

Efficient Code for Relativistic Quantum Summoning

Ya-Dong Wu,¹ Abdullah Khalid,¹ and Barry C. Sanders^{1,2,3,4}

¹*Institute for Quantum Science and Technology, University of Calgary, Alberta T2N 1N4, Canada*

²*Institute for Quantum Information and Matter,*

California Institute of Technology, Pasadena, California 91125, USA

³*Program in Quantum Information Science, Canadian Institute for Advanced Research, Toronto, Ontario M5G 1Z8, Canada*

⁴*Shanghai Branch, National Laboratory for Physical Sciences at Microscale, University of Science and Technology of China, Shanghai 201315, China*

Summoning retrieves quantum information, prepared somewhere in spacetime, at another specified point in spacetime, but this task is limited by the quantum no-cloning principle and the speed-of-light bound. We develop a thorough mathematical framework for summoning quantum information in a relativistic system and formulate a quantum summoning protocol for any valid configuration of causal diamonds in spacetime. For single-qubit summoning, we present a protocol based on a Calderbank-Shor-Steane code that decreases the space complexity for encoding by a factor of two compared to the previous best result and reduces the gate complexity from scaling as the cube to the square of the number of causal diamonds. Our protocol includes decoding whose gate complexity scales linearly with the number of causal diamonds. Our thorough framework for quantum summoning enables full specification of the protocol, including spatial and temporal implementation and costs, which enables quantum summoning to be a well posed protocol for relativistic quantum communication purposes.

I. INTRODUCTION

Quantum summoning is the task of encoding and transmitting quantum information to a configuration of spacetime causal diamonds such that the quantum information can be reconstructed in any one of these causal diamonds [1–4]. Quantum summoning cannot be guaranteed to work for every configuration of causal diamonds because quantum information cannot be copied [5–8] or transmitted superluminally [6]. Summoning is only possible for a configuration of causal diamonds if every pair of diamonds is causally related, where two diamonds are causally related if the earliest point of one can communicate with the latest point of the other [2]. Our aim is to construct efficient protocols for summoning quantum information in any configuration of N pairwise-related causal diamonds.

A variety of work has been done on summoning ever since Kent introduced this task and presented a no-summoning theorem [1]. Hayden and May [2] showed that quantum summoning can be reduced to the primitives of quantum secret sharing [9–11] and teleportation [12, 13]. They exploited a codeword-stabilized (CWS) quantum code [14] to design a summoning protocol that is efficient in the sense that the number of qubits Q used by the code is polynomial in N . Hayden et al. [3] proposed a continuous-variable version of summoning and an efficient protocol to perform this task, as well as showing that optical circuits can be used to realize summoning experimentally. In 2016, Adlam and Kent proposed a summoning task with multiple summonses and provided a protocol, which employs teleportation, to accomplish this task for the configuration being an ordered set of causal diamonds [4].

Our protocol for summoning quantum information

uses a Calderbank-Shor-Steane (CSS) code [15, 16]

$$\left[\left[\binom{\tilde{N}}{2}, 1, \frac{\tilde{N}}{2} \right] \right], \quad \tilde{N} = 2 \left\lfloor \frac{N}{2} \right\rfloor \in 2\mathbb{Z}, \quad (1)$$

that encodes one qubit into $\binom{\tilde{N}}{2}$ physical qubits, with the restriction that \tilde{N} is even. We calculate that this CSS code distance $\frac{\tilde{N}}{2}$, and this code is constructed from the relation between graphs and linear algebra [17, 18]. Our code is a qubit version of the homological continuous-variable quantum error correcting code [3] and corrects erasure errors that occur in summoning.

We provide a procedure to construct the encoding and decoding circuits for our CSS code for any even positive integer \tilde{N} . The number of qubits Q used by our protocol is reduced by a factor of two compared to the previous best [2], and the number of quantum gates G is reduced from $O(N^3)$ [2] to $O(N^2)$. Our decoding procedure has gate complexity $O(N)$. Our results are significant in that we complete the quantum summoning protocol [1–3] by providing both encoding and decoding schemes, explain how to utilize quantum error correction for summoning, analyze quantum resources, and demonstrate improved efficiency for our protocol.

Our paper is organized as follows. Section II reviews the background knowledge regarding summoning, quantum error correction and algebraic graph theory. Section III provides the mathematical definition of summoning. In section IV, we study a protocol for summoning using a CSS code, including the encoding and the decoding methods, and the resource analysis of the CSS code and the CWS code. Sections V and VI give the discussion and the conclusion, respectively.

II. BACKGROUND

Here we explain the quantum information processing task of summoning and the conditions for the configurations to make summoning feasible [1–3]. Then we give the background knowledge on stabilizer quantum error correcting codes [21], especially CSS codes [15, 16]. We introduce the relation between graphs and binary vectors [17], which is useful for the construction of the CSS stabilizer code. Finally, we briefly review the CWS code [14] used by Hayden and May to summon quantum information [2].

A. Summoning

Summoning is an information processing task involving Alice and Bob [1–3]. Bob’s role is to provide the quantum information to Alice and to designate where the quantum information is to be summoned and Alice’s role is to summon quantum information at the designated spacetime location. Associated to each request point y is a reveal point z_y that is in the causal future of y . The intersection of the future light cone of y with the past light cone of z_y is called a causal diamond, expressed as \diamond . We label causal diamonds and show a label i in the diamond as \diamond_i . Besides the request and reveal points, Alice and Bob also agree upon a starting point s , where Bob provides the quantum information to Alice.

Alice and Bob can arrange their agents at various points in spacetime prior to the start of summoning [3]. Bob designates one agent to be the referee who sends quantum information to point s and classical information to all the request points. Alice designates one agent to be the starting agent S , who is situated at point s , and she delegates agents to each request and reveal point. We label the agent at point x by A_x . Figure 1 shows an example of Alice’s and Bob’s agents arranged in spacetime.

When summoning starts, the referee prepares a quantum state

$$|\psi\rangle \in \mathcal{H}, \quad (2)$$

where \mathcal{H} is a finite d -dimensional Hilbert space [2], and transmits $|\psi\rangle$ to the starting agent. Alice and all her agents do not have any knowledge of $|\psi\rangle$. The referee randomly chooses one request point, say y , and sends the request only to A_y . Then Alice’s task is to present the quantum state $|\psi\rangle$ at the corresponding reveal point z_y , by her agents’ collaboration.

Given a set of causal diamonds $\{\diamond_i\}_{i=1}^N$, summoning might be infeasible [1] due to the restrictions of both the no-cloning theorem [5–8] and no superluminal communication [6]. Summoning is possible if and only if the following two conditions are satisfied [2].

