Title

N-Sum Box: An Abstraction for Linear Computation over Many-to-one Quantum Networks

Authors

Allaix, Matteo
Lu, Yuxiang
Yao, Yuhang
et al.

Publication Date

2023-04-17

N-Sum Box: An Abstraction for Linear Computation over Many-to-one Quantum Networks

Matteo Allaix *, Yuxiang Lu †, Yuhang Yao †, Tefjol Pllaha ‡, Camilla Hollanti *, Syed Jafar †
* Aalto University, Finland. E-mails: {matteo.allaix, camilla.hollanti}@aalto.fi
† University of California, Irvine, CA, USA. E-mails: {yuxianl7, yuhangy5, syed}@uci.edu
‡ University of Nebraska, Lincoln, NE, USA. E-mail: tefjol.pllaha@unl.edu

***Abstract*—Linear computations over quantum many-to-one communication networks offer opportunities for communication cost improvements through schemes that exploit quantum entanglement among transmitters to achieve superdense coding gains, combined with classical techniques such as interference alignment. The problem becomes much more broadly accessible if suitable abstractions can be found for the underlying quantum functionality via classical black box models. This work formalizes such an abstraction in the form of an "N-sum box", a black box generalization of a two-sum protocol of Song *et al.* with recent applications to N-servers private information retrieval. The N-sum box has communication cost of N qudits and classical output of a vector of N q-ary digits linearly dependent (via an $N \times 2N$ transfer matrix) on $2N$ classical inputs distributed among N transmitters. We characterize which transfer matrices are feasible by our construction, both with and without the possibility of additional locally invertible classical operations at the transmitters and receivers.**

I. INTRODUCTION

Distributed computation networks are often limited by their communication costs. Improving the efficiency of distributed computation by reducing communication costs is an active area of research. Reductions in communication cost may be achieved by coding techniques that are specialized for the type of distributed computation task (e.g., aggregation [1], MapReduce [2], matrix multiplication [3]) as well as the nature of the communication network (wireless [1], cable [4], optical fiber [5], quantum networks [6]). For instance, coding for over-the-air computation reduces the communication cost of linear computation over many-to-one wireless networks, by taking advantage of the natural superposition property of the wireless medium [1].

This work was carried out while M. Allaix was visiting the research group of S. Jafar at University of California, Irvine.

C. Hollanti and M. Allaix were supported by the Academy of Finland, under Grant No. 318937. M. Allaix was also supported by a doctoral research grant from the Emil Aaltonen Foundation, Finland.

Y. Lu, Y. Yao and S. Jafar were supported by grants NSF CCF-1907053 and CCF-2221379 and ONR N00014-21-1-2386.

Our focus in this work is on linear computations over *quantum* many-to-one communication networks. The potential for reduced communication costs in this setting comes from quantum-entanglement among the transmitters, which creates opportunities for superdense coding gains [7]–[10] as well as classical techniques such as interference alignment. However, unlike wireless networks for which there exists an abundance of simplified channel models and abstractions to facilitate analysis from coding, information-theoretic and signal-processing perspectives [11]–[13], similarly convenient abstractions of quantum communication networks are not readily available, which limits the study of quantum communication networks largely to quantum-experts. Our work is motivated by the observation that a convenient abstraction for linear computation over quantum many-to-one networks is indeed available, although somewhat implicitly, in the works of Song *et al.*, in the form of a quantum two-sum protocol [14], and its subsequent generalizations as applied to QPIR [14]–[20]. The main contribution of our work is to crystallize this abstraction and explore its scope and limitations. What we present is a black box generalization of the two-sum protocol, involving N qudits instead of 2 qubits, in short, an "N-sum box".

The two-sum protocol [14] is shown in Fig. 1, both as a quantum circuit and as a black box. In the quantum circuit, we see two transmitters (Tx1 and Tx2), each in possession of one qubit of an entangled pair. The entangled state in this case is

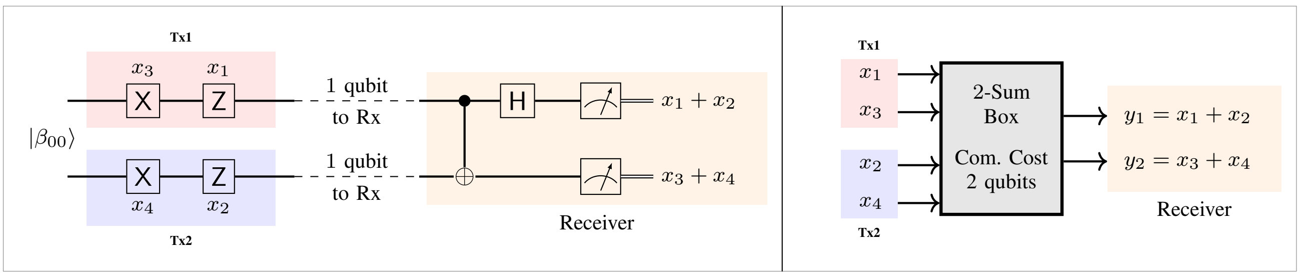

Fig. 1. Quantum circuit and black box representation for two-sum transmission protocol with $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

the Bell state $|\beta_{00}\rangle$. As classical 2-bit inputs become available to the two transmitters ((x_1, x_3) to Tx1, (x_2, x_4) to Tx2), they perform conditional quantum operations (X, Z gates) on their respective qubits and then send them to the receiver, for a total communication cost of 2 qubits. The receiver performs a Bell measurement and obtains $(y_1, y_2) = (x_1 + x_2, x_3 + x_4)$. The two-sum protocol can be abstracted into a black box, also shown in Fig. 1, with inputs $(x_1, x_3), (x_2, x_4)$ controlled by Tx1 and Tx2, respectively, and output $\mathbf{y} = \mathbf{M}\mathbf{x}$, where $\mathbf{M} = \left(\begin{smallmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{smallmatrix}\right)$ is the *transfer matrix* of this 2-sum box and $\mathbf{x}^\top = \big(x_1, x_2, x_3, x_4\big)$. The black box representation hides the details of the quantum circuit and specifies only the functionality (transfer matrix $\mathbf{M}$) and the communication cost (2 qubits), which makes it possible for non-quantum-experts to design low-communication-cost coding schemes for quantum communication networks using this black box, *e.g.*, to take advantage of super-dense coding. Note that in the two-sum protocol, if Tx1 uses only zeros for its data ($x_1 = x_3 = 0$), then the protocol allows Tx2 to send both its classical input bits (x_2, x_4) to the receiver, even though it sends only one qubit, provided Tx1 sends its qubit to the receiver as well. This is an example of superdense coding, made possible by the entanglement between the two qubits. Indeed, without the entanglement, qubits are worth no more than classical bits by the Holevo bound [21].

The generalization of the 2-sum box to the N-sum box is based on the stabilizer formalism [22], and similarly allows designs of classical coding schemes at larger scales that take advantage of the quantum entanglement implied by the N-sum box without the need to deal directly with the underlying quantum-circuits. Feasible N-sum box transfer functions turn out to be precisely those transfer matrices $\mathbf{M} \in \mathbb{F}_q^{N \times 2N}$ that are either strongly self-orthogonal themselves (cf. Def. 3), or can be made strongly self-orthogonal by locally invertible transformations (cf. Def. 1) at various transmitters and/or the receiver. Existing results on the capacity of QPIR become much more accessible when seen through the lens of the N-sum box. The simplicity of the N-sum box will facilitate coding schemes employing interference alignment/cancelation for computation over quantum communication networks, *e.g.*, various forms of quantum private information retrieval, quantum secure distributed matrix multiplication, and quantum linear computation multiple-access, without the need for concern about the details of quantum computation.

The N-sum box presented in this work is based on the stabilizer formalism that originates in quantum error correction coding literature [22]–[25]. As a caveat, we cannot rule out that there may exist other constructions different from ours, that are capable of producing N-sum boxes with transfer functions that are not feasible with our construction and locally invertible transformations (cf. Sec. IV). On the other hand, we are not aware of any such (implicit or explicit) constructions in the existing literature on quantum linear error correcting codes. We are cautiously optimistic that the stabilizer-based construction exhausts the scope of the N-sum box functionality, which would make it an object of fundamental interest to study the information-theoretic limits of transmitter-side entanglement-assisted distributed linear computation over quantum many-to-one communication networks.

