Q}_2, \mathcal{Q}_3, \mathcal{Q}_4$ are prepared in advance, and distributed to the corresponding servers. Each Server $s, s \in [S]$ encodes its classical data-stream(s) into its quantum system $\mathcal{Q}_s$ by local operations, and sends $\mathcal{Q}_s$ to Alice, incurring communication cost $\log_d |\mathcal{Q}_s|$ qudits,[1] where $|\mathcal{Q}_s|$ denotes the dimension of the quantum system $\mathcal{Q}_s$. By measuring the received quantum systems, Alice must be able to recover $\mathsf{A} + \mathsf{B} + \mathsf{C} + \mathsf{D}$. If L dits of the desired sum can be computed with total communication cost N qudits, then we say rate $R \leq L/N$ (dits/qudit) is achievable. The capacity C is defined as the supremum of the set of all achievable rates. The capacity in the classical setting[2] (Σ-MAC) is labeled as C_c.

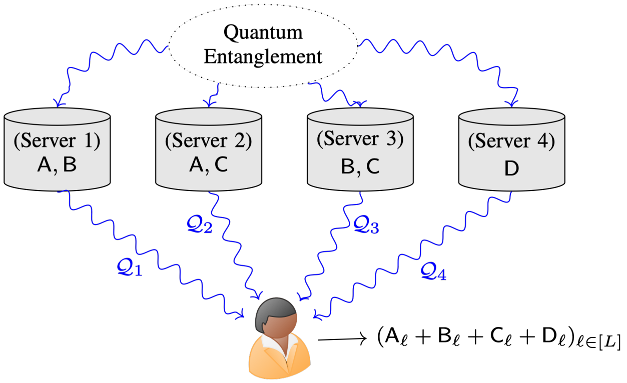

Fig. 1. A Σ-QMAC setting, with $K = 4$ data streams $(\mathsf{A}, \mathsf{B}, \mathsf{C}, \mathsf{D})$ and $S = 4$ servers. Server $s, s \in [S]$ sends quantum subsystem $\mathcal{Q}_s$ to Alice, with communication cost $\log_d |\mathcal{Q}_s|$ qudits.

Prior works in [1]–[3] explore sum-computation over a QMAC with correlated data streams and noisy quantum channels, but with the restriction that there are only 2 servers. Prior works on Quantum Private Information Retrieval (QPIR) [4]–[7] implicitly explore specialized linear computations over a QMAC with multiple transmitters, but since each server in QPIR tends to generate a unique answer, it is as if each server has a unique data stream. The key distinctive aspect that makes the Σ-QMAC setting interesting is that we allow *both* arbitrary number of servers as well as arbitrary replication patterns for the data streams across the servers.

The main motivation of this work is to determine the capacity of the Σ-QMAC. As an elemental setting, a sharp capacity characterization of Σ-QMAC is a stepping stone

[1] In contrast to a *dit*, which is a classical d-ary symbol, a *qudit*, short for a quantum-dit, represents a d-dimensional quantum system. For $d = 2$ these are the common ‘bit’ and ‘qubit,’ respectively.

[2] The Σ-MAC is obtained from the Σ-QMAC by removing all quantum resources, and having the servers send classical dits instead of qudits.

towards understanding the capacity of a QMAC for *general* linear computation tasks. Additional motivation comes from the perspectives of *superdense coding* [8] and the *N-sum box abstraction* [9]. Quantum systems are particularly interesting because of quantum-entanglements, which lead to counter-intuitive phenomena, e.g., quantum teleportation. In the context of quantum communication, the benefits of quantum-entanglements are manifested in the possibility of *super-dense coding* gains. It is well known that in the absence of entanglements, each qudit of quantum communication can deliver no more information than a classical dit (Holevo Bound). Quantum entanglements have the *potential* to double[3] the capacity of the Σ-QMAC through superdense coding. Since the data-streams are distributed among arbitrary subsets of servers, the challenge is to design capacity-optimal distributed quantum encoding schemes that maximally exploit superdense coding gain.

Our approach to this task is facilitated by the N-sum box abstraction formalized recently in [9]. The N-sum box is a classical 'black-box' abstraction of a QMAC protocol, that translates certain quantum protocols into a classical MIMO MAC functionality[4] subject to certain constraints on the feasible channel matrices. Conceptually, the challenge from the achievability perspective is to design suitable precoding schemes as well as channel matrices that satisfy those constraints while performing the computation task (summation in this case) with maximal efficiency, whereas the challenge from the converse perspective is to prove information theoretic optimality not just within the class of coding schemes allowed by the N-sum box abstraction, but among all possible coding schemes. As our main result we characterize the exact capacity of Σ-QMAC by providing N-sum box based achievable schemes, with matching information theoretic converse bounds.

To complete the picture for our motivating example in Fig. 1, let us explicitly state our results for this case. For this example, our results show that the capacity $C = 4/5$ dits/qudit. From existing results on capacity of classical sum-networks [10], [11], it is not difficult to see that without entanglements, the capacity is only $C_C = 2/5$ dits/qudit. Thus a factor of 2 super-dense coding gain is available in this case. We also show that if coding schemes are restricted to 2-sum protocols [7], then the capacity for this example is $3/4$ dits/qudit. Evidently, 2-sum protocols are in general not sufficient to achieve the capacity of the Σ-QMAC.

Notation: $\mathbb{N}$ denotes the set of positive integers. $\mathbb{Z}^+ \triangleq \{0\} \cup \mathbb{N}$. For $n \in \mathbb{N}$, $[n]$ denotes the set $\{1, 2, \cdots, n\}$. $A_{[n]}$ is the compact notation of the tuple $(A_1, A_2, \cdots, A_n)$. $\mathbb{F}_d$ denotes the finite field with $d = p^r$ a power of a prime. $\mathbb{C}$ denotes the set of complex numbers. $\mathbb{R}_+$ denotes the set of non-negative real numbers. For any field $\mathbb{F}$, $\mathbb{F}^{a \times b}$ denotes the set of $a \times b$ matrices with elements in $\mathbb{F}$. $\mathbf{I}_a$ denotes the $a \times a$ identity matrix. $\mathbf{0}_{a \times b}$ denotes the $a \times b$ zero matrix. $2^{\mathcal{N}}$ denotes the power set of $\mathcal{N}$. The notation $f : \mathcal{A} \to \mathcal{B}$ denotes a map f from $\mathcal{A}$ to $\mathcal{B}$. The dimension of a quantum system $\mathcal{Q}$ is denoted as $|\mathcal{Q}|$.