C1 All reveal points are in the causal future of s .

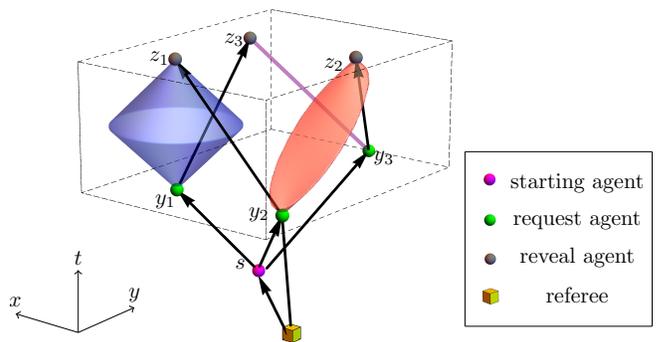


FIG. 1: Three causal diamonds (red, blue and purple) in spacetime. A referee, a starting agent, three request agents and three reveal agents are arranged in spacetime. An arrow represents a quantum communication channel from one agent to another agent, and a line segment between two agents represents a classical channel from one to the other. The referee sends a quantum state $|\psi\rangle$ to the starting agent, and randomly chooses y_2 to send a classical request to A_{y_2} . The starting agent encodes $|\psi\rangle$ to three qutrits and distribute them to three request agents respectively. A_{y_2} sends her qutrit to A_{z_2} . Receiving no request, the request agents at y_1 and y_3 send their qutrits to A_{z_3} and A_{z_2} respectively. Hence, A_{z_2} receives two qutrits and decodes the state $|\psi\rangle$.

C2 Each pair of causal diamonds is causally related, which means that there exists a point in one causal diamond that is causally related with at least one point in the other causal diamond.

We call a set of causal diamonds satisfying these two conditions a “valid configuration” for summoning. We represent a configuration of causal diamonds by a graph G as follows [2, 3]. We assign each causal diamond to a vertex and use the label of the causal diamond to label the vertex. If two causal diamonds are causally related, an edge e is inserted between the two corresponding vertices in G . A valid configuration of N causal diamonds is represented by an N -vertex complete graph denoted K_N , for which each pair of vertices is connected by an edge [17].

In Fig. 1, we present an example of using quantum secret sharing [9–11] to summon quantum information [2]. After receiving a qubit $|\psi\rangle$, the starting agent encodes $|\psi\rangle$ into three qutrits [9] and distributes the three qutrits to the three request agents. If A_{y_i} ($i = 1, 2$, or 3) receives the request, then the request agent sends her qutrit to the reveal point

$$z_i := z_{y_i}. \quad (3)$$

Otherwise, she sends her qutrit to the reveal point $z_{(i-1) \bmod 3}$. In such a way, no matter which request agent receives the request, the associated reveal agent receives two qutrits to retrieve the original qubit $|\psi\rangle$.

B. Stabilizer codes

In this subsection, we begin by introducing the Pauli group and the representation of Pauli operators using binary vectors. We explain the parameters characterizing a quantum error correcting code and the definition of erasure errors. Then we explain stabilizer codes [21], specially CSS codes [15, 16]. Finally, we show the encoding of a stabilizer code.

An n -qubit Pauli group [22] is

$$\mathcal{G}_n := \pm\{I, X, Y, Z\}^{\otimes n}, \quad (4)$$

where

$$X := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Z := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \text{ and } Y := ZX. \quad (5)$$

The Pauli group module sign is isomorphic to a cartesian product of binary vector spaces according to

$$\mathcal{I}_P : \mathcal{G}_n / \mathbb{Z}_2 \rightarrow \mathbb{Z}_2^n \times \mathbb{Z}_2^n : \bigotimes_{i=1}^n Z^{u_i} X^{v_i} \mapsto [\mathbf{u} \ \mathbf{v}], \quad (6)$$

where

$$\mathbf{u} := [u_1 \dots u_n], \ \mathbf{v} := [v_1 \dots v_n]. \quad (7)$$

Two Pauli operators represented as binary vectors, $[\mathbf{u} \ \mathbf{v}]$ and $[\mathbf{u}' \ \mathbf{v}']$, mutually commute if and only if [22]

$$\mathbf{u} \cdot \mathbf{v}' + \mathbf{v} \cdot \mathbf{u}' = 0, \quad (8)$$

where \cdot is the indefinite inner product

$$\mathbf{u} \cdot \mathbf{v} := \sum_{i=1}^n u_i v_i \in \mathbb{Z}_2. \quad (9)$$

Otherwise, these two Pauli operators anti-commute with each other.

In quantum error correcting codes, $[[n, k, d]]$ denotes a quantum code, where k qubits are encoded into n qubits, and d is the distance of the code [22]. Given a Pauli operator $P \in \mathcal{G}_n$, the weight of P is the number of non-identity single-qubit Pauli operators, i.e., X, Y and Z in the tensor product P . The distance of a quantum error correcting code is the minimum weight of a Pauli operator P such that

$$\langle i|P|j\rangle \neq C(P)\delta_{ij}, \quad (10)$$

where $|i\rangle$ and $|j\rangle$ are basis elements of the code, $C(P)$ is a constant depending on P , and δ_{ij} is the Kronecker delta function. When transmitting a block of n qubits, if t qubits ($t < n$) are lost or never received, while the other $n - t$ qubits are undamaged, then the errors at these t qubits are called erasure errors [23].

A stabilizer code [21] is the simultaneous eigenspace of all the elements of an Abelian subgroup \mathcal{S} of \mathcal{G}_n with

eigenvalue one. A generator set of \mathcal{S} is a set of independent elements in \mathcal{S} such that every element of \mathcal{S} can be expressed as a product of the elements in this generator set. An $[[n, k, d]]$ stabilizer code has $n - k$ independent stabilizer generators, each of which can be represented by a $2n$ -dimensional binary vector. The $[[n, k, d]]$ stabilizer code is characterized by an $(n - k) \times 2n$ stabilizer generator matrix, where each row represents a stabilizer generator.

Now we introduce CSS codes, which are a type of stabilizer codes. A CSS code [15, 16] is specified by two classical linear codes \mathcal{C}_1 and \mathcal{C}_2 , where \mathcal{C}_2 is a subcode of \mathcal{C}_1 , i.e.,

$$\mathcal{C}_2 \subseteq \mathcal{C}_1. \quad (11)$$

Each basis element of a CSS code corresponds to a coset [24] of \mathcal{C}_2 in \mathcal{C}_1 , where the basis element is an equally weighted superposition of all the codewords in the coset. A CSS code is a stabilizer code whose stabilizer generators are either tensor products of X operators and identities, or tensor products of Z operators and identities [21]. Hence, the CSS stabilizer code is characterized by an $(n - k) \times 2n$ stabilizer generator matrix

$$\begin{bmatrix} H_Z & \mathbf{0} \\ \mathbf{0} & H_X \end{bmatrix}, \quad (12)$$

where H_Z and H_X are two matrices, and the $\mathbf{0}$ s are appropriately sized zero matrices.