Notation. We denote by $[N]$ the set $\{1, \ldots, N\}$, $n \in \mathbb{N}$, and by $\mathbb{F}_q$ the finite field with q elements. We use bold lower-case letters and bold upper-case letters to denote vectors and matrices, respectively. Given a matrix $\mathbf{A}$, $\langle \mathbf{A} \rangle_{\mathsf{row}}$ and $\langle \mathbf{A} \rangle_{\mathsf{col}}$ denote the spaces spanned by the rows and columns of $\mathbf{A}$, respectively, while $\mathbf{A}^\top$ and $\mathbf{A}^\dagger$ represent its transpose and its conjugate transpose, respectively.

II. Stabilizer formalism over finite fields

Stabilizer formalism [22] is a compact framework for quantum computation that provides a useful bridge to classical computation. Recently, this framework has been leveraged to boost several classical protocols. We first describe the stabilizer formalism over a finite field, for the details of which we refer the reader to [23], [24]. Throughout, we will use the same notation as in [19].

Let $q = p^r$ with a prime number p and a positive integer r. Let $\mathcal{H}$ be a q-dimensional Hilbert space spanned by orthonormal states $\{|j\rangle \mid j \in \mathbb{F}_q\}$. For $x \in \mathbb{F}_q$, we define $\mathbf{T}_x$ on $\mathbb{F}_p^r$ as the linear map $y \mapsto xy \in \mathbb{F}_q$, $y \in \mathbb{F}_q$, by identifying the finite field $\mathbb{F}_q$ with the vector space $\mathbb{F}_p^r$. Let $\operatorname{tr} x := \operatorname{Tr} \mathbf{T}_x \in \mathbb{F}_p$ for $x \in \mathbb{F}_q$. Let $\omega := \exp(2\pi i/p)$. For $a, b \in \mathbb{F}_q$, we define unitary matrices $\mathsf{X}(a) := \sum_{j \in \mathbb{F}_q} |j + a\rangle\langle j|$ and $\mathsf{Z}(b) := \sum_{j \in \mathbb{F}_q} \omega^{\operatorname{tr} bj} |j\rangle\langle j|$ on $\mathcal{H}$. For $\mathbf{s} = (s_1, \ldots, s_{2N}) \in \mathbb{F}_q^{2N}$, we define a unitary matrix $\tilde{\mathbf{W}}(\mathbf{s}) := \mathsf{X}(s_1)\mathsf{Z}(s_{N+1}) \otimes \cdots \otimes \mathsf{X}(s_N)\mathsf{Z}(s_{2N})$ on $\mathcal{H}^{\otimes N}$.

For $\mathbf{x} = (x_1, \ldots, x_N)$, $\mathbf{y} = (y_1, \ldots, y_N) \in \mathbb{F}_q^N$, we define the tracial bilinear form $\langle \mathbf{x}, \mathbf{y} \rangle := \operatorname{tr} \sum_{i=1}^N x_i y_i \in \mathbb{F}_p$ and the trace-symplectic bilinear form $\langle \mathbf{x}, \mathbf{y} \rangle_{\mathbb{S}} := \langle \mathbf{x}, \mathbf{J}\mathbf{y} \rangle$, where $\mathbf{J}$ is a $2N \times 2N$ matrix $\mathbf{J} = \left(\begin{smallmatrix} \mathbf{0} & -\mathbf{I} \\ \mathbf{I} & \mathbf{0} \end{smallmatrix}\right)$. The dual of a subspace $\mathcal{V}$ of $\mathbb{F}_q^{2N}$ with respect to this form is $\mathcal{V}^{\perp_{\mathbb{S}}} := \{\mathbf{s} \in \mathbb{F}_q^{2N} \mid \langle \mathbf{v}, \mathbf{s} \rangle_{\mathbb{S}} = 0 \text{ for any } \mathbf{v} \in \mathcal{V}\}$.

A matrix $\mathbf{F} \in \mathbb{F}_q^{2N \times 2N}$ is called *symplectic* if $\mathbf{F}^\top \mathbf{J} \mathbf{F} = \mathbf{J}$. Symplectic matrices are precisely those matrices that preserve $\langle \cdot, \cdot \rangle_{\mathbb{S}}$, and its columns form a symplectic basis for $\mathbb{F}_q^{2N}$. If we write $\mathbf{F} = \left(\begin{smallmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{B} & \mathbf{D} \end{smallmatrix}\right)$, then $\mathbf{F}$ is symplectic if and only if $\mathbf{B}^\top \mathbf{A}, \mathbf{D}^\top \mathbf{C}$ are symmetric and $\mathbf{A}^\top \mathbf{D} - \mathbf{B}^\top \mathbf{C} = \mathbf{I}$. Thus,

$$\mathbf{F}^{-1} = \mathbf{J}^\top \mathbf{F}^\top \mathbf{J} = \begin{pmatrix} \mathbf{D}^\top & -\mathbf{C}^\top \\ -\mathbf{B}^\top & \mathbf{A}^\top \end{pmatrix}. \tag{1}$$

The *Heisenberg-Weyl group* is defined as $\mathrm{HW}_q^N := \Big\{ c\tilde{\mathbf{W}}(\mathbf{s}) \mid \mathbf{s} \in \mathbb{F}_q^{2N},\ c \in \mathbb{C} \setminus \{0\} \Big\}$. There is a surjective homomorphism $c\tilde{\mathbf{W}}(\mathbf{s}) \in \mathrm{HW}_q^N \mapsto \mathbf{s} \in \mathbb{F}_q^{2N}$ with kernel $\{c\mathbf{I}_{q^N} \mid c \in \mathbb{C} \setminus \{0\}\}$. Two matrices $c_1\tilde{\mathbf{W}}(\mathbf{s}_1), c_2\tilde{\mathbf{W}}(\mathbf{s}_2)$ commute if and only if $\langle \mathbf{s}_1, \mathbf{s}_2 \rangle_{\mathbb{S}} = 0$, and thus commutativity in HW_q^N is equivalent to orthogonality in $\mathbb{F}_q^{2N}$.

A commutative subgroup of HW_q^N not containing $c\mathbf{I}_{q^N}$ for any $c \neq 1$ is called a *stabilizer group*. Such groups are precisely those groups for which the aforementioned homomorphism is actually an isomorphism. Thus, a stabilizer group defines a *self-orthogonal subspace*, that is $\mathcal{V} \subseteq \mathcal{V}^{\perp_{\mathbb{S}}}$, in

$\mathbb{F}_q^{2N}$. Conversely, given a self-orthogonal subspace $\mathcal{V}$ of $\mathbb{F}_q^{2N}$, there exist complex numbers $c_{\mathbf{v}}$ so that

$$\mathcal{S}(\mathcal{V}) := \{\mathbf{W}(\mathbf{v}) := c_{\mathbf{v}}\tilde{\mathbf{W}}(\mathbf{v}) \mid \mathbf{v} \in \mathcal{V}\} \subseteq \mathrm{HW}_q^N \qquad (2)$$

forms a stabilizer group. Thus, there is a one-to-one correspondence between stabilizer groups in HW_q^N and self-orthogonal subspaces in $\mathbb{F}_q^{2N}$.

Throughout this paper, we will consider only *maximal* stabilizers, since we expect that they exhaust the scope of all possible stabilizer-based N-sum boxes (cf. Remark 6). Maximal stabilizers are in one-to-one correspondence with *strongly self-orthogonal (SSO) subspaces*, *i.e.*, $\mathcal{V} = \mathcal{V}^{\perp_{\mathbb{S}}}$, so $\dim(\mathcal{V}) = N$.

While $\mathcal{V}$ defines the stabilizer $\mathcal{S}(\mathcal{V})$, the quotient space $\mathbb{F}_q^{2N}/\mathcal{V}^{\perp_{\mathbb{S}}}$ defines orthogonal projectors

$$\mathcal{P}^{\mathcal{V}} := \{\mathbf{P}_{\overline{\mathbf{s}}}^{\mathcal{V}} \mid \overline{\mathbf{s}} \in \mathbb{F}_q^{2N}/\mathcal{V}^{\perp_{\mathbb{S}}}\} \qquad (3)$$

which we use as a projective-value measurement (PVM). We will denote $|\overline{\mathbf{s}}\rangle$ the state which $\mathbf{P}_{\overline{\mathbf{s}}}^{\mathcal{V}}$ projects onto.