II. Problem Formulation

A. Σ-QMAC and Σ-MAC

The Σ-QMAC problem, and its corresponding classical Σ-MAC problem, are both specified by a 4-tuple $\big(\mathbb{F}_d, S, K, \mathcal{W}\big)$. $\mathbb{F}_d$ is a finite field of order d with $d = p^r$ being a power of a prime. S is the number of servers. K is the number of independent classical data-streams. The k^{th} data stream is denoted by W_k and is comprised of symbols $\mathsf{W}_k(\ell) \in \mathbb{F}_d, \ell \in \mathbb{N}$. For each $\ell \in \mathbb{N}$, let $\mathsf{W}(\ell) \triangleq (\mathsf{W}_1(\ell), \mathsf{W}_2(\ell), \cdots, \mathsf{W}_K(\ell)) \in \mathbb{F}_d^{1 \times K}$ denote the ℓ^{th} data instance. The mapping $\mathcal{W} : [K] \to 2^{[S]}$ identifies $\mathcal{W}(k) \subset [S]$ as the subset of servers where W_k is available. There is a user (Alice) who wishes to compute the sum $\mathsf{W}_\Sigma(\ell) \triangleq \sum_{k \in [K]} \mathsf{W}_k(\ell)$ for all $\ell \in \mathbb{N}$. The distinction between Σ-QMAC and Σ-MAC lies in the coding schemes allowed in the two settings. In the Σ-QMAC the servers code their information into quantum systems using quantum gates, and send their quantum systems to Alice, whereas in the Σ-MAC setting, no quantum resource is assumed, each server codes only over classical dits and sends the classical dits to Alice.

B. General Quantum Coding Scheme

A general quantum coding scheme specifies the batch size for the computation, i.e., how many data instances are to be coded together, the initial quantum entanglement, the assignments of the entangled resources to transmitters, the local quantum encoding operations to be performed at each transmitter, the measurement to be performed at the receiver, and a mapping of the measured value to the desired computation results. Specifically, for a Σ-QMAC $\big(\mathbb{F}_d, S, K, \mathcal{W}\big)$, a coding scheme is specified by a 6-tuple $\big(L, \delta_{[S]}, \rho, \Phi_{[S]}, \{M_y\}_{y \in \mathcal{Y}}, \Psi\big)$. $L \in \mathbb{N}$ is referred to as the batch size, which is the number of computations (sums) to be encoded by the coding scheme, i.e., the coding scheme allows Alice to compute $\mathsf{W}_\Sigma(\ell)$ for all $\ell \in [L]$. Denote the first L data instances of all K data streams collectively as,

$$\mathsf{W}^{(L)} = (\mathsf{W}(1)^T, \mathsf{W}(2)^T, \cdots, \mathsf{W}(L)^T)^T \in \mathbb{F}_d^{L \times K}, \quad (1)$$

the first L instances of the k^{th} data stream as

$$\mathsf{W}_k^{(L)} \triangleq (\mathsf{W}_k(1), \mathsf{W}_k(2), \cdots, \mathsf{W}_k(L))^T \in \mathbb{F}_d^{L \times 1}, \quad (2)$$

and the desired computation at Alice as,

$$\mathsf{W}_\Sigma^{(L)} = (\mathsf{W}_\Sigma(1), \mathsf{W}_\Sigma(2), \cdots, \mathsf{W}_\Sigma(L))^T \in \mathbb{F}_d^{L \times 1}. \quad (3)$$

Independent of data-streams, quantum systems $\mathcal{Q}_1, \mathcal{Q}_2, \cdots, \mathcal{Q}_S$ are prepared in advance, with the initial (in general, entangled) state of the composite system $\mathcal{Q}_1 \mathcal{Q}_2 \cdots \mathcal{Q}_S$ denoted by the density matrix ρ. For all $s \in [S]$, $\delta_s \in \mathbb{Z}^+$ specifies the dimension of the

[3] Parallels are noteworthy to wireless research on full-duplex radios which is motivated by a similar potential for doubling the network capacity.

[4] Taking advantage of the N-sum box abstraction, the achievability is presented almost entirely in classical information theoretic terms, while limiting explicitly quantum theoretic descriptions to the minimum necessary.

quantum subsystem $\mathcal{Q}_s$, i.e., $|\mathcal{Q}_s| = \delta_s$. The quantum system $\mathcal{Q}_s$ is distributed to Server s, for all $s \in [S]$. The parameters $\Phi_{[S]} = (\Phi_1, \Phi_2, \cdots, \Phi_S)$ are functions that specify the local quantum operations performed by each Server s on its quantum system $\mathcal{Q}_s$, by which the classical information is encoded into the quantum systems. Specifically, the local quantum operations at Server s are described by a $\mathbb{C}^{|\mathcal{Q}_s| \times |\mathcal{Q}_s|}$ unitary matrix U_s, that is chosen depending on the data streams available to Server s, as $U_s = \Phi_s(\mathsf{W}_k^{(L)}, k : s \in \mathcal{W}(k))$. The resulting state of the composite system is $\rho' = U\rho\, U^\dagger, \;\; U \triangleq U_1 \otimes U_2 \otimes \cdots \otimes U_S$. The composite system is then sent to Alice, who performs a quantum measurement (POVM) with the set of operators $\{M_y\}_{y \in \mathcal{Y}}$. The output of the measurement is denoted as Y, which is a random variable with realizations in $\mathcal{Y}$. Finally, the function $\Psi : \mathcal{Y} \to \mathbb{F}_d^{L \times 1}$ maps the measurement output Y to the desired computation, i.e., $\mathsf{W}_\Sigma^{(L)} = \Psi(Y)$. Any coding scheme must work for all d^{KL} realizations of $\mathsf{W}^{(L)}$. Let $\mathfrak{C}$ denote the set of feasible quantum coding schemes.