Here we explain the encoding of a stabilizer code with stabilizer \mathcal{S} . The Pauli operators that preserve the stabilizer code space but act nontrivially on the encoded state are the logical Pauli operators on the encoded state [21]. The logical Pauli operators commute with all stabilizers in \mathcal{S} but lie outside \mathcal{S} .

For an $[[n, 1, d]]$ stabilizer code with stabilizer \mathcal{S} , we denote \bar{Z} and \bar{X} as the logical Z and logical X operators on an n -qubit encoded state. Suppose

$$\bar{Z}|\psi_0\rangle = |\psi_0\rangle, \quad (13)$$

and

$$\{M_i\}_{i=1}^{n-1}$$

are $n - 1$ independent stabilizer generators of \mathcal{S} . The encoded logical states are [21]

$$|0\rangle_L := \prod_{i=1}^{n-k} (I + M_i) |\psi_0\rangle, \quad (14)$$

and

$$|1\rangle_L := \bar{X} \prod_{i=1}^{n-k} (I + M_i) |\psi_0\rangle = \prod_{i=1}^{n-k} (I + M_i) \bar{X} |\psi_0\rangle. \quad (15)$$

Equations (14) and (15) indicate how to encode one qubit by a stabilizer code.

We have discussed quantum error correction, especially stabilizer codes in this subsection. Next we study the close relation between a graph and a binary vector, which provides a powerful tool to construct the CSS stabilizer code.

C. Graphs and linear algebra

In this subsection, we begin by defining graphs and the binary linear space. After explaining these two concepts, we describe an isomorphism from sets of edges of an n -vertex graph to binary vectors with length $\binom{n}{2}$ [17]. Our approach is inspired by homology theory to construct quantum error correcting codes [3, 18]. Finally, we present the examples of triangle graphs and star graphs.

A graph [17]

$$G := (V, E) \quad (16)$$

comprises a set of vertices V and a set of edges

$$E \subseteq V \times V. \quad (17)$$

One example of a graph is the n -vertex complete graph, K_n .

To explain the binary linear space, we introduce $GF(2)$, which is the smallest finite field containing two elements $\{0, 1\}$, together with addition and multiplication operations [25]. The linear space [24] over field $GF(2)$, denoted by \mathbb{Z}_2^m , is a set $\{0, 1\}^m$, together with vector addition,

$$+ : \mathbb{Z}_2^m \times \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^m, \quad (18)$$

and scalar multiplication,¹

$$\cdot : GF(2) \times \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^m. \quad (19)$$

Next we explain the relation between an edge set E of a graph G and a binary vector with length $\binom{|V|}{2}$, where $|V|$ is the cardinality of V .

Given $K_n = (V_K, E_K)$, the power set of E_K , which is the set of all the subsets of E_K , forms a binary linear space \mathcal{E} [17]. The power set of E_K is denoted 2^{E_K} . For $U, U' \in 2^{E_K}$, the addition of U and U' amounts to the symmetric difference of U and U' ,

$$U + U' := (U \cup U') \setminus (U \cap U'). \quad (20)$$

The empty set \emptyset is the zero element and

$$\forall U \in 2^{E_K}, -U := U. \quad (21)$$

For $\diamond i$ and $\diamond j$, an edge e_{ij} is a unit vector in \mathcal{E} , and $e_{ji} = e_{ij}$ because we are dealing with undirected graphs. The set of edges

$$\{e_{ij}\}_{1 \leq i < j \leq n} \quad (22)$$

¹ Note we use \cdot for the scalar multiplication only in Eq. (19) and Table I. After this subsection, we use \cdot only for the indefinite inner product.

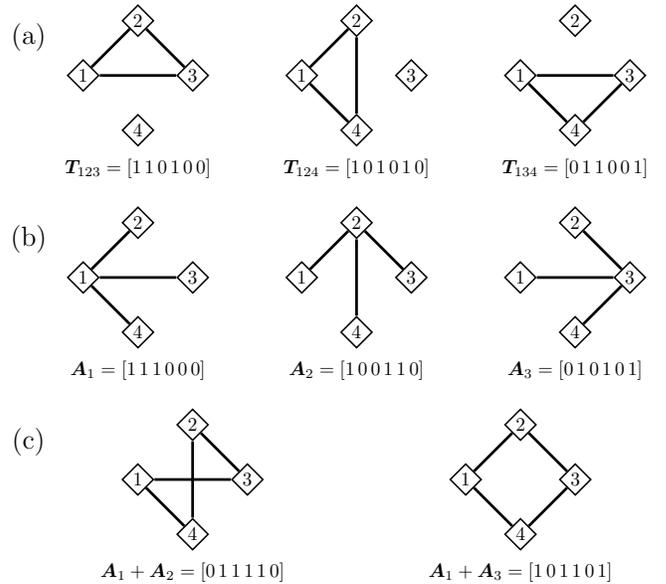


FIG. 2: For $n = 4$, (a) the triangle graphs representing T_{1jk} ($2 \leq j < k \leq 4$), (b) the star graphs representing A_l ($1 \leq l \leq 3$) and (c) the graphs representing $A_1 + A_m$ ($2 \leq m \leq 3$).

forms an orthonormal basis of \mathcal{E} . As $\binom{n}{2}$ edges exist in K_n ,

$$\dim \mathcal{E} = \binom{n}{2}. \quad (23)$$

Now we show that \mathcal{E} is isomorphic to $\mathbb{Z}_2^{\binom{n}{2}}$ [17]. Given any $U \in \mathcal{E}$, an isomorphism is

$$\mathcal{I}_G : \mathcal{E} \rightarrow \mathbb{Z}_2^{\binom{n}{2}} : U \mapsto \mathbf{u} = [u_1 \dots u_{\binom{n}{2}}], \quad (24)$$

where

$$\{u_i\}_{i=1}^{\binom{n}{2}}$$

are the coefficients of U with respect to the basis in Eq. (22). The isomorphic mappings of the vector addition and the scalar multiplication are shown in Table I.

Here we introduce two types of $\binom{n}{2}$ -dimensional binary vectors and two linear subspaces spanned by these two types of vectors as examples of the isomorphism (24).