Measuring with $\mathcal{P}^{\mathcal{V}}$ would yield a coset. The next proposition aims to clarify the notation of [19, Prop. 2.2] (cf. App. A) by giving a unique representative of the outputted equivalence class.

Proposition 1: Let $\mathbf{G} \in \mathbb{F}_q^{2N\times N}$ be such that

1) $\mathbf{G}^\top \mathbf{J}\mathbf{G} = \mathbf{0}$,
2) there exists $\mathbf{H} \in \mathbb{F}_q^{2N\times N}$ such that $\begin{pmatrix}\mathbf{G} & \mathbf{H}\end{pmatrix}$ is full rank.

Let $\mathcal{V} = \langle \mathbf{G}\rangle_{\mathsf{col}}$ and $(\cdot)_h : \mathbb{F}_q^{2N} \to \mathbb{F}_q^N$ be such that

$$(\mathbf{x})_h := \begin{pmatrix}\mathbf{0} & \mathbf{I}\end{pmatrix}\begin{pmatrix}\mathbf{G} & \mathbf{H}\end{pmatrix}^{-1}\mathbf{x}.$$

Then performing the PVM $\{\mathbf{P}_{\overline{\mathbf{s}}}^{\mathcal{V}} \mid \overline{\mathbf{s}} \in \mathbb{F}_q^{2N}/\mathcal{V}^{\perp_{\mathbb{S}}}\}$ on the state $|\overline{\mathbf{x}}\rangle$ gives the outcome $(\mathbf{x})_h$.

Proof: Since by condition 1 we have $\langle \mathbf{v}_i, \mathbf{v}_j\rangle_{\mathbb{S}} = 0$ for any pair of column vectors $\mathbf{v}_i, \mathbf{v}_j$ of $\mathbf{G}$, $i, j \in [N]$, it follows that the symplectic inner product of any pair of linear combinations of column vectors of $\mathbf{G}$ is zero. This implies that $\mathcal{V} \subseteq \mathcal{V}^{\perp_{\mathbb{S}}}$, and since $\mathbf{G}$ has rank N, we have that $\dim(\mathcal{V}) = N$. It follows that $\dim(\mathcal{V}^{\perp_{\mathbb{S}}}) = N$ and $\mathcal{V} = \mathcal{V}^{\perp_{\mathbb{S}}}$. Then the subgroup $\mathcal{S}(\mathcal{V})$ as in Eq. (2) is a stabilizer, and since $\mathcal{V}$ has dimension N, it is maximal. Furthermore, $\mathcal{H}^{\otimes N} = \mathcal{W}$ [19, Eq. (5)], where $\mathcal{W}$ is the q^N-dimensional Hilbert space spanned by $\{|\overline{\mathbf{s}}\rangle \mid \overline{\mathbf{s}} \in \mathbb{F}_q^{2N}/\mathcal{V}^{\perp_{\mathbb{S}}}\}$.

Let $\mathbf{x} \in \mathbb{F}_q^{2N}$. By condition 2, we can uniquely decompose $\mathbf{x}$ as $\mathbf{x} = \mathbf{G}\mathbf{x}_g + \mathbf{H}\mathbf{x}_h,\ \mathbf{x}_h, \mathbf{x}_g \in \mathbb{F}_q^N$. Notice now that $(\mathbf{x})_h = \mathbf{x}_h$ and $(\mathbf{x}+\mathbf{g})_h = \mathbf{x}_h$ for any $\mathbf{g} \in \mathcal{V}$. Since $\overline{\mathbf{s}} = \mathbf{s} + \mathcal{V}^{\perp_{\mathbb{S}}} = \mathbf{s} + \mathcal{V} = \{\mathbf{s}+\mathbf{g} \mid \mathbf{g} \in \mathcal{V}\}$, it follows that every $\mathbf{x} \in \overline{\mathbf{s}}$ maps to a unique element $\mathbf{s}_h \in \mathbb{F}_q^N$. Thus, we can identify each coset $\overline{\mathbf{s}}$ with the element $\mathbf{s}_h$. Then we identify the states

$$|\mathbf{s}_h\rangle_{\mathcal{W}} = |\overline{\mathbf{s}}\rangle \qquad (4)$$

to avoid confusion with the computational basis, since $\mathcal{W}$ is the space spanned by the states $|\overline{\mathbf{s}}\rangle$.

In the decomposition given by [19, Eq. (5)] there are q^N distinct elements, since each $\mathcal{H}_{\overline{\mathbf{s}}}^{\mathcal{V}}$ has dimension 1. There are q^N vectors $\mathbf{s}_h \in \mathbb{F}_q^N$, so we can write [19, Eq. (2)] as $\mathbf{W}(\mathbf{v}) = \sum_{\mathbf{s}_h \in \mathbb{F}_q^N} \omega^{\langle \mathbf{v}, \mathbf{H}\mathbf{s}_h\rangle_{\mathbb{S}}} \mathbf{P}_{\mathbf{s}_h}^{\mathcal{V}}$, where $\mathbf{P}_{\mathbf{s}_h}^{\mathcal{V}}$ is the projection associated with the measurement outcome $\mathbf{s}_h$. Since $\dim(\operatorname{Im}\mathbf{P}_{\mathbf{s}_h}^{\mathcal{V}}) = 1$, we can decompose it as $\mathbf{P}_{\mathbf{s}_h}^{\mathcal{V}} := |\mathbf{s}_h\rangle_{\mathcal{W}}\langle \mathbf{s}_h|_{\mathcal{W}}$. Assuming that the system is in the state $|\overline{\mathbf{x}}\rangle$ for some $\overline{\mathbf{x}} \in \mathbb{F}_q^{2N}/\mathcal{V}_{\mathbb{S}}^{\perp}$, and since we can identify $\overline{\mathbf{x}}$ with a unique $\mathbf{x}_h \in \mathbb{F}_q^N$, we have that $\mathbf{P}_{\mathbf{s}_h}^{\mathcal{V}}|\overline{\mathbf{x}}\rangle = |\mathbf{s}_h\rangle_{\mathcal{W}}\langle \mathbf{s}_h|\mathbf{x}_h\rangle_{\mathcal{W}}$ equals $|\mathbf{x}_h\rangle_{\mathcal{W}}$ if $\mathbf{s}_h = \mathbf{x}_h$ and is 0 otherwise. We thus obtain $(\mathbf{x})_h$ with probability 1 after performing the PVM $\{\mathbf{P}_{\overline{\mathbf{s}}}^{\mathcal{V}} \mid \overline{\mathbf{s}} \in \mathbb{F}_q^{2N}/\mathcal{V}^{\perp_{\mathbb{S}}}\} = \{\mathbf{P}_{\mathbf{s}_h}^{\mathcal{V}} \mid \mathbf{s}_h \in \mathbb{F}_q^N\}$ on the state $|\overline{\mathbf{x}}\rangle$. ■

Remark 1: The PVM can be more clearly expressed as

$$\mathcal{P}^{\mathcal{V}} := \{\mathbf{P}_{\mathbf{s}_h}^{\mathcal{V}} = |\mathbf{s}_h\rangle_{\mathcal{W}}\langle \mathbf{s}_h|_{\mathcal{W}} \mid \mathbf{s}_h \in \mathbb{F}_q^N\}. \qquad (5)$$

III. N-SUM BOX

An N-sum box is a black box with the functional form $\mathbf{y} = \mathbf{M}\mathbf{x}$, where $\mathbf{y} \in \mathbb{F}_q^N$ is the output vector, $\mathbf{x} = (x_1, \ldots, x_{2N})^\top \in \mathbb{F}_q^{2N}$ is the input vector, and $\mathbf{M} \in \mathbb{F}_q^{N\times 2N}$ is the *transfer matrix*. The inputs to the N-sum box are controlled by N parties (*transmitters*), where transmitter $n \in [N]$ is controlling (x_n, x_{N+n}). The output vector $\mathbf{y}$ is measured by another party, which we label as the *receiver*. The N-sum box is initialized with shared quantum entanglement among the N transmitters, *i.e.*, each of N entangled q-dimensional qudits is supplied to a transmitter. The initial qudit entanglement is independent of the inputs $\mathbf{x}$ and any data that subsequently becomes available to the transmitters. No quantum resource is initially available to the receiver. In the course of operation of the N-sum box, each of the N transmitters acquires data from various sources, including possibly the receiver (*e.g.*, queries in private information retrieval), based on which it performs conditional X, Z-gate operations on its own qudits, and then sends its qudit to the receiver. The receiver performs a quantum measurement on the N qudits, from which he recovers $\mathbf{y}$.