C. Feasible Region, Capacity

For the Σ-QMAC $\big(\mathbb{F}_d, S, K, \mathcal{W}\big)$, the download-cost per computation (qudits/dit) tuple,

$$\Delta = (\Delta_1, \Delta_2, \cdots, \Delta_S) \in \mathbb{R}_+^S \tag{4}$$

is said to be feasible, if there exists a coding scheme $\big(L, \delta_{[S]}, \rho, \Phi_{[S]}, \{M_y\}_{y \in \mathcal{Y}}, \Psi\big) \in \mathfrak{C}$ such that

$$\Delta_s \geq \log_d |\mathcal{Q}_s| / L = \log_d \delta_s / L, \qquad \forall s \in [S]. \tag{5}$$

Define $\mathcal{D}$ as the closure of the set of all feasible download-cost tuples Δ, so that any Δ inside $\mathcal{D}$ is feasible, and any Δ outside $\mathcal{D}$ is not feasible. In terms of computation rates (computations/qudit), a rate R is feasible if there exists a coding scheme $\big(L, \delta_{[S]}, \rho, \Phi_{[S]}, \{M_y\}_{y \in \mathcal{Y}}, \Psi\big) \in \mathfrak{C}$ such that

$$R \leq \frac{L}{\log_d \delta_1 + \log_d \delta_2 + \cdots + \log_d \delta_S}. \tag{6}$$

Define

$$C \triangleq \sup_{\mathfrak{C}} R \tag{7}$$

as the computation capacity. Note that the reciprocal of capacity, $1/C = \min_{\Delta \in \mathcal{D}} \sum_{s \in [S]} \Delta_s$.

D. The N-sum Box

While we seek optimality among general quantum coding schemes described above, our results will remarkably show that coding schemes based on N-sum box abstractions turn out to be capacity-achieving for the Σ-QMAC. The N-sum box abstraction from [9] is summarized next.

Building on the stabilizer formalism and quantum error correction, the N-sum box is a MIMO MAC setting with $2N$ classical inputs, labeled $x_1, x_2, \cdots, x_{2N} \in \mathbb{F}_d$, and N classical outputs $y_1, y_2, \cdots, y_N \in \mathbb{F}_d$, described as,

$$\begin{bmatrix} y_1 \\ \vdots \\ y_N \end{bmatrix} = \begin{bmatrix} M_{1,1} & \cdots & M_{1,2N} \\ \vdots & \vdots & \vdots \\ M_{N,1} & \cdots & M_{N,2N} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_{2N} \end{bmatrix} \tag{8}$$

which can be represented compactly as $\mathbf{y} = \mathbf{M}\mathbf{x}$. The N-sum box abstraction represents the setting where N entangled qudits are distributed among S transmitters, such that each transmitter can perform conditional quantum X, Z gate operations on its qudit(s) to encode classical information. The transmitter that has the n^{th} qudit controls the inputs x_n and x_{N+n} of the N-sum box. For example, if Qudits 1 and 3 are given to Transmitter 1, then in the N-sum box abstraction the inputs $x_1, x_{1+N}, x_3, x_{3+N}$ are the inputs available to Transmitter 1. The N outputs are the result of the quantum measurement performed by Alice. Since the N qudits are sent to Alice for the quantum measurement, the N-sum box has a quantum communication cost of N qudits. Now let us consider the channel matrix $\mathbf{M}$. Different choices of entanglement states and quantum-measurement bases produce different channel matrices. Depending on the desired computation task a suitable $\mathbf{M}$ may be chosen from the set of feasible choices. The channel matrices that can be obtained from the stabilizer-based construction are precisely those (see [9]) that are strongly self-orthogonal, i.e., that satisfy the following two conditions,

$$\text{rank}(\mathbf{M}) = N, \qquad \mathbf{M}\mathbf{J}_{2N}\mathbf{M}^T = \mathbf{0}_{N \times N} \tag{9}$$

where $\mathbf{J}_{2N} = \left(\begin{smallmatrix} \mathbf{0} & -\mathbf{I}_N \\ \mathbf{I}_N & \mathbf{0} \end{smallmatrix}\right)$ and $\mathbf{I}_N$ is the $N \times N$ identity matrix. Designing quantum-codes for the Σ-QMAC using the N-sum box abstraction entails a choice of not only which N-sum boxes to use, how many of the inputs of each N-sum box to assign to each transmitter, and how to precode at each transmitter in the MIMO MAC for the desired computation, but in contrast to conventional (wireless) MIMO MAC settings where the channels are randomly chosen by nature, here we also have the freedom to design suitable channel matrices $\mathbf{M}$ for the desired computation task, within the class of feasible choices. The N-sum box abstraction then guarantees that corresponding to these choices there exist initial quantum entanglements, quantum-coding operations at the transmitters, and quantum-measurement operations at the receiver, that achieve the desired MIMO MAC functionality, at the communication cost of N qudits for each N-sum box utilized by the coding scheme.

III. Results

A. Capacity of Σ-QMAC

Theorem 1. *For the Σ-QMAC $\big(\mathbb{F}_d, K, S, \mathcal{W}\big)$, the feasible region $\mathcal{D}$ is characterized as,*

$$\mathcal{D} = \left\{ \Delta \in \mathbb{R}_+^S \;\middle|\; \begin{array}{l} \sum_{s \in [S]} \Delta_s \geq 1, \\ \sum_{s \in \mathcal{W}(k)} \Delta_s \geq 1/2, \forall k \in [K]. \end{array} \right\}. \tag{10}$$