	\mathcal{E}	$\mathbb{Z}_2^{\binom{n}{2}}$
+	$(U \cup U') \setminus (U \cap U')$	$\mathbf{u} + \mathbf{u}'$
\cdot	$0U = \emptyset, 1U = U$	$0\mathbf{u} = \mathbf{0}, 1\mathbf{u} = \mathbf{u}$

TABLE I: The mapping of the vector addition and the scalar multiplication on \mathcal{E} to those operations on $\mathbb{Z}_2^{\binom{n}{2}}$

These examples are used later for the construction of the CSS stabilizer code. The two types of vectors in $\mathbb{Z}_2^{\binom{n}{2}}$ are

$$\mathbf{T}_{ijk} := \mathbf{e}_{ij} + \mathbf{e}_{jk} + \mathbf{e}_{ki}, \quad \mathbf{A}_j := \sum_{1 \leq l \leq n, l \neq j} \mathbf{e}_{lj}, \quad (25)$$

where \mathbf{e}_{ij} is the unit vector $\mathcal{I}_G(\mathbf{e}_{ij})$. From the isomorphism (24), these two types of vectors can be represented by two different types of graphs. \mathbf{T}_{ijk} is represented by a triangle graph connecting vertices

$$\{\diamond i, \diamond j, \diamond k\}, \quad (26)$$

and \mathbf{A}_j is represented by a star graph with vertex $\diamond j$ connected to every other vertex.

We construct the linear space

$$\mathcal{C}_1 := \text{span}\{\mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_{n-1}\} \quad (27)$$

spanned by $n - 1$ linearly independent $\{\mathbf{A}_j\}$, and the orthogonal linear space

$$\mathcal{C}_1^\perp := \text{span}\{\mathbf{T}_{123}, \mathbf{T}_{124}, \dots, \mathbf{T}_{12n}, \mathbf{T}_{134}, \dots, \mathbf{T}_{1_{n-1}n}\} \quad (28)$$

spanned by $\binom{n-1}{2}$ linearly independent $\{\mathbf{T}_{ijk}\}$. The elements in \mathcal{C}_1^\perp are represented by Eulerian cycles (graph cycles that use each edge exactly once) [17]. Meanwhile, \mathcal{C}_1 comprises vectors orthogonal to all vectors in \mathcal{C}_1^\perp [17], i.e.,

$$\mathcal{C}_1 = (\mathcal{C}_1^\perp)^\perp. \quad (29)$$

We introduce an $(n - 2)$ -dimensional linear subspace of \mathcal{C}_1

$$\mathcal{C}_2 := \text{span}\{\mathbf{A}_1 + \mathbf{A}_2, \mathbf{A}_1 + \mathbf{A}_3, \dots, \mathbf{A}_1 + \mathbf{A}_{n-1}\} \subset \mathcal{C}_1. \quad (30)$$

\mathcal{C}_2 together with \mathcal{C}_1 specifies the CSS code for summoning in Subsec. IV B. Figure 2(a), (b) and (c) depict the graphs representing bases of linear spaces \mathcal{C}_1^\perp , \mathcal{C}_1 and \mathcal{C}_2 respectively for $n = 4$.

This subsection has shown that the power set of the edge set of an n -vertex complete graph forms a binary linear space, isomorphic to $\mathbb{Z}_2^{\binom{n}{2}}$. Hence, we have constructed a graph representation of any $\binom{n}{2}$ -binary vector. The examples given in this subsection are useful to construct the CSS code for summoning.

D. The CWS code for summoning

In this subsection, we first introduce CWS codes [14], then explain the graph-state formalism of CWS codes. Finally we discuss the CWS code used by Hayden and May for quantum summoning [2]. In Subsec. IV D, we study the gate complexity of the encoding of the CWS code for summoning and compare it with the CSS code.

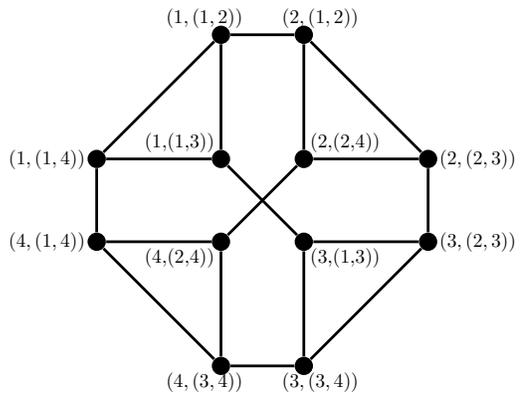


FIG. 3: G_{CWS} for $N = 4$. Each vertex of G_{CWS} is labeled by $(j, (j, k))$ for $1 \leq j, k \leq 4$ and $k \neq j$. Each $(j, (j, k))$ is adjacent to $(k, (j, k))$ and $(j, (j, l))$, where $1 \leq l \leq 4$ and $l \neq j$ or k .

An $((n, k))$ CWS code [14] encodes a k -dimensional Hilbert space to n qubits. This CWS code is specified by a word stabilizer, which is a 2^n -element Abelian subgroup \mathcal{S} of \mathcal{G}_n , and a set of k word operators, which are n -qubit Pauli operators

$$\{W_l\}_{l=1}^k.$$

The word stabilizer \mathcal{S} specifies a unique $|\psi_{\mathcal{S}}\rangle$ such that $\forall M \in \mathcal{S}$,

$$M |\psi_{\mathcal{S}}\rangle = |\psi_{\mathcal{S}}\rangle. \quad (31)$$

The CWS code is spanned by the basis

$$\{ |w_l\rangle := W_l |\psi_{\mathcal{S}}\rangle \}_{l=1}^k. \quad (32)$$

Under local Clifford operations, any CWS code is equivalent to its standard form [14], whose word stabilizer is a graph-state stabilizer [26], and whose word operators contain only Z operators and identities. Thus, the stabilized state $|\psi_{\mathcal{S}}\rangle$ of a CWS code in its standard form is a graph state. Given a graph $G = (V, E)$, the associated graph state is [26]

$$|G\rangle = \prod_{(i, j) \in E} CZ_{(i, j)} H^{\otimes |V|} |0\rangle^{|V|}, \quad (33)$$

where $CZ_{(i, j)}$ is the controlled- Z gate with control qubit i and target qubit j , and H is the Hadamard gate.

Hayden and May propose a $\left(\binom{N}{2}, 2\right)$ CWS code to summon a qubit in N causal diamonds [2]. This $\left(\binom{N}{2}, 2\right)$ CWS code is specified by a graph-state stabilizer represented by a graph G_{CWS} and two word operators

$$\{I, Z^{\otimes N(N-1)}\}. \quad (34)$$

Given an N -vertex complete graph $K_N = \{V_K, E_K\}$, G_{CWS} is the line graph [17] of $G' := \{V', E'\}$, where

$$V' = V_K \cup E_K, \quad (35)$$

and

$$E' = \{(v, (v, w)); v \in V_K, (v, w) \in E_K\}. \quad (36)$$

Figure 3 presents G_{CWS} for $N = 4$. This CWS code can be used to summon one qubit in four causal diamonds [2] by employing twelve qubits.