In this setting, we allow the inputs (x_n, x_{n+N}) from each transmitter $n \in [N]$ to be transformed by an invertible matrix. This corresponds to multiplying the input vector by local invertible transformations, which are defined as follows.

Definition 1: Let $\mathrm{diag}_{N,\mathbb{F}_q}$ be the set of diagonal matrices of dimension $N \times N$ and entries in $\mathbb{F}_q$. The set of *local invertible transformations (LITs)* is defined as

$$\mathrm{LIT}_{N,\mathbb{F}_q} := \big\{\left(\begin{smallmatrix}\mathbf{\Lambda}_1 & \mathbf{\Lambda}_2\\ \mathbf{\Lambda}_3 & \mathbf{\Lambda}_4\end{smallmatrix}\right) \mid \mathbf{\Lambda}_i \in \mathrm{diag}_{N,\mathbb{F}_q},\ i \in [4],\ \det(\mathbf{\Lambda}_1\mathbf{\Lambda}_4 - \mathbf{\Lambda}_2\mathbf{\Lambda}_3) \neq 0\big\}.$$

We also allow *receiver invertible transformations*, *i.e.*, we allow the receiver to transform the output vector of the N-sum box by multiplying it by $\mathbf{P} \in \mathrm{GL}_{N,\mathbb{F}_q}$, where $\mathrm{GL}_{N,\mathbb{F}_q}$ is the set of invertible matrices with dimension N and entries in $\mathbb{F}_q$. This gives equivalent representations of the N-sum box as

$$\mathbf{y} = \mathbf{P}\mathbf{M}\mathbf{\Lambda}\mathbf{x}, \quad \mathbf{P} \in \mathrm{GL}_{N,\mathbb{F}_q},\ \mathbf{\Lambda} \in \mathrm{LIT}_{N,\mathbb{F}_q}.$$

Definition 2: The relation $\overset{\mathrm{LIT}}{\equiv}$ defines an equivalence class of pairs of matrices $\mathbf{M}_1, \mathbf{M}_2 \in \mathbb{F}_q^{N\times 2N}$ up to local and receiver invertible transformations, *i.e.*,

$$\mathbf{M}_1 \overset{\mathrm{LIT}}{\equiv} \mathbf{M}_2 \iff \mathbf{M}_1 = \mathbf{P}\mathbf{M}_2\mathbf{\Lambda}.$$

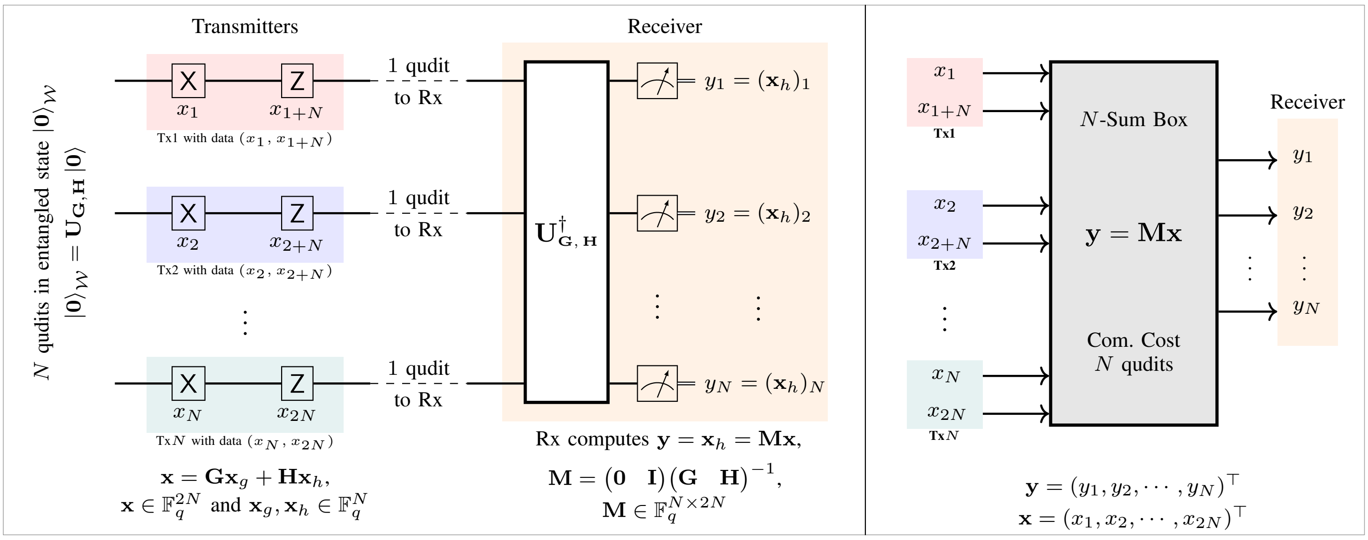

Fig. 2. Quantum circuit and black box representation for an N-sum box with transfer function $\mathbf{y} = \mathbf{M}\mathbf{x}$.

IV. Stabilizer-based N-sum boxes

First, we define SSO matrices, which are used in the construction of N-sum boxes based on stabilizer formalism.

Definition 3: A matrix $\mathbf{M} \in \mathbb{F}_q^{2N\times N}$ is said to be *strongly self-orthogonal (SSO)* if its columns span an SSO subspace, or equivalently, if $\mathbf{M}^\top\mathbf{J}\mathbf{M} = \mathbf{0}$ and $\mathrm{rank}(\mathbf{M}) = N$. The set of SSO matrices is denoted by $\mathcal{M}_o$.

Remark 2: If $\mathbf{F} \in \mathbb{F}_q^{2N\times 2N}$ is a symplectic matrix, then its left-half $\mathbf{F}\left(\begin{smallmatrix}\mathbf{I}\\ \mathbf{0}\end{smallmatrix}\right)$ is an SSO matrix. Conversely, an SSO matrix can be completed to a symplectic matrix (*e.g.*, using the Gram-Schmidt Algorithm).

Let us now characterize some classes of N-sum boxes that can be constructed based on the stabilizer formalism.

A. Case with disallowed LITs

The following theorem describes which transfer matrices are feasible from a stabilizer-based construction when LITs are disallowed.

Theorem 1: Suppose there exists $\mathbf{G} \in \mathbb{F}_q^{2N\times N}$ such that

1) $\mathbf{G} \in \mathcal{M}_o$,
2) there exists $\mathbf{H} \in \mathbb{F}_q^{2N\times N}$ such that $\begin{pmatrix}\mathbf{G} & \mathbf{H}\end{pmatrix}$ is full rank,
3) $\mathbf{M} \in \mathbb{F}_q^{N\times 2N}$ is the submatrix comprised of the bottom N rows of $\begin{pmatrix}\mathbf{G} & \mathbf{H}\end{pmatrix}^{-1}$, *i.e.*, $\mathbf{M} := \begin{pmatrix}\mathbf{0} & \mathbf{I}\end{pmatrix}\begin{pmatrix}\mathbf{G} & \mathbf{H}\end{pmatrix}^{-1}$.

Then there exists a stabilizer-based construction for an N-sum box over $\mathbb{F}_q$ with transfer matrix $\mathbf{M}$.