We present the proof in Section IV. To illustrate the result, let us briefly sketch the solution to the example in Fig. 1. For a more intuitive notation, let us use subscripts 'ab','ac','bc','d' to represent '1', '2', '3', '4', respectively, reflecting the data-streams available at the corresponding servers. For example, we indicate server $\mathcal{S}_1$ as $\mathcal{S}_{ab}$, making it explicit that this server has data-streams A, B. With this notation, according to Theorem 1 the feasible region is explicitly expressed as,

$$\mathcal{D} = \left\{ \begin{array}{c|l} (\Delta_{ab}, \Delta_{ac}, & \Delta_{ab} + \Delta_{ac} + \Delta_{bc} + \Delta_d \geq 1, \\ & \Delta_{ab} + \Delta_{ac} \geq 1/2, \\ \Delta_{bc}, \Delta_d) \in \mathbb{R}_+^4 & \Delta_{ab} + \Delta_{bc} \geq 1/2, \\ & \Delta_{ac} + \Delta_{bc} \geq 1/2, \\ & \Delta_d \geq 1/2. \end{array} \right\}.$$

Minimizing $\Delta_{ab} + \Delta_{ac} + \Delta_{bc} + \Delta_d$ over $\mathcal{D}$ leads to a linear program with optimal value $5/4$, thus establishing the capacity for this example as $C = 4/5$. To show the achievability of $4/5$, we specify a coding scheme that allows Alice to recover $L = 4$ instances of the desired sums, based on an $(N = 5)$-sum box in $\mathbb{F}_d$ so that in the 5-sum box server $\mathcal{S}_{ab}$ controls 1 pair of inputs x_1, x_6; $\mathcal{S}_{ac}$ controls 1 pair of inputs x_2, x_7; $\mathcal{S}_{bc}$ controls 1 pair of inputs x_3, x_8; and $\mathcal{S}_d$ controls 2 pair of inputs x_4, x_5, x_9, x_{10}. The input-output relationship for the 5-sum box is $\mathbf{y} = \mathbf{M}\mathbf{x}$ with the transfer function $\mathbf{M} \in \mathbb{F}_d^{5\times 10}$ specified as,

$$\mathbf{M} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}. \tag{11}$$

Note that (9) is satisfied, so it is a valid 5-sum box.

Each server precodes its accessible data streams and maps the coded symbols to the inputs of the 5-sum box controlled by that server. For example, Server $\mathcal{S}_{ab}$, precodes the $L\times 1 = 4\times 1$ vector of data stream A (say, $\mathsf{A}^{(L)} = \mathsf{A}^{(4)}$) with the $2N_{ab}\times L = 2\times 4$ precoding matrix V_{ab}^a. Similarly, $\mathcal{S}_{ab}$ precodes data stream B with the 2×4 precoding matrix V_{ab}^b. The precoded symbols are then mapped to the inputs controlled by Server $\mathcal{S}_{ab}$, i.e., x_1, x_6, so that we have,

$$\begin{bmatrix} x_1 \\ x_6 \end{bmatrix} = V_{ab}^a \mathsf{A}^{(4)} + V_{ab}^b \mathsf{B}^{(4)}. \tag{12}$$

Each server similarly precodes the data streams available to it with its corresponding precoding matrices.

To the output $\mathbf{y} \in \mathbb{F}_d^{5\times 1}$, Alice applies a 4×5 decoding matrix V_{dec} specified as,

$$V_{\text{dec}} = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}. \tag{13}$$

Fig. 2 illustrates the precoding and decoding operations. The precoding matrices are now specified as,

$$\begin{bmatrix} V_{ab}^a \\ V_{ac}^a \end{bmatrix} = \left(V_{\text{dec}}\mathbf{M}_{[1,6,2,7]}\right)^{-1}, \ \begin{bmatrix} V_{ab}^b \\ V_{bc}^b \end{bmatrix} = \left(V_{\text{dec}}\mathbf{M}_{[1,6,3,8]}\right)^{-1},$$
$$\begin{bmatrix} V_{ac}^c \\ V_{bc}^c \end{bmatrix} = \left(V_{\text{dec}}\mathbf{M}_{[2,7,3,8]}\right)^{-1}, \ V_d^d = \left(V_{\text{dec}}\mathbf{M}_{[4,5,9,10]}\right)^{-1}. \tag{14}$$

where $\mathbf{M}_{[i_1, i_2, \cdots, i_n]}$ is an $N \times n$ submatrix of $\mathbf{M}$ comprised of the $(i_1, i_2, \cdots, i_n)^{th}$ columns of $\mathbf{M}$. It is easy to verify that $\det(V_{\text{dec}}\mathbf{M}_{[1,6,2,7]}) = \det(V_{\text{dec}}\mathbf{M}_{[2,7,3,8]}) = 1$ and $\det(V_{\text{dec}}\mathbf{M}_{[1,6,3,8]}) = \det(V_{\text{dec}}\mathbf{M}_{[4,5,9,10]}) = -1$, thus all 4 inverses in (14) exist. With all choices explicitly specified, it is similarly easy to verify that we have,

$$V_{\text{dec}}\mathbf{y} = V_{\text{dec}}\mathbf{M}\mathbf{x} = \mathsf{A}^{(4)} + \mathsf{B}^{(4)} + \mathsf{C}^{(4)} + \mathsf{D}^{(4)}. \tag{15}$$

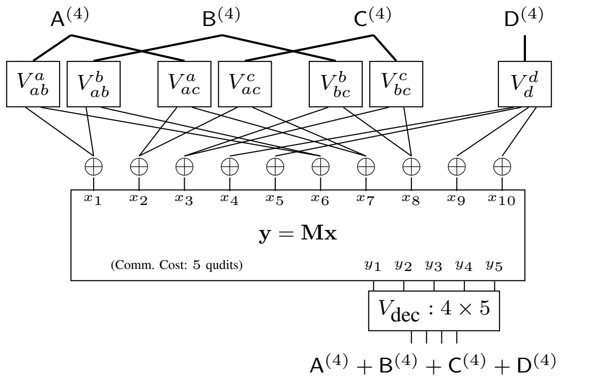
$\mathsf{A}^{(4)}$
$\mathsf{B}^{(4)}$
$\mathsf{C}^{(4)}$
$\mathsf{D}^{(4)}$
V_{ab}^a
V_{ab}^b
V_{ac}^a
V_{ac}^c
V_{bc}^b
V_{bc}^c
V_d^d
x_1 x_2 x_3 x_4 x_5 x_6 x_7 x_8 x_9 x_{10}
$\mathbf{y} = \mathbf{M}\mathbf{x}$
(Comm. Cost: 5 qudits)
y_1 y_2 y_3 y_4 y_5
$V_{\text{dec}} : 4 \times 5$
$\mathsf{A}^{(4)} + \mathsf{B}^{(4)} + \mathsf{C}^{(4)} + \mathsf{D}^{(4)}$

Fig. 2. Precoding and decoding for the Σ-QMAC example of Fig. 1.