This section has introduced quantum summoning as a quantum information processing task in spacetime and explained the conditions on the configurations to make quantum summoning feasible. We have briefly reviewed the background knowledge on quantum error correction, especially stabilizer codes and CSS codes, which are used for quantum summoning in this paper. We have explained the connection between graphs and binary vectors, which is useful for the construction of the CSS code for summoning. Finally, we have reviewed the CWS code used for quantum summoning [2], with which we compare our CSS code in Subsec. IV D.

III. MATHEMATICAL DEFINITION OF SUMMONING

In this section, we mathematically define both classical and quantum summoning. We begin by formalizing the notions of past and future light cones and causal diamonds. We then establish notations for a configuration of causal diamonds and the sets of request and reveal points. Subsequently, we give a careful definition of both classical and quantum summoning, and when these tasks are trivial.

Each spacetime point is $x \in \mathcal{M}$, where \mathcal{M} denotes Minkowski spacetime [27]. The future light cone for x is

$$\text{fut}(x) := \{w \in \mathcal{M}; w \succ x\}, \quad (37)$$

where $w \succ x$ indicates that information can be sent from x to w . The past light cone for x is

$$\text{pas}(x) := \{w \in \mathcal{M}; w \prec x\}, \quad (38)$$

where $w \prec x$ indicates that information can be received at x from w . A causal diamond for a pair of points $(y_i, z_i) \in \mathcal{M} \times \mathcal{M}$ satisfying $y_i \prec z_i$ is

$$\diamond_i := \{x \in \mathcal{M}; x \in \text{fut}(y_i) \cap \text{pas}(z_i)\}. \quad (39)$$

A configuration of causal diamonds is

$$\mathcal{C} := \{\diamond_i; y_i \prec z_i\}, \quad (40)$$

and $N := |\mathcal{C}|$. Two causal diamonds \diamond_i and \diamond_j are causally related if and only if $\exists x \in \diamond_i, \exists w \in \diamond_j$ such

that either $x \in \text{fut}(w)$, or $x \in \text{pas}(w)$. The set of request points is

$$\text{REQ} := \{y_i \in \mathcal{M}; \diamond_i \in \mathcal{C}\}, \quad (41)$$

and the set of reveal points is

$$\text{REV} := \{z_i \in \mathcal{M}; \diamond_i \in \mathcal{C}\}. \quad (42)$$

A starting point is $s \in \mathcal{M}$ such that $\forall z \in \text{REV}, z \in \text{fut}(s)$, where there is a starting agent S .

We now formalize Kent's classical summoning protocol [1] by making each object mathematically well defined. Given starting agent S at $s \in \mathcal{M}$, request agents

$$\text{REQAG} := \{A_y; y \in \text{REQ}\} \quad (43)$$

and corresponding reveal agents

$$\text{REVAG} := \{A_z; z \in \text{REV}\}, \quad (44)$$

and S possessing n -bit string $m \in \{0, 1\}^n$, summoning is the task of delivering m to any agent in REVAG given arbitrary external selection of some $y \in \text{REQ}$, which is only revealed at spacetime point y .

Remark 1. Classical summoning is trivial because S broadcasts m to all $z \in \text{REV}$ [1].

The notion of quantum summoning [1, 2] builds on the concept of classical summoning, which we formalize as follows. Given a starting agent S , REQAG and REVAG, and S possessing quantum information

$$|\Psi\rangle \in \mathcal{H}_2^{\otimes n} \quad (45)$$

(with S possibly oblivious to $|\Psi\rangle$), summoning is the task of delivering $|\Psi\rangle$ to any agent in REVAG given arbitrary external selection of some $y \in \text{REQ}$, which is only revealed at spacetime point y .

Remark 2. Summoning is trivial if S has a classical description of $|\Psi\rangle$ because S broadcasts this description such that all agents in REVAG receive and can reconstruct $|\Psi\rangle$.

Remark 3. Quantum summoning is trivial if there is a causal curve, which starts from s and runs sequentially through all $\diamond_i \in \mathcal{C}$ in any order. The protocol is trivial in this case because quantum information can simply be sent along this causal curve. When quantum information arrives at \diamond_j , A_{y_j} decides whether to send it to z_j or to send it to the next causal diamond depending on whether she receives the request or not.

IV. SUMMONING BY QUANTUM ERROR CORRECTION

Here we present a protocol for Alice to summon quantum information. We specify the actions that the starting agent and each of the request and reveal agents perform to fulfill any summoning request (Subsec. IV A). For

any valid configuration of causal diamonds, we propose a CSS code for the protocol of quantum summoning (Subsec. IV B). The encoding and decoding circuits of the CSS code are provided (Subsec. IV C). We show that the CSS code consumes fewer quantum resources than the CWS code [2] (Subsec. IV D).

A. Protocol

Here we propose a protocol using the CSS code (1) for summoning one qubit in any valid spacetime configuration. This CSS code assigns one qubit to each edge of the complete graph $K_{\tilde{N}}$; hence, the number of qubits used by the protocol is

$$Q = \binom{\tilde{N}}{2}, \quad (46)$$

for N and \tilde{N} related according to Eq. (1).

For a spacetime configuration with an even number N of causal diamonds, $\tilde{N} := N$ and S employs the CSS code (1) to encode a qubit,

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad (47)$$

into Q (46) qubits and assigns each qubit to an edge of the complete graph $K_{\tilde{N}}$. The qubit assigned to the edge e_{ij} is called q_{ij} , where e_{ij} denotes the edge connecting \diamond_i to \diamond_j for $i, j \in [N]$ and $i \neq j$.

S sends q_{ij} to A_{y_i} if

$$y_i \prec z_j, \quad (48)$$

and to A_{y_j} if

$$y_j \prec z_i. \quad (49)$$

If A_{y_i} receives the summoning request, she sends all the qubits in her possession to A_{z_i} . Otherwise, she sends each qubit q_{ij} in her possession to A_{z_j} . As each vertex is adjacent to $N - 1$ edges, any reveal agent, who receives the summoning request, receives $N - 1$ qubits. Later, we prove that $\forall r \in [N] := \{1, 2, \dots, N\}$, the qubits

$$\{q_{rk}; k \in [N] \setminus \{r\}\} \quad (50)$$

can be used to decode $|\psi\rangle$ perfectly. Fig. (4) shows how the qubits are assigned to the request agents for a configuration of four causal diamonds.