Proof: Let $\mathbf{U}_{\mathbf{G},\mathbf{H}} \in \mathbb{C}^{q^N\times q^N}$ be the unitary matrix such that its i^{th} column is the vector representing the state $|\nu(i)\rangle_{\mathcal{W}}$, $i \in [q^N]$, identified by Eq. (4), where $\nu : [q^N] \to \mathbb{F}_q^N$ is the natural isomorphism (cf. Remark 5). Let $|\mathbf{0}\rangle_{\mathcal{W}} = \mathbf{U}_{\mathbf{G},\mathbf{H}}|\mathbf{0}\rangle$ be the initial entangled state over $\mathcal{H}^{\otimes N}$. Let $\mathcal{V} = \langle\mathbf{G}\rangle_{\mathsf{col}}$. If transmitter $n \in [N]$ applies $\mathsf{X}(x_n), \mathsf{Z}(x_{N+n})$ on his qudit and sends it to the receiver, then the received qudit is in the state $\mathbf{W}(\mathbf{x})|\mathbf{0}\rangle_{\mathcal{W}} = |(\mathbf{x})_h\rangle_{\mathcal{W}}$. After performing the PVM $\mathcal{P}^{\mathcal{V}}$ (cf. Eq. (5)) on the qudits the receiver measures $(\mathbf{x})_h$ without error by Prop. 1. Let $\mathbf{M}$ be as in condition 3, then we have that $\mathbf{M}\mathbf{x} = \mathbf{x}_h$, which is the output of the measurement. ■

Remark 3: The terminology "stabilizer-based construction" stems from the aforementioned correspondence between maximal stabilizers and SSO spaces. Explicitly, let $\mathbf{s}_i \in \mathbb{F}_q^{2N}$, $i \in [N]$, and let $\mathcal{S} = \langle\mathbf{W}(\mathbf{s}_1), \ldots, \mathbf{W}(\mathbf{s}_N)\rangle \subseteq \mathrm{HW}_q^N$ be a maximal stabilizer group, *i.e.*, a stabilizer group with N independent generators, where $|\mathbf{0}\rangle_{\mathcal{W}}$ is its stabilized state. Let $\mathbf{G} \in \mathbb{F}_q^{2N\times N}$ be the matrix that has $\mathbf{s}_i$ as its i^{th} column, then $\mathbf{G} \in \mathcal{M}_o$. For non-maximal stabilizers, see Remark 6.

Remark 4: A stabilizer-based construction for any feasible N-sum box is information-theoretically optimal as a black box implementation in the sense that it has the least possible quantum communication cost. In other words, since the transfer matrix is full rank, there cannot exist a less costly construction of the same N-sum box by some non-stabilizer-based means so that the output delivers N q-ary digits to the receiver, which cannot be done with a communication cost of less than N qudits by the Holevo bound [21].

We denote by $\mathcal{M}_{sbc}$ the set of all the transfer matrices resulting from stabilizer-based constructions with disallowed LITs. In the following, we establish that such set is the same as the set of SSO matrices, *i.e.*,

Lemma 1: $\mathcal{M}_o = \mathcal{M}_{sbc}$.

Proof: Let $\mathbf{M} \in \mathbb{F}_q^{N\times 2N}$ be such that $\mathbf{M}^\top \in \mathcal{M}_{sbc}$. By condition 3 of Thm. 1 we have that $\mathbf{M}\mathbf{G} = \mathbf{0} = \mathbf{G}^\top\mathbf{J}\mathbf{G}$. Since $\mathrm{rank}(\mathbf{G}^\top\mathbf{J}) = N$ we have that $\langle\mathbf{M}\rangle_{\mathsf{row}} = \langle\mathbf{G}^\top\mathbf{J}\rangle_{\mathsf{row}}$, which implies that $\mathbf{M} = \mathbf{P}\mathbf{G}^\top\mathbf{J}$ for $\mathbf{P} \in \mathrm{GL}_{N,\mathbb{F}_q}$. Trivially $\mathbf{M}^\top = \mathbf{J}^\top\mathbf{G}\mathbf{P}^\top \in \mathcal{M}_o$, so we conclude that $\mathcal{M}_{sbc} \subseteq \mathcal{M}_o$.

Now, let $\mathbf{M} \in \mathbb{F}_q^{N\times 2N}$ be such that $\mathbf{M}^\top \in \mathcal{M}_o$. Let $\mathbf{N} \in \mathbb{F}_q^{N\times 2N}$ be such that $\begin{pmatrix}\mathbf{N}^\top & \mathbf{M}^\top\end{pmatrix}$ is full rank, then its inverse can be written as $\begin{pmatrix}\mathbf{G} & \mathbf{H}\end{pmatrix}$, where $\mathbf{G}, \mathbf{H} \in \mathbb{F}_q^{N\times 2N}$. Clearly, $\mathbf{M}\begin{pmatrix}\mathbf{G} & \mathbf{H}\end{pmatrix} = \begin{pmatrix}\mathbf{0} & \mathbf{I}\end{pmatrix}$, so by the same argument above it is easy to see that $\mathbf{G} \in \mathcal{M}_o$, *i.e.*, $\mathcal{M}_o \subseteq \mathcal{M}_{sbc}$. ■

Remark 5: Let $\mathbf{G} = \left(\begin{smallmatrix}\mathbf{A}\\ \mathbf{B}\end{smallmatrix}\right) \in \mathcal{M}_o$ and $\mathbf{H} = \left(\begin{smallmatrix}\mathbf{C}\\ \mathbf{D}\end{smallmatrix}\right)$ be such that $\mathbf{F} := \begin{pmatrix}\mathbf{G} & \mathbf{H}\end{pmatrix}$ is symplectic. By Eq. (1) we have $\begin{pmatrix}\mathbf{0} & \mathbf{I}\end{pmatrix}\mathbf{F}^{-1} = \begin{pmatrix}-\mathbf{B}^\top & \mathbf{A}^\top\end{pmatrix}$ which is again an SSO matrix. Lemma 1 implies that we only need to complete $\mathbf{G}$ to a symplectic matrix (instead of invertible). The well-known connection between symplectic matrices and the stabilizer formalism [25] allows for a simpler description of the matrix $\mathbf{U}_{\mathbf{G},\mathbf{H}}$, as the following example illustrates.

Example 1: Suppose we have two parties, Tx1 and Tx2, both possessing two bits (cf. Fig 1). The two-sum transmission protocol computes (x_1+x_2, x_3+x_4) starting with the state $|\beta_{00}\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, which is stabilized by $\mathcal{S} = \langle \mathbf{W}(0,0,1,1), \mathbf{W}(1,1,0,0)\rangle$. Consider

$$\mathbf{F} = \begin{pmatrix}\mathbf{G} & \mathbf{H}\end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix},$$

where $\mathbf{G}$ is determined by $\mathcal{S}$ and $\mathbf{H}$ is chosen so that $\mathbf{F}$ is a symplectic matrix. The symplectic matrix can be decomposed, *e.g.*, using the Bruhat decomposition [26], [27], as

$$\mathbf{F} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

The components correspond to quantum gates CNOT and a partial Hadamard $\mathsf{H} \otimes \mathsf{I}$ on the first qudit [28]. This is precisely the circuit $\mathbf{U}_{\mathbf{G},\mathbf{H}}$ for which $|\beta_{00}\rangle = \mathbf{U}_{\mathbf{G},\mathbf{H}}|00\rangle$. Using Eq. (1) we then obtain the transfer matrix

$$\mathbf{M} = \begin{pmatrix}\mathbf{0} & \mathbf{I}\end{pmatrix}\mathbf{F}^{-1} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix},$$

which is exactly the functional form of the two-sum transmission protocol. This approach allows for a straightforward generalization that computes $\mathbf{Mx}$ starting with the state $(|0..0\rangle + |1..1\rangle)/\sqrt{2}$, where

$$\mathbf{M} = \left(\begin{array}{c|c} 110\cdots00 & 000\cdots00 \\ 011\cdots00 & 000\cdots00 \\ \vdots & \vdots \\ 000\cdots11 & 000\cdots00 \\ \hline 000\cdots00 & 111\cdots11 \end{array}\right) \in \mathbb{F}_q^{N\times 2N}.$$

The following theorem fully characterizes N-sum boxes without LITs and follows directly from Thm. 1, Remark 3 and Lemma 1.

Theorem 2: Let $\mathbf{M} \in \mathcal{M}_o$. A construction based on a stabilizer $\mathcal{S} \subseteq \mathrm{HW}_q^N$ exists for an N-sum box over $\mathbb{F}_q$ with transfer matrix $\mathbf{M}^\top$ if and only if $\mathcal{S}$ is a maximal stabilizer.