Thus, Alice is able to compute 4 instances of the desired sum, with the total download cost of 5 qudits. The rate achieved is $4/5$ dits/qudit, matching the capacity of this Σ-QMAC setting.

B. 2-sum Protocol Capacity of Σ-QMAC in Fig. 1

If in Fig. 1 the servers are only allowed to use the 2-sum protocol [7], we will show that the capacity (largest possible rate under this restriction), denoted as $C_{\text{2-sum}} = 3/4$ dits/qudit.

Consider a classical Σ-MAC setting, denoted as Σ^2-MAC, with 6 servers, each constructed by merging the storage of a pair of servers in the original Σ-QMAC, so that they store $\mathsf{ABC}, \mathsf{ABC}, \mathsf{ABD}, \mathsf{ABC}, \mathsf{ACD}, \mathsf{BCD}$, respectively. The three servers with the same storage ABC can be considered as the same server to obtain a Σ^2-MAC with 4 servers. Label the servers as $\mathcal{S}_{abc}, \mathcal{S}_{abd}, \mathcal{S}_{acd}$ and $\mathcal{S}_{bcd}$. Now consider any use of the 2-sum protocol by any pair of the servers in Σ-QMAC, the output of the 2-sum protocol is 2 dits, which can always be locally generated by a server in the Σ^2-MAC. For example, if $\mathcal{S}_{ab}$ and $\mathcal{S}_{ac}$ use the 2-sum protocol to output (y_1, y_2), then $\mathcal{S}_{abc}$ is able to directly generate (y_1, y_2). Since each use of the 2-sum protocol costs 2 qudits, and sending (y_1, y_2) directly costs 2 dits, it follows that the capacity of the Σ-QMAC cannot be greater than the capacity of the Σ^2-MAC. Now the capacity of the Σ^2-MAC is bounded by cut-set bounds as,

$$\begin{aligned} &\Delta_{abc} + \Delta_{abd} + \Delta_{acd} \geq 1, \ \Delta_{abc} + \Delta_{abd} + \Delta_{bcd} \geq 1, \\ &\Delta_{abc} + \Delta_{acd} + \Delta_{bcd} \geq 1, \ \Delta_{abd} + \Delta_{acd} + \Delta_{bcd} \geq 1, \end{aligned} \tag{16}$$

which together yield that $\Delta_{abc} + \Delta_{abd} + \Delta_{acd} + \Delta_{bcd} \geq 4/3$. Thus, the (classical) capacity of the Σ^2-MAC is not greater than $3/4$, which implies in turn that $C_{\text{2-sum}} \leq 3/4$. For achievability, first note that in the Σ^2-MAC, the rate $3/4$ is achieved by downloading the 4 dits $Y_{abc} = \mathsf{A}_1 - \mathsf{A}_2 + \mathsf{A}_3 + \mathsf{B}_1 - \mathsf{B}_2 + \mathsf{C}_1$, $Y_{abd} = \mathsf{A}_2 - \mathsf{A}_3 + \mathsf{B}_2 + \mathsf{D}_1$, $Y_{acd} = \mathsf{A}_3 + \mathsf{C}_2 + \mathsf{D}_2 - \mathsf{D}_1$, $Y_{bcd} = \mathsf{B}_3 + \mathsf{C}_3 - \mathsf{C}_2 + \mathsf{D}_3 - \mathsf{D}_2 + \mathsf{D}_1$, which allows Alice to recover 3 instances of the desired sum from $Y_{abc} + Y_{abd}, Y_{abd} + Y_{acd}, Y_{acd} + Y_{bcd}$. Then note that two independent instances of each of these downloads can be equivalently recovered from a 2-sum box in the Σ-QMAC. For example, two instances of Y_{abc} can be recovered from $\mathcal{S}_{ab}, \mathcal{S}_{ac}$ using a 2-sum box. Thus, the Σ-QMAC allows Alice to recover 6 dits of desired sum computation by downloading $2 \times 4 = 8$ qudits, thus achieving the rate $3/4$ dits/qudit.

IV. Proof of Theorem 1

A. Proof of Achievability

The following two lemmas will be useful in the proof.

Lemma 1. *Let $\mathbf{M}_k \in \mathbb{F}_q^{N\times m_k}, k \in [K]$ such that $\min_{k\in[K]} \mathrm{rk}(\mathbf{M}_k) \geq L$. If $q > KL$, then $\exists \mathbf{U} \in \mathbb{F}_q^{L\times N}, \mathbf{V}_k \in \mathbb{F}_q^{m_k\times L}, k \in [K]$ such that $\mathbf{U}\mathbf{M}_k\mathbf{V}_k = \mathbf{I}_L$ for all $k \in [K]$.*

Proof. For each $k \in [K]$, since $\mathrm{rk}(\mathbf{M}_k) \geq L$, there exist matrices $\overline{\mathbf{U}}_k \in \mathbb{F}_q^{L\times N}$, $\overline{\mathbf{V}}_k \in \mathbb{F}_q^{m_k\times L}$ such that $\overline{\mathbf{U}}_k\mathbf{M}_k\overline{\mathbf{V}}_k = \mathbf{I}_L$. Now consider a matrix $\mathbf{U} \in \mathbb{F}_q^{L\times N}$ whose elements are variables with values yet to be determined. Note that $P_k \triangleq \det(\mathbf{U}\mathbf{M}_k\overline{\mathbf{V}}_k)$ is a polynomial of degree L' in these variables, and it is not a zero polynomial because setting $\mathbf{U} = \overline{\mathbf{U}}_k$ yields the valuation $P_k = \det(\mathbf{I}_L) = 1$. It follows that $P \triangleq \prod_{k\in[K]} P_k$ is a non-zero polynomial with degree KL. By Schwartz-Zippel Lemma, the probability of P evaluating to zero is not more than $\frac{KL}{q}$. Therefore, if $q > KL$, there exists a realization of $\mathbf{U}$ for which the evaluation of P is non-zero $\implies$ $\mathbf{U}\mathbf{M}_k\overline{\mathbf{V}}_k$ is invertible for all $k \in [K]$ for this realization of $\mathbf{U}$. Now let $\mathbf{V}_k \triangleq \overline{\mathbf{V}}_k(\mathbf{U}\mathbf{M}_k\overline{\mathbf{V}}_k)^{-1}$. We obtain that $\mathbf{U}\mathbf{M}_k\mathbf{V}_k = \mathbf{I}_L$ for all $k \in [K]$. □