In a configuration of an odd number of causal diamonds,

$$\tilde{N} := N + 1. \quad (51)$$

S introduces one more vertex



to obtain graph K_{N+1} . This new vertex can be seen as fictitious causal diamond causally related with every causal diamond, but the summoning request is never sent to this causal diamond. Then S employs the CSS code (1), which encodes $|\psi\rangle$ into $\binom{N+1}{2}$ qubits. As before, S sends each qubit q_{ij} , where $i, j \in [N]$, to A_{y_i} if

$$y_i \prec z_j, \quad (52)$$

and to A_{y_j} if

$$y_j \prec z_i. \quad (53)$$

S sends each additional qubit $q_{j, N+1}$ to reveal agent A_{z_j} . As in the even case, if A_{y_i} receives the summoning request, A_{y_i} sends all the qubits in her possession to A_{z_i} . Otherwise, she sends each qubit q_{ij} in her possession to A_{z_j} . Any reveal agent who receives the summoning request, ultimately receives N qubits to decode $|\psi\rangle$. For any $r \in [N + 1]$, the qubits

$$\{q_{rk}; k \in [N + 1] \setminus \{r\}\} \quad (54)$$

can be used to decode $|\psi\rangle$ perfectly.

This protocol can also be used to accomplish a variant of the summoning task [4]. In this modified task, the set of causal diamonds are causally ordered and the request may be sent to multiple request agents but only one of them needs to comply with the summon. If the causal diamonds are causally ordered, then in the subset of request agents to whom the requests are sent,

$$\{A_{y_i}; i \in K \subseteq [N]\}, \quad (55)$$

let A_{y_r} be the earliest request agent according to the causal order of the diamonds. By following the above protocol, the reveal agent A_{z_r} receives the $N - 1$ qubits if N is even and the N qubits if N is odd. Hence, A_{z_r} can decode the state $|\psi\rangle$.

This subsection has explained our protocol for quantum summoning. Subsection IV B provides the detail of the CSS code (1) used in our protocol.

B. The CSS code

In this subsection, we propose a stabilizer code with each qubit assigned to an edge of $K_{\tilde{N}}$. We show that it is an $\left[\left[\binom{\tilde{N}}{2}, 1, \frac{\tilde{N}}{2}\right]\right]$ CSS code, which can be used to summon a qubit by following the protocol in Subsec. IV A.

Theorem 1. *The stabilizer code, specified by a*

$$\left[\left[\binom{\tilde{N}}{2} - 1\right] \times 2 \binom{\tilde{N}}{2}\right]$$

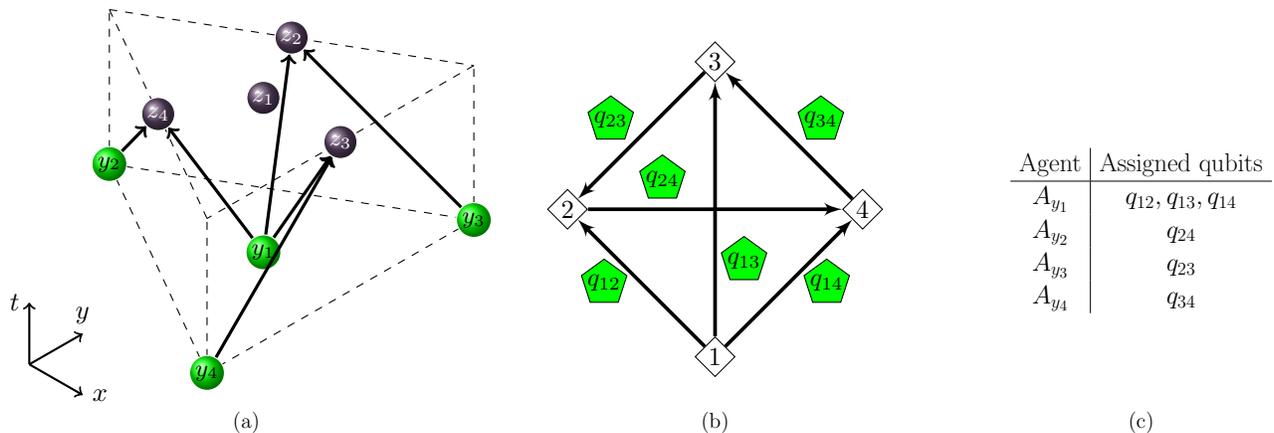


FIG. 4: (a) A configuration of four causal diamonds in $2 + 1$ dimensions. Three request points (y_2, y_3, y_4) are placed at the base vertices of an equilateral triangular prism and a fourth (y_4) is placed at the centroid of base vertices. The reveal points are placed at the midpoints of the top vertices (z_1, z_2, z_3) and the centroid of the top vertices. The volume of the diamond is not shown for visual clarity. The black arrows represent causal connections between points. (b) A complete graph representing the causal connections between the diamonds depicted in (a). For the CSS code the qubit q_{ij} is assigned to edge e_{ij} . (c) A table showing which requests agents is each physical qubit sent to.

stabilizer generator matrix

$$H_{\tilde{N}} = \left[\begin{array}{c|c} \begin{matrix} \mathbf{T}_{123} \\ \mathbf{T}_{124} \\ \vdots \\ \mathbf{T}_{12\tilde{N}} \\ \mathbf{T}_{134} \\ \vdots \\ \mathbf{T}_{1\tilde{N}-1\tilde{N}} \end{matrix} & \begin{matrix} \mathbf{0} \\ \mathbf{0} \\ \vdots \\ \mathbf{0} \\ \mathbf{0} \\ \vdots \\ \mathbf{0} \end{matrix} \\ \hline \begin{matrix} \mathbf{0} \\ \mathbf{0} \\ \vdots \\ \mathbf{0} \end{matrix} & \begin{matrix} \mathbf{A}_1 + \mathbf{A}_2 \\ \mathbf{A}_1 + \mathbf{A}_3 \\ \vdots \\ \mathbf{A}_1 + \mathbf{A}_{\tilde{N}-1} \end{matrix} \end{array} \right], \quad (56)$$

where $\mathbf{0}$ is an $\binom{\tilde{N}}{2}$ -dimensional zero vector, is an $\left[\left[\binom{\tilde{N}}{2}, 1, \frac{\tilde{N}}{2} \right] \right]$ CSS code, which can correct erasure errors at qubits q_{ij} for $i, j \in [N] \setminus \{r\}$ for any $r \in [\tilde{N}]$.