Remark 6: For non-maximal stabilizers, one can create a K-sum box with *weakly* self-orthogonal transfer matrix $\mathbf{M} \in \mathbb{F}_q^{K\times 2N}$, *i.e.*, a matrix that spans a *(weakly) self-orthogonal subspace* [19], starting from a stabilizer group with K generators. This could be done, for instance, by first completing to a maximal stabilizer and then continuing the computation with communication cost of N qudits.

B. Case with allowed LITs

The following theorem shows that the transfer matrix of any $(\mathbf{G},\mathbf{H})$ construction is equivalent (up to LITs) to $\mathbf{G}^\perp$, *i.e.*, the null-space of $\mathbf{G}$, which can be represented as $\mathbf{G}^\perp := \mathbf{J}^\top\mathbf{G}$.

Theorem 3: Let $\mathbf{M} \in \mathbb{F}_q^{N\times 2N}$ be such that $\mathbf{M}^\top \in \mathcal{M}_{sbc}$. Then $\mathbf{M} \overset{\text{LIT}}{\equiv} \mathbf{G}^\top\mathbf{J} = (\mathbf{G}^\perp)^\top$.

Proof: This follows directly from the proof of Lemma 1, since we can write $\mathbf{M} = \mathbf{P}\mathbf{G}^\top\mathbf{J}$ for $\mathbf{P} \in \mathrm{GL}_{N,\mathbb{F}_q}$. ■

A known property of SSO matrices is that they can be written in the so-called *standard form* [29], *i.e.*, if $\mathbf{M} \in \mathcal{M}_o$ then there exist $\mathbf{P} \in \mathrm{GL}_{N,\mathbb{F}_q}$, $\mathbf{Q} \in \mathrm{GL}_{2N,\mathbb{F}_q}$ such that

$$\mathbf{P}\mathbf{M}^\top\mathbf{Q} = \begin{pmatrix}\mathbf{I} & \mathbf{S}\end{pmatrix}, \tag{6}$$

where $\mathbf{S}$ is a symmetric $N\times N$ matrix, *i.e.*, $\mathbf{S}^\top = \mathbf{S}$. We define the set of transfer matrices in standard form

$$\mathcal{M}_s := \{\mathbf{M} \in \mathbb{F}_q^{2N\times N} \mid \mathbf{M}^\top = \begin{pmatrix}\mathbf{I} & \mathbf{S}\end{pmatrix},\ \mathbf{S}^\top = \mathbf{S}\}.$$

The following lemma shows that any SSO matrix $\mathbf{M}$ can be transformed by at most N signed column-swapping operations into a matrix $\mathbf{M}' = \begin{pmatrix}\mathbf{M}'_l & \mathbf{M}'_r\end{pmatrix}^\top \in \mathcal{M}_o$ such that $\mathbf{M}'_l$ is full rank. For completeness, the proof is included in App. B.

Lemma 2: For any $\mathbf{M} \in \mathcal{M}_o$ there exists a diagonal matrix $\mathbf{\Sigma} \in \{0,1\}^{N\times N}$ such that

$$(\mathbf{M}')^\top = \mathbf{M}^\top \begin{pmatrix} \mathbf{I}-\mathbf{\Sigma} & \mathbf{\Sigma} \\ -\mathbf{\Sigma} & \mathbf{I}-\mathbf{\Sigma} \end{pmatrix} \overset{\text{LIT}}{\equiv} \mathbf{M}^\top, \tag{7}$$

$$\mathbf{M}' \in \mathcal{M}_o, \tag{8}$$

$$\det(\mathbf{M}'_l) \neq 0. \tag{9}$$

Our next result shows that with LITs, every feasible transfer matrix $\mathbf{M} \in \mathcal{M}_o$ has an equivalent representation in the standard form $\mathbf{M} \overset{\text{LIT}}{\equiv} \begin{pmatrix}\mathbf{I} & \mathbf{S}\end{pmatrix}$, where $\mathbf{S}^\top = \mathbf{S}$. Notice that in Eq. (6) the matrix $\mathbf{Q}$ is not necessarily an LIT. The contribution here is to show that the standard form remains valid when only LITs are allowed.

Theorem 4: For every $\mathbf{M} \in \mathcal{M}_{sbc}$ there exists $\mathbf{M}' \in \mathcal{M}_s$ such that $(\mathbf{M}')^\top \overset{\text{LIT}}{\equiv} \mathbf{M}^\top$. Conversely, $\mathcal{M}_s \subseteq \mathcal{M}_{sbc}$.

Proof: By Lemma 2 in Appendix B, there exists $\mathbf{M}' := \begin{pmatrix}\mathbf{M}'_l & \mathbf{M}'_r\end{pmatrix}^\top \in \mathcal{M}_o$ such that $\mathbf{M}^\top \overset{\text{LIT}}{\equiv} (\mathbf{M}')^\top$ and $\mathbf{M}'_l$ is full rank. Thus, $(\mathbf{M}'')^\top := (\mathbf{M}'_l)^{-1}(\mathbf{M}')^\top = \begin{pmatrix}\mathbf{I} & \mathbf{F}\end{pmatrix}$ and $\mathbf{M}'' \in \mathcal{M}_o$. It is trivial to see that $\mathbf{F}$ is symmetric, since $\mathbf{M}'' = \begin{pmatrix}\mathbf{I} & \mathbf{F}\end{pmatrix}^\top \in \mathcal{M}_o$, so we can conclude that $\mathbf{M}'' \in \mathcal{M}_s$.

The converse is trivial by Lemma 1. ■

Remark 7: The standard form is not unique up to LITs, *e.g.*,

$$\begin{aligned}\begin{pmatrix}\mathbf{I} & \mathbf{S}_1\end{pmatrix} &= \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix} \overset{\text{LIT}}{\equiv} \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix} \\ &\overset{\text{LIT}}{\equiv} \begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & -1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} = \begin{pmatrix}\mathbf{I} & \mathbf{S}_2\end{pmatrix}, \quad \mathbf{S}_2 \neq \mathbf{S}_1.\end{aligned}$$

Next, we define the set $\mathcal{M}_{\mathrm{LIT}}$ of all possible transfer matrices that we can obtain by applying LITs:

$$\mathcal{M}_{\mathrm{LIT}} := \left\{\mathbf{M} \in \mathbb{F}_q^{2N\times N} \mid \exists \mathbf{M}' \in \mathcal{M}_{sbc},\ \mathbf{M} \overset{\text{LIT}}{\equiv} \mathbf{M}'\right\}.$$

The following theorem shows that any $\mathbf{M} \in \mathcal{M}_{\mathrm{LIT}}$ is equivalent, up to LITs, to a transfer matrix in standard form.

Theorem 5: For every $\mathbf{M} \in \mathcal{M}_{\mathrm{LIT}}$ there exists $\mathbf{M}' \in \mathcal{M}_s$ such that $\mathbf{M}' \overset{\mathrm{LIT}}{\equiv} \mathbf{M}$. Conversely, for every $\mathbf{M}' \in \mathcal{M}_s$ there exists $\mathbf{M} \in \mathcal{M}_{\mathrm{LIT}}$ such that $\mathbf{M} \overset{\mathrm{LIT}}{\equiv} \mathbf{M}'$.

Proof: By definition, for every $\mathbf{M} \in \mathcal{M}_{\mathrm{LIT}}$ there exists $\mathbf{M}' \in \mathcal{M}_{sbc}$ such that $\mathbf{M}' \overset{\mathrm{LIT}}{\equiv} \mathbf{M}$. By Thm. 4 there exists $\mathbf{M}'' \in \mathcal{M}_s$ such that $\mathbf{M}'' \overset{\mathrm{LIT}}{\equiv} \mathbf{M}'$, and since the equivalence is transitive, we have that $\mathbf{M}'' \overset{\mathrm{LIT}}{\equiv} \mathbf{M}$.

The converse is trivial by the definitions. ■

REFERENCES

[1] B. Nazer and M. Gastpar, "Computation over multiple-access channels," *IEEE Transactions on information theory*, vol. 53, no. 10, pp. 3498–3516, 2007.