Definition: Say $\mathbf{M} = [\mathbf{M}^l, \mathbf{M}^r] \in \mathbb{F}_q^{N\times 2N}$ is the transfer matrix of an N-sum box operating in $\mathbb{F}_q$. $\mathbf{M}^l, \mathbf{M}^r \in \mathbb{F}_q^{N\times N}$ denote the left and right halves. Let $i_1, i_2, \cdots, i_n \in \mathbb{N}$ be $n \leq N$ distinct indices not greater than N. We say $\mathbf{M}$ is half-MDS if for all such indices, $\mathrm{rk}\big(\big[\mathbf{M}^l_{[i_1,\cdots,i_n]}, \mathbf{M}^r_{[i_1,\cdots,i_n]}\big]\big) = \min\{2n, N\}$, where $\mathbf{M}_{[i_1,i_2,\cdots,i_n]}$ denotes the $N\times n$ submatrix of $\mathbf{M}$ comprised of the $(i_1, i_2, \cdots, i_n)^{th}$ columns of $\mathbf{M}$.

As an example, consider feasible transfer matrices for 2-sum boxes,

$$\mathbf{M}_1 = \left(\begin{smallmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{smallmatrix}\right), \quad \mathbf{M}_2 = \left(\begin{smallmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{smallmatrix}\right). \tag{17}$$

Note that $\mathbf{M}_1$ is half-MDS while $\mathbf{M}_2$ is not. The submatrix comprised of the 2^{nd} and 4^{th} columns of $\mathbf{M}_2$ has rank $1 < 2$.

Lemma 2 (Half-MDS N-sum box)**.** *If $q \geq N$, there exists an N-sum box with half-MDS transfer matrix $\mathbf{M} \in \mathbb{F}_q^{N\times 2N}$.*

The proof of Lemma 2 appears in the Appendix. Let us describe a general linear scheme based on the N-sum box. Given $z \in \mathbb{N}$, denote $q = d^z$. Servers $s \in [S]$ together implement an N-sum box operating in $\mathbb{F}_q$ with Server s controlling N_s pairs of inputs so that $N_1 + N_2 + \cdots + N_S = N$. This requires the dimension of the quantum system $\mathcal{Q}_s$ to be $q^{N_s} = d^{N_s z}$ for $s \in [S]$. The transfer matrix of the N-sum box is denoted by $\mathbf{M} \in \mathbb{F}_q^{N\times 2N}$. Recall that for each data stream $\mathsf{W}_k, k \in [K]$, one can consider each z symbols in $\mathbb{F}_d$ as one symbol in $\mathbb{F}_q$. Therefore, let $\mathbf{W}_k \in \mathbb{F}_q^{L'\times 1}$ denote the first L' symbols of W_k considered in $\mathbb{F}_q$ (which correspond to $L'z$ symbols in the original field $\mathbb{F}_d$, i.e., $\mathsf{W}_k^{(L'z)}$). For the N-sum box, the output is $\mathbf{y} = \mathbf{M}\mathbf{x} \in \mathbb{F}_q^{N\times 1}$ where $\mathbf{x} \in \mathbb{F}_q^{2N\times 1}$.

For $s \in [S], k \in [K]$, $V_s^k \in \mathbb{F}_q^{2N_s\times L'}$ specifies a coder at Server s if $s \in \mathcal{W}(k)$. Otherwise, let V_s^k be an empty matrix with size $0 \times 2N_s$. The input to the N-sum box at Server s is specified as $\sum_{k: s\in\mathcal{W}(k)} V_s^k\mathbf{W}_k$. The output is,

$$\mathbf{y} = \mathbf{M}\mathbf{x} = \sum_{k\in[K]} \mathbf{M}_k \underbrace{\begin{pmatrix} V_1^k \\ V_2^k \\ \vdots \\ V_S^k \end{pmatrix}}_{\mathbf{V}_k} \mathbf{W}_k, \tag{18}$$

where $\mathbf{M}_k$ is a submatrix of $\mathbf{M}$ comprised of $\sum_{s\in\mathcal{W}(k)} 2N_s$ columns of $\mathbf{M}$ that are accessible by $\mathbf{W}_k$. To see this, for any $k \in [K]$, consider $\mathbf{W}_{k'} = \mathbf{0}_{L'\times 1}$ for $k' \neq k, k' \in [K]$. The input to the n-sum box at Server s is then $V_s^k\mathbf{W}_k$ if $s \in \mathcal{W}(k)$, or $\mathbf{0}_{2N_s\times 1}$ otherwise. The output $\mathbf{y}$ is then $\mathbf{M}_k\mathbf{V}_k\mathbf{W}_k$. Note that $\mathbf{y}$ is a linear function of $\mathbf{W}_1, \mathbf{W}_2, \cdots, \mathbf{W}_K$. Therefore, we obtain the general expression of the output $\mathbf{y}$ as in (18).