The stabilizer generator matrix (56) is analogous to the stabilizer generator matrix of the homological continuous-variable quantum error correcting code [3]. By changing -1 to 1 in the stabilizer generator matrix of the continuous-variable code, one obtains the generator matrix (56) from the generator matrix of the continuous-variable code. In continuous-variable codes, ± 1 in the generator matrix represents the phase-space displacement operators $e^{\pm i\hat{X}}$ or $e^{\pm i\hat{P}}$, where \hat{X} and \hat{P} are quadrature operators [28, 29]. On the other hand, in the qubit code, 1 in the generator matrix represent Pauli operators Z or X .

To prove this theorem, we prove the following three lemmas.

Lemma 2. $H_{\tilde{N}}$ (56) is a stabilizer generator matrix of a CSS code, which encodes one qubit into $\binom{\tilde{N}}{2}$ qubits.

Proof. From Eqs. (27) and (28),

$$\mathbf{T}_{1jk} \cdot (\mathbf{A}_1 + \mathbf{A}_l) = 0 \quad (57)$$

for any j, k, l such that $2 \leq j < k \leq \tilde{N}$ and $2 \leq l \leq \tilde{N} - 1$. Using Eq. (8), we know that all the stabilizer generators in $H_{\tilde{N}}$ (56) commute with each other, thereby generating an Abelian subgroup \mathcal{S} of $\mathcal{G}_{\binom{\tilde{N}}{2}}$. There are $\binom{\tilde{N}}{2} - 1$ independent stabilizer generators, so this stabilizer code encodes one qubit into $\binom{\tilde{N}}{2}$ qubits. The first $\binom{\tilde{N}-1}{2}$ stabilizer generators contain only Z operators and identities and the other $\tilde{N} - 2$ stabilizer generators contain only X operators and identities. Thus, the stabilizer code is a CSS code. \square

In $H_{\tilde{N}}$, the vectors representing the Z -type stabilizers and the X -type stabilizers span \mathcal{C}_1^\perp (28) and \mathcal{C}_2 (30) for $n = \tilde{N}$ respectively. Thus, the CSS code in Theorem 1 is specified by the linear codes \mathcal{C}_1 (27) and \mathcal{C}_2 (30) for $n = \tilde{N}$.

Now we show that by assigning each of the $\binom{\tilde{N}}{2}$ physical qubits to an edge in $K_{\tilde{N}}$, this CSS code can correct the erasure errors at those qubits, which are not connected to vertex $\diamond r$, for any $r \in [\tilde{N}]$. Hence, by following the protocol of quantum summoning in Subsec. IV A, no matter which A_{y_r} receives the request, the associated reveal agent A_{z_r} can decode the original state $|\psi\rangle$ from her $\tilde{N} - 1$ qubits in Eq. (50) or Eq. (54).

Lemma 3. For any $r \in [\tilde{N}]$, the CSS code in Theorem 1 can correct erasure errors at qubits q_{ij} for $i, j \in [\tilde{N}] \setminus \{r\}$.

The proof of Lemma 3 is in Appendix A. The proof is a modified version of that for the continuous-variable code [3] with the infinite-dimensional field \mathbb{R} replaced by the finite-dimensional field \mathbb{Z}_2 . One side effect of this modification is that \tilde{N} has to be even. Lemma 3 is no longer true if \tilde{N} is odd. To see this, we consider an example of a three-qubit code with stabilizer generators $\{ZZZ, IXX\}$. If $r = 3$, this code should correct any Pauli error at q_{12} . This is obviously false, because the Pauli error at q_{12} , ZII , commutes with both stabilizer generators but does not lie in the stabilizer group.

Now we find the distance of the CSS code, which is an important parameter characterizing the capability of the code to detect and correct errors.

Lemma 4. The distance of the CSS code in Theorem 1 is $\tilde{N}/2$.

Proof of Lemma 4 is in Appendix B. Lemma 4 implies that the CSS code can correct any $(\tilde{N}/2 - 1)$ -qubit erasure errors. Although the distance of this CSS code scales as $O(\tilde{N})$, Lemma 3 implies that the CSS code can correct particular erasure errors at $O(\tilde{N}^2)$ qubits.

This subsection has specified the CSS code (1) by its stabilizer generator matrix (56). We have shown the erasure errors that the CSS code, can correct and the distance of the CSS code. In next subsection, we explain how to encode and decode this CSS code.

C. Encoding and decoding

In last subsection, we have shown that the encoding of our CSS code employs $O(N^2)$ qubits while the decoding uses only $O(N)$ qubits. In this subsection, we present systematic methods to construct encoding and decoding circuits for our CSS code. The encoding method used here follows the standard method of encoding stabilizer codes [21], discussed in Subsec. II B. Our decoding method differs from the stabilizer code decoding method because it only corrects erasure errors, which occur in summoning. We also calculate the gate complexity of both the encoding and the decoding circuits. It is shown that G in the encoding is $O(N^2)$ and G in the decoding is $O(N)$.

To build the encoding circuit of this CSS code, we introduce logical operations on the encoded state. By using the vector representation (6), the logical operations are defined as

$$\bar{X} := \begin{bmatrix} \mathbf{0} & \mathbf{A}_1 \end{bmatrix} \quad (58)$$

and

$$\bar{Z} := \begin{bmatrix} \mathbf{A}_1 & \mathbf{0} \end{bmatrix}. \quad (59)$$

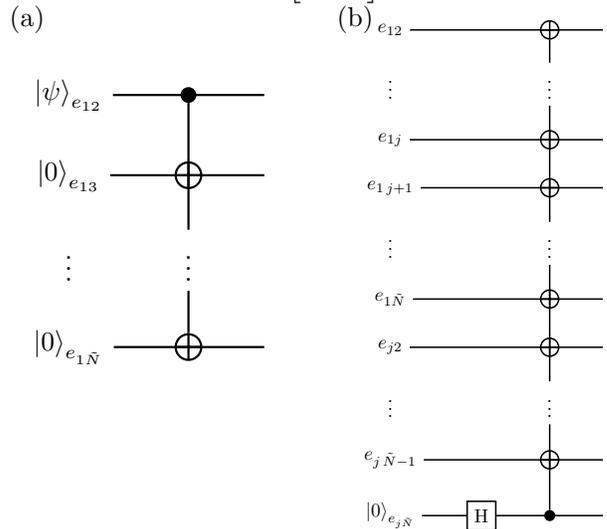


FIG. 5: (a) Multiple CNOT gates with $|\psi\rangle_{e_{12}}$ as the control qubit and $\{|0\rangle_{e_{1i}}\}_{i=2}^{\tilde{N}}$ as the target qubits; (b) A Hadamard gate is applied at $|0\rangle_{e_{jN}}$ followed by multiple CNOT gates with $|0\rangle_{e_{jN}}$ as the control qubit and the qubits assigned to $\{e_{1l}\}_{l=[\tilde{N}], l \neq j} \cup \{e_{jk}\}_{k=2}^{\tilde{N}-1}$ as target qubits.