[2] J. Dean and S. Ghemawat, "MapReduce: simplified data processing on large clusters," *Communications of the ACM*, vol. 51, no. 1, pp. 107–113, 2008.

[3] Z. Jia and S. A. Jafar, "On the capacity of secure distributed batch matrix multiplication," *IEEE Transactions on Information Theory*, vol. 67, no. 11, pp. 7420–7437, 2021.

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

[5] M. Belzner and H. Haunstein, "Network coding in passive optical networks," in *2009 35th European Conference on Optical Communication*. IEEE, 2009, pp. 1–2.

[6] M. Hayashi, K. Iwama, H. Nishimura, R. Raymond, and S. Yamashita, "Quantum network coding," in *STACS 2007: 24th Annual Symposium on Theoretical Aspects of Computer Science, Aachen, Germany, February 22-24, 2007. Proceedings 24*. Springer, 2007, pp. 610–621.

[7] 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.

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

[9] X. S. Liu, G. L. Long, D. M. Tong, and F. Li, "General scheme for superdense coding between multiparties," *Physical Review A*, vol. 65, no. 2, p. 022304, 2002.

[10] V. N. Gorbachev, A. I. Trubilko, A. A. Rodichkina, and A. I. Zhiliba, "Teleportation and dense coding via a multiparticle quantum channel of the ghz-class." *Quantum Inf. Comput.*, vol. 2, no. 5, pp. 367–378, 2002.

[11] A. El Gamal and Y.-H. Kim, *Network information theory*. Cambridge university press, 2011.

[12] D. Tse and P. Viswanath, *Fundamentals of wireless communication*. Cambridge university press, 2005.

[13] A. Goldsmith, *Wireless communications*. Cambridge university press, 2005.

[14] S. Song and M. Hayashi, "Capacity of quantum private information retrieval with collusion of all but one of servers," in *2019 IEEE Information Theory Workshop (ITW)*. IEEE, 2019, pp. 1–5.

[15] ——, "Capacity of quantum private information retrieval with multiple servers," *IEEE Transactions on Information Theory*, vol. 67, no. 1, pp. 452–463, 2020.

[16] M. Allaix, L. Holzbaur, T. Pllaha, and C. Hollanti, "Quantum private information retrieval from coded and colluding servers," *IEEE Journal on Selected Areas in Information Theory*, vol. 1, no. 2, pp. 599–610, 2020.

[17] M. Allaix, L. Holzbaur, T. Pllaha, and C. Hollanti, "High-rate quantum private information retrieval with weakly self-dual star product codes," in *2021 IEEE International Symposium on Information Theory (ISIT)*, 2021, pp. 1046–1051.

[18] S. Song and M. Hayashi, "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] S. Song and M. Hayashi, "Quantum private information retrieval for quantum messages," in *2021 IEEE International Symposium on Information Theory (ISIT)*, 2021, pp. 1052–1057.

[21] 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.

[22] D. Gottesman, "Stabilizer codes and quantum error correction," 1997, PhD thesis, California Institute of Technology.

[23] A. Ashikhmin and E. Knill, "Nonbinary quantum stabilizer codes," *IEEE Transactions on Information Theory*, vol. 47, no. 7, pp. 3065–3072, 2001.

[24] S. K. A. Ketkar, A. Klappenecker and P. Sarvepalli, "Nonbinary stabilizer codes over finite fields," *IEEE Transactions on Information Theory*, vol. 52, no. 11, pp. 4892–4914, 2006.

[25] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction via codes over $\mathrm{GF}(4)$," *IEEE Trans. Inform. Theory*, vol. 44, no. 4, pp. 1369–1387, 1998.

[26] D. Maslov and M. Roetteler, "Shorter stabilizer circuits via Bruhat decomposition and quantum circuit transformations," *IEEE Transactions on Information Theory*, vol. 64, no. 7, pp. 4729–4738, 2018.

[27] T. Pllaha, O. Tirkkonen, and R. Calderbank, "Binary subspace chirps," *IEEE Transactions on Information Theory*, vol. 68, no. 12, pp. 7735–7752, 2022.

[28] T. Pllaha, N. Rengaswamy, O. Tirkkonen, and R. Calderbank, "Un-Weyling the Clifford Hierarchy," *Quantum*, vol. 4, p. 370, Dec. 2020.

[29] O. T. O'Meara, *Symplectic groups*, ser. Mathematical Surveys. American Mathematical Society, Providence, R.I., 1978, vol. 16.

APPENDIX A
PROP. 2.2, [19]

We denote the elements of the quotient space $\mathbb{F}_q^{2\mathsf{n}}/\mathcal{V}^{\perp_{\mathrm{S}}}$ by $\overline{\mathbf{s}} := \mathbf{s} + \mathcal{V}^{\perp_{\mathrm{S}}} \in \mathbb{F}_q^{2\mathsf{n}}/\mathcal{V}^{\perp_{\mathrm{S}}}$.

Let $\mathcal{V}$ be a d-dimensional self-orthogonal subspace of $\mathbb{F}_q^{2\mathsf{n}}$ and $\mathcal{S}(\mathcal{V})$ be a stabilizer defined from $\mathcal{V}$. Then, we obtain the following statements.

(a) For any $\mathbf{v} \in \mathcal{V}$, the operation $\mathbf{W}(\mathbf{v}) \in \mathcal{S}(\mathcal{V})$ is simultaneously and uniquely decomposed as

$$\mathbf{W}(\mathbf{v}) = \sum_{\overline{\mathbf{s}} \in \mathbb{F}_q^{2\mathsf{n}}/\mathcal{V}^{\perp_{\mathrm{S}}}} \omega^{\langle \mathbf{v}, \mathbf{s} \rangle_{\mathrm{S}}} \mathbf{P}_{\overline{\mathbf{s}}}^{\mathcal{V}} \tag{10}$$

with orthogonal projections $\{\mathbf{P}_{\overline{\mathbf{s}}}^{\mathcal{V}}\}$ such that

$$\mathbf{P}_{\overline{\mathbf{s}}}^{\mathcal{V}} \mathbf{P}_{\overline{\mathbf{t}}}^{\mathcal{V}} = \mathbf{0} \text{ for any } \overline{\mathbf{s}} \neq \overline{\mathbf{t}}, \tag{11}$$

$$\sum_{\overline{\mathbf{s}} \in \mathbb{F}_q^{2\mathsf{n}}/\mathcal{V}^{\perp_{\mathrm{S}}}} \mathbf{P}_{\overline{\mathbf{s}}}^{\mathcal{V}} = \mathbf{I}_{q^{\mathsf{n}}}. \tag{12}$$

(b) Let $\mathcal{H}_{\overline{\mathbf{s}}}^{\mathcal{V}} := \operatorname{Im} \mathbf{P}_{\overline{\mathbf{s}}}^{\mathcal{V}}$. We have $\dim \mathcal{H}_{\overline{\mathbf{s}}}^{\mathcal{V}} = q^{\mathsf{n}-d}$ for any $\overline{\mathbf{s}} \in \mathbb{F}_q^{2\mathsf{n}}/\mathcal{V}^{\perp_{\mathrm{S}}}$ and the quantum system $\mathcal{H}^{\otimes \mathsf{n}}$ is decomposed as

$$\mathcal{H}^{\otimes \mathsf{n}} = \bigotimes_{\overline{\mathbf{s}} \in \mathbb{F}_q^{2\mathsf{n}}/\mathcal{V}^{\perp_{\mathrm{S}}}} \mathcal{H}_{\overline{\mathbf{s}}}^{\mathcal{V}} = \mathcal{W} \otimes \mathbb{C}^{q^{\mathsf{n}-d}}, \tag{13}$$

where the system $\mathcal{W}$ is the q^d-dimensional Hilbert space spanned by $\{|\overline{\mathbf{s}}\rangle \mid \overline{\mathbf{s}} \in \mathbb{F}_q^{2\mathsf{n}}/\mathcal{V}^{\perp_{\mathrm{S}}}\}$ with the property $\mathcal{H}_{\overline{\mathbf{s}}}^{\mathcal{V}} = |\overline{\mathbf{s}}\rangle \otimes \mathbb{C}^{q^{\mathsf{n}-d}} := \{|\overline{\mathbf{s}}\rangle \otimes |\psi\rangle \mid |\psi\rangle \in \mathbb{C}^{q^{\mathsf{n}-d}}\}$.