Next, $V_{\text{dec}} \in \mathbb{F}_q^{L'\times N}$ specifies a decoder so that Alice is able to compute $V_{\text{dec}} \sum_{k\in[K]} \mathbf{M}_k\mathbf{V}_k\mathbf{W}_k$. Let $q > KL'$, i.e., $z > \log_d KL'$ and $L' \leq \min_{k\in[K]} \mathrm{rk}(\mathbf{M}_k)$. With Lemma 1, there exist such V_{dec} and $\mathbf{V}_k, k \in [K]$ so that

$$V_{\text{dec}} \sum_{k\in[K]} \mathbf{M}_k\mathbf{V}_k\mathbf{W}_k = \sum_{k\in[K]} \mathbf{W}_k, \tag{19}$$

which is the desired sum in $\mathbb{F}_q$ for L' instances. Equivalently, this is the desired sum in $\mathbb{F}_d$ for $L = L'z$ instances. This shows that the download-cost tuple $(\log_d |\mathcal{Q}_1|/L, \cdots, \log_d |\mathcal{Q}_S|/L) = (N_1/L', \cdots, N_S/L')$ is feasible if $L' \leq \min_{k\in[K]} \mathbf{M}_k$. With Lemma 2, if $q \geq N$, i.e., $z \geq \log_d N$, then there exists a half-MDS N-sum box. Now that $\mathbf{M}$ is half-MDS, the rank of $\mathbf{M}_k$ is equal to $\min\{\sum_{s\in\mathcal{W}(k)} 2N_s, N\}$. Therefore, the download-cost tuple $(N_1/L', \cdots, N_S/L')$ is feasible if $L' \leq N$ and $L' \leq \sum_{s\in\mathcal{W}(k)} 2N_s$ for all $k \in [K]$. It follows that the feasible region contains

$$\text{closure}\left\{ \Delta \in \mathbb{R}_+^S \;\middle|\; \begin{array}{l} L', N_1, N_2, \cdots, N_S \in \mathbb{Z}^+ \\ \sum_{s\in[S]} N_s \geq L', \\ \sum_{s\in\mathcal{W}(k)} 2N_s \geq L', \forall k \in [K], \\ \Delta_s \geq N_s/L', s \in [S]. \end{array} \right\} \tag{20}$$

$$= \left\{ \Delta \in \mathbb{R}_+^S \;\middle|\; \begin{array}{l} \sum_{s\in[S]} \Delta_s \geq 1, \\ \sum_{s\in\mathcal{W}(k)} \Delta_s \geq 1/2, \forall k \in [K]. \end{array} \right\} \tag{21}$$

which is the feasible region $\mathcal{D}$ specified in Theorem 1.

B. Proof of Converse

For the converse, consider this scenario. Bob has a quantum system $\mathcal{Q}_B$ with dimension $|\mathcal{Q}_B|$ and Alice has a quantum system $\mathcal{Q}_A$ with dimension $|\mathcal{Q}_A|$. Bob observes a random variable X that is independent of the initial state of the composite system $\mathcal{Q}_B\mathcal{Q}_A$. Bob encodes X into $\mathcal{Q}_B$ and transmits $\mathcal{Q}_B$ to Alice, who measures $\mathcal{Q}_B\mathcal{Q}_A$ by a POVM [12] and gets output Y. The Holevo bound [13] implies $I(X;Y) \leq \log_d |\mathcal{Q}_B\mathcal{Q}_A|$ dits. In addition, [14, Prop. 6] implies $I(X;Y) \leq 2\log_d |\mathcal{Q}_B|$ dits, reflecting the Information Causality Principle [15].

Now let us go back to the proof. Consider any feasible coding scheme $\big(L, \mathcal{Q}_{[S]}, \rho, \Phi_{[S]}, \{M_y\}_{y\in\mathcal{Y}}, \Psi\big)$. Since the scheme must work for all d^{KL} realizations of $\mathsf{W}^{(L)}$, for any $k \in [K]$, it must work for the cases when $\mathsf{W}_{k'}^{(L)} =$

$\mathbf{0}_{L\times 1}, \forall k' \in [K], k' \neq k$. In these cases, Alice must be able to decode $\mathsf{W}_k^{(L)}$. Assume the L elements of $\mathsf{W}_k^{(L)}$ are drawn i.i.d. uniform in $\mathbb{F}_d$. Let us denote $\mathcal{B}_k \triangleq \mathcal{W}(k)$ and $\mathcal{A}_k \triangleq [S]\backslash\mathcal{B}_k$. Assume that Servers in Group $\mathcal{A}_k$ collaborate with Alice by bringing their quantum resource and sharing their accessible data with her. In other words, every server that *does not* have access to the k-th data stream collaborates with Alice. Consider the servers in Group $\mathcal{B}_k$ collectively as the transmitter, while Alice and the servers in Group $\mathcal{A}_k$ collectively form the receiver. Denote $\mathcal{Q}_{B_k}$ as the quantum system sent from Group $\mathcal{Q}_{B_k}$, $\mathcal{Q}_{A_k}$ as the quantum system brought from Group $\mathcal{A}_k$ and $\mathcal{Q}_{B_k}\mathcal{Q}_{A_k}$ as the composite system. We obtain that $\min\left(\log_d \prod_{s\in[S]} |\mathcal{Q}_s|, 2\log_d \prod_{s\in\mathcal{B}_k} |\mathcal{Q}_s|\right) = \min\left(\log_d |\mathcal{Q}_{B_k}\mathcal{Q}_{A_k}|, 2\log_d |\mathcal{Q}_{B_k}|\right) \geq I(\mathsf{W}_k^{(L)}; Y) \geq I(\mathsf{W}_k^{(L)}; \mathsf{W}_k^{(L)}) = H(\mathsf{W}_k^{(L)}) = L$ dits, where Y is the measurement result of the composite system $\mathcal{Q}_{B_k}\mathcal{Q}_{A_k}$. Therefore, $\min\left(\sum_{s\in[S]} \log_d |\mathcal{Q}_s|, 2\sum_{s\in\mathcal{B}_k} \log_d |\mathcal{Q}_s|\right) \geq L \implies \min\left(\sum_{s\in[S]} \Delta_s, \sum_{s\in\mathcal{B}_k} 2\Delta_s\right) \geq 1, \forall k \in [K]$. Since $\sum_{s\in[S]} \Delta_s$ does not depend on k, the condition is equivalent to that in (10).

V. Conclusion

The Σ-QMAC is an elementary and idealized setting to explore the potential for distributed superdense coding gain. As such its sharp capacity characterization is a promising step towards future generalizations, e.g., towards noisy quantum channels, generalized models for limited entanglements, and generalized distributed function computations. The sufficiency of the N-sum box abstraction for the Σ-QMAC is also promising, and further generalizations will reveal the limitations of this abstraction.

Acknowledgment

The authors gratefully acknowledge helpful discussions with Matteo Allaix from Aalto University and Yuxiang Lu from UC Irvine.

Appendix

The proof is by construction. We make use of the Generalized Reed Solomon (GRS) code. Let $\mathbb{F}_q$ be a field. $n, k \in \mathbb{N}$ such that $k \leq n$. $\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_n) \in \mathbb{F}_q^n$, $\boldsymbol{u} = (u_1, \cdots, u_n) \in \mathbb{F}_q^n$, such that $\alpha_i \neq \alpha_j$ for $i \neq j$ and $u_i \neq 0$ for $i \in [n]$. This requires that $q \geq n$. Define $\mathrm{GRS}_{k,n}^q(\boldsymbol{\alpha}, \mathbf{u})$ as the $k \times n$ generator matrix of an $[n, k]$ GRS code over $\mathbb{F}_q$, whose $(i,j)^{th}$ element is $u_j \alpha_j^{i-1}$. GRS codes have the properties [16] that (1) GRS codes are MDS, i.e., any k columns of the matrix $\mathrm{GRS}_{k,n}^q(\boldsymbol{\alpha}, \boldsymbol{u})$ are linearly independent, and (2) the dual code of an GRS code is also a GRS code, i.e., there exists $\boldsymbol{v} = (v_1, v_2, \cdots, v_n) \in \mathbb{F}_q^n$, $v_i \neq 0$ for $i \in [n]$ such that

$$\mathrm{GRS}_{k,n}^q(\boldsymbol{\alpha}, \mathbf{u}) \cdot \mathrm{GRS}_{n-k,n}^q(\boldsymbol{\alpha}, \boldsymbol{v})^T = \mathbf{0}_{k\times(n-k)}. \tag{22}$$

Note that $\lceil N/2 \rceil + \lfloor N/2 \rfloor = N$. Given $q \geq N$, define

$$\mathbf{M} = \begin{bmatrix} \mathrm{GRS}_{\lceil N/2\rceil,N}^q(\boldsymbol{\alpha}, \boldsymbol{u}) & \mathbf{0}_{\lceil N/2\rceil\times N} \\ \mathbf{0}_{\lfloor N/2\rfloor\times N} & \mathrm{GRS}_{\lfloor N/2\rfloor,N}^q(\boldsymbol{\alpha}, \boldsymbol{v}) \end{bmatrix} \in \mathbb{F}_q^{N\times 2N}. \tag{23}$$

We claim that this $\mathbf{M}$ is half-MDS and it is a valid transfer matrix of an N-sum box. Let us first verify that it is a valid transfer matrix of an N-sum box.

$$\begin{aligned}
&(\mathbf{M}\mathbf{J}_{2N})\mathbf{M}^T \\
&= \begin{bmatrix} \mathbf{0}_{\lceil N/2\rceil\times N} & -\mathrm{GRS}(\boldsymbol{\alpha}, \boldsymbol{u}) \\ \mathrm{GRS}(\boldsymbol{\alpha}, \boldsymbol{v}) & \mathbf{0}_{\lfloor N/2\rfloor\times N} \end{bmatrix} \begin{bmatrix} \mathrm{GRS}(\boldsymbol{\alpha}, \boldsymbol{u}) & \mathbf{0}_{\lceil N/2\rceil\times N} \\ \mathbf{0}_{\lfloor N/2\rfloor\times N} & \mathrm{GRS}(\boldsymbol{\alpha}, \boldsymbol{v}) \end{bmatrix}^T \\
&= \begin{bmatrix} \mathbf{0}_{\lceil N/2\rceil\times\lceil N/2\rceil} & -\mathrm{GRS}(\boldsymbol{\alpha}, \boldsymbol{u}) \cdot \mathrm{GRS}(\boldsymbol{\alpha}, \boldsymbol{v})^T \\ \mathrm{GRS}(\boldsymbol{\alpha}, \boldsymbol{v}) \cdot \mathrm{GRS}(\boldsymbol{\alpha}, \boldsymbol{u})^T & \mathbf{0}_{\lfloor N/2\rfloor\times\lfloor N/2\rfloor} \end{bmatrix} \\
&= \mathbf{0}_{N\times N}
\end{aligned} \tag{24}$$

Finally, since GRS codes are MDS, it follows that the $\mathbf{M}$ constructed in (23) is half-MDS. □

References

[1] M. A. Sohail, T. A. Atif, and S. S. Pradhan, "Unified approach for computing sum of sources over CQ-MAC," in *2022 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2022, pp. 1868–1873.

[2] M. A. Sohail, T. A. Atif, A. Padakandla, and S. S. Pradhan, "Computing sum of sources over a classical-quantum MAC," *IEEE Transactions on Information Theory*, vol. 68, no. 12, pp. 7913–7934, 2022.

[3] 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.

[4] 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.

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

[6] 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.

[7] S. Song and M. Hayashi, "Capacity of quantum symmetric private information retrieval with collusion of all but one of servers," *IEEE Journal on Selected Areas in Information Theory*, vol. 2, no. 1, pp. 380–390, 2021.

[8] C. H. Bennett and S. J. Wiesner, "Communication via one-and two-particle operators on Einstein-Podolsky-Rosen states," *Physical review letters*, vol. 69, no. 20, p. 2881, 1992.

[9] 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

[10] 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.

[11] 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.

[12] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[13] 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.

[14] S. Massar, S. Pironio, and D. Pitalúa-García, "Hyperdense coding and superadditivity of classical capacities in hypersphere theories," *New Journal of Physics*, vol. 17, no. 11, p. 113002, 2015.

[15] M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Żukowski, "Information causality as a physical principle," *Nature*, vol. 461, no. 7267, pp. 1101–1104, 2009.

[16] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*. Elsevier, 1977, vol. 16.