(c) For any $\mathbf{s}, \mathbf{t} \in \mathbb{F}_q^{2\mathsf{n}}$, we have

$$\mathbf{W}(\mathbf{t})|\overline{\mathbf{s}}\rangle \otimes \mathbb{C}^{q^{\mathsf{n}-d}} = |\overline{\mathbf{s}+\mathbf{t}}\rangle \otimes \mathbb{C}^{q^{\mathsf{n}-d}}, \tag{14}$$

$$\mathbf{W}(\mathbf{t})\big(|\overline{\mathbf{s}}\rangle\langle\overline{\mathbf{s}}| \otimes \mathbf{I}_{q^{\mathsf{n}-d}}\big)\mathbf{W}(\mathbf{t})^{\dagger} = |\overline{\mathbf{s}+\mathbf{t}}\rangle\langle\overline{\mathbf{s}+\mathbf{t}}| \otimes \mathbf{I}_{q^{\mathsf{n}-d}}. \tag{15}$$

(d) For any $\mathbf{v} \in \mathcal{V}$ and any $|\psi\rangle \in |\overline{\mathbf{0}}\rangle \otimes \mathbb{C}^{q^{\mathsf{n}-d}}$, we have

$$\mathbf{W}(\mathbf{v})|\psi\rangle = |\psi\rangle. \tag{16}$$

APPENDIX B
PROOF OF LEMMA 2

Proof: The first two claims (7) and (8) are true not just for a particular $\mathbf{\Sigma}$, but for every diagonal $\mathbf{\Sigma}$ with elements in $\{0, 1\}$.

Let $\mathbf{\Lambda} = \begin{pmatrix} \mathbf{I}-\mathbf{\Sigma} & \mathbf{\Sigma} \\ -\mathbf{\Sigma} & \mathbf{I}-\mathbf{\Sigma} \end{pmatrix}$. First, we prove Eq. (7) by testing the LIT condition on $\mathbf{\Lambda}$. We have that $\det((\mathbf{I}-\mathbf{\Sigma})^2 + \mathbf{\Sigma}^2) = \det(\mathbf{I} - 2\mathbf{\Sigma} + 2\mathbf{\Sigma}^2) = \det(\mathbf{I}) = 1$, since $\mathbf{\Sigma}^2 = \mathbf{\Sigma}$ by the fact that $\mathbf{\Sigma}$ is a diagonal matrix with entries in $\{0, 1\}$.

Eq. (8) follows by the fact that $\mathbf{\Lambda}\mathbf{J}\mathbf{\Lambda}^{\top} = \mathbf{J}$ (that is, $\mathbf{\Lambda}^{\top}$ is symplectic), which can be easily proved by employing $\mathbf{\Sigma}^2 = \mathbf{\Sigma}$.

Finally, we prove that there exists a signed column-swap operation ($\mathbf{\Sigma}$) that gives us the desired full-rank left half-matrix of $(\mathbf{M}')^{\top}$. For this we proceed according to Algorithm 1, which tries at most N different signed-swap operations before declaring either success or failure.

If the algorithm exits with success, then we obtain a full-rank $\mathbf{M}'_l$ as desired. To show that the algorithm cannot fail, let us show that failure would lead to a contradiction. Suppose the algorithm fails and exits with the value $i < N$. At this point, the first $i-1$ columns of $\mathbf{M}'_l$ are linearly independent, but the i^{th} column of $\mathbf{M}_l$ and the i^{th} column of $\mathbf{M}_r$ are each linearly dependent on the first i columns of $\mathbf{M}_l$. Note that since the only manipulations performed by the algorithm are signed-swap operations, by Eq. (8) $\mathbf{M}' \in \mathcal{M}_o$. The remainder of the proof of Eq. (9) uses the following two trivial facts.

1) Since $\mathbf{M}' \in \mathcal{M}_o$, the $2N \times N$ matrix $(\mathbf{M}')^{\perp} = \mathbf{J}\mathbf{M}' \in \mathcal{M}_o$ spans the null-space of $\mathbf{M}'$. Thus, any matrix whose columns are null vectors of $\mathbf{M}$ must be self-orthogonal.
2) If $\mathbf{V} = \begin{pmatrix} \mathbf{V}_l & \mathbf{V}_r \end{pmatrix}^{\top} \in \mathcal{M}_o$, then the dot product between the i^{th} row of $\mathbf{V}_l$ and the j^{th} row of $\mathbf{V}_r$ is equal to the dot product between the j^{th} row of $\mathbf{V}_l$ and the i^{th} row of $\mathbf{V}_r$.

Since the $(i+1)^{th}$ column of $\mathbf{M}_l$ and the $(i+1)^{th}$ column of $\mathbf{M}_r$ are each linearly dependent on the first i columns of $\mathbf{M}_l$, there exists a $2N \times N$ matrix $\mathbf{V}$ such that

$$\begin{aligned}\mathbf{V}^{\top} &= \begin{pmatrix} \mathbf{V}_l & \mathbf{V}_r \end{pmatrix} \\ &= \left(\begin{array}{ccccc|ccccc} \alpha_1 & \cdots & \alpha_i & \alpha_{i+1} & \mathbf{0} & 0 & \cdots & 0 & 0 & \mathbf{0} \\ \beta_1 & \cdots & \beta_i & 0 & \mathbf{0} & 0 & \cdots & 0 & \beta_{i+1} & \mathbf{0} \end{array}\right),\end{aligned}$$

$\alpha_{i+1}\beta_{i+1} \neq 0$, and $(\mathbf{M}')^{\top}\mathbf{V} = \mathbf{0}$. In fact, since the first $(i+1)$ columns of $\mathbf{M}_l$ are linearly dependent, there exists a non-trivial linear combination of them with coefficients $\alpha_1, \ldots, \alpha_{i+1}$ that produces the zero vector. Notice that α_{i+1} cannot be zero because the first i columns are linearly independent by assumption. Thus, the first row of $\mathbf{V}^{\top}$ is in the null-space of $\mathbf{M}'$ and $\alpha_{i+1} \neq 0$. The second row of $\mathbf{V}^{\top}$ is similarly in the null-space of $\mathbf{M}'$ and $\beta_{i+1} \neq 0$. So, $\mathbf{V} \in \mathcal{M}_o$ by fact 1), but the dot product of the first row of $\mathbf{V}_l$ with the second row of $\mathbf{V}_r$ is $\alpha_{i+1}\beta_{i+1} \neq 0$, whereas the dot product

---

Algorithm 1: Signed column swap

input : $\mathbf{M} = \begin{pmatrix} \mathbf{M}_l & \mathbf{M}_r \end{pmatrix} \in \mathbb{F}_q^{N \times 2N}$
output: $\mathbf{M}' = \begin{pmatrix} \mathbf{M}'_l & \mathbf{M}'_r \end{pmatrix} \in \mathbb{F}_q^{N \times 2N} \mid \det(\mathbf{M}'_l) \neq 0$

$\mathbf{M}' \leftarrow \mathbf{M}$;
$\mathbf{M}'_l \leftarrow \mathbf{M}_l$;
$\mathbf{M}'_r \leftarrow \mathbf{M}_r$;
$i \leftarrow 1$;
while $i \leq N$ **do**
  if $(\mathbf{M}'_l)_{\cdot,i}$ *is linearly independent of the first* $i-1$ *columns of* $\mathbf{M}'_l$ **then**
    $i \leftarrow i+1$;
  else if $(\mathbf{M}'_r)_{\cdot,i}$ *is linearly independent of the first* $i-1$ *columns of* $\mathbf{M}'_l$ *that are already fixed* **then**
    $(\mathbf{M}'_l)_{\cdot,i}, (\mathbf{M}'_r)_{\cdot,i} \leftarrow (-\mathbf{M}'_r)_{\cdot,i}, (\mathbf{M}'_l)_{\cdot,i}$;
    $i \leftarrow i+1$;
  else
    return Failure;
  end
end
return Success;

of the second row of $\mathbf{V}_l$ with the first row of $\mathbf{V}_r$ is 0, which contradicts fact 2). This contradiction proves Eq. (9). $\blacksquare$