From $\mathbf{A}_1 \cdot \mathbf{A}_1 = 1$ and Eq. (8), \bar{X} and \bar{Z} anti-commute with each other.

We choose

$$|\psi_0\rangle = |\mathbf{0}\rangle := |0\rangle^{\binom{\tilde{N}}{2}}, \quad (60)$$

which is an eigenstate of \bar{Z} with eigenvalue one. To encode $|\psi\rangle$ (47), using Eqs. (14) and (15), and the fact that Z -type stabilizers act trivially on $|\psi_0\rangle$, we obtain the encoded state

$$\alpha |0\rangle_L + \beta |1\rangle_L = \frac{1}{\sqrt{2^{\tilde{N}-2}}} \prod_{j=2}^{\tilde{N}-1} \left(I + \bigotimes_{i=1}^{\binom{\tilde{N}}{2}} X^{(\mathbf{A}_1 + \mathbf{A}_j)_i} \right) (\alpha |\mathbf{0}\rangle + \beta |\mathbf{A}_1\rangle), \quad (61)$$

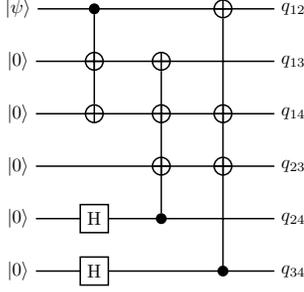


FIG. 6: The encoding circuit of the CSS code comprising Hadamard gates and CNOT gates when $\tilde{N} = 4$. The inputs of this circuit are $|\psi\rangle \otimes |00000\rangle$ and the outputs of this circuit are the qubits assigned to each edge of the complete graph K_4 shown in Fig. 4(b).

where

$$|\mathbf{A}_1\rangle = \prod_{i=1}^{\binom{\tilde{N}}{2}} X^{(\mathbf{A}_1)_i} |0\rangle, \quad (62)$$

and $(\mathbf{A}_1 + \mathbf{A}_j)_i$ and $(\mathbf{A}_1)_i$ are the i -th entries of vectors $\mathbf{A}_1 + \mathbf{A}_j$ and \mathbf{A}_1 respectively.

S applies CNOT gates as in Fig. 5(a) to the product state

$$|\psi\rangle \otimes |0\rangle^{\binom{\tilde{N}}{2}-1}, \quad (63)$$

to obtain

$$\alpha |\mathbf{0}\rangle + \beta |\mathbf{A}_1\rangle. \quad (64)$$

Then S implements each operation

$$I + \bigotimes_{i=1}^m X^{(\mathbf{A}_1 + \mathbf{A}_j)_i}, \quad (65)$$

where $1 \leq j \leq \tilde{N} - 2$, by using CNOT gates and a Hadamard gate as in Fig. 5(b). Finally, S obtains the encoded state (61). Figure 6 presents an example of the encoding circuit for $\tilde{N} = 4$.

The number of CNOT gates in Fig. 5(a) is $O(N)$. In Fig. 5(b), the number of CNOT gates is $O(N)$ and the number of Hadamard gate is one. As the circuit in Fig. 5(a) is only applied once and the circuit in Fig. 5(b) must be applied $O(N)$ times. the encoding of the CSS code consumes $O(N^2)$ CNOT gates and $O(N)$ Hadamard gates. Hence, for the encoding of the CSS code, $G \in O(N^2)$.

The decoding scheme is explained in the following. Suppose the request is sent to y_r . Reveal agent A_{z_r} cannot decode by measuring the syndromes as she has only $\tilde{N} - 1$ qubits. The encoded state (61) is an equally weighted superposition of the codewords given

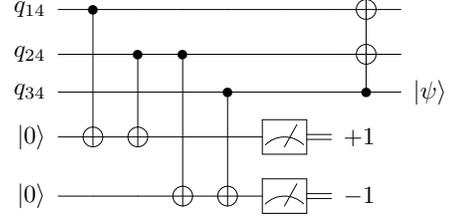


FIG. 7: One example of the decoding circuit comprising CNOT gates and measurements of Z operators for $\tilde{N} = 4$. The inputs of the circuit are three physical qubits q_{14} , q_{24} and q_{34} and two ancillary qubits $|00\rangle$. The measurement outcomes on the two ancillary qubits are $+1$ and -1 , based on which two CNOT gates are applied with the third qubit as the control qubit and the first two qubits as the target qubits. The third output qubit is the original qubit $|\psi\rangle$.

in Eqs. (C1) and (C2) (see Appendix C). After tracing out the lost qubits, the reduced state ρ_r (C12) becomes a mixture of the codewords. To decode the original state $|\psi\rangle$ from the $\tilde{N} - 1$ qubits with reduced density matrix ρ_r , reveal agent A_{z_r} measures the set of mutually commutative Hermitian operators

$$\left\{ Z_{q_{rk}} Z_{q_{r,k+1}}; k \in [\tilde{N} - 1] \setminus \{r\} \right\}, \quad (66)$$

where $Z_{q_{rk}}$ represents the Z operator on the qubit q_{rk} . After applying the projective measurements, the reduced state is projected onto one codeword, becoming a pure state (see Appendix C).

According to the measurement outcomes, by applying $\tilde{N} - 2$ CNOT gates with one control qubit and distinct target qubits, A_{z_r} obtains the original state $|\psi\rangle$ at the control qubit. Fig. 7 presents an example of the decoding circuit when the request is received at $\diamond 4$. In decoding, $G \in O(N)$ and the number of single-qubit measurements is also $O(N)$.

D. Comparison with the CWS code

Now we compare the quantum resources required by our CSS code with Hayden and May's CWS code. To investigate the complexity of the encoding of the CWS code, we need to know the complexity of preparing graph state $|G_{CWS}\rangle$. From Eq. (33), we know that the number of controlled- Z gates and Hadamard gates in preparing a graph state equals to the number of edges and vertices in the graph, respectively. The numbers of edges and vertices in G_{CWS} are

$$|E(G_{CWS})| = \frac{N(N-1)^2}{2}, \quad (67)$$

$$|V(G_{CWS})| = N(N-1). \quad (68)$$

Thus, preparing $|G_{\text{CWS}}\rangle$ requires $O(N^3)$ controlled- Z gates and $O(N^2)$ Hadamard gates. Applying the codeword operators (34) requires additional $O(N^2)$ controlled- Z gates.

In conclusion, the encoding of the CWS code consumes $O(N^3)$ controlled- Z gates and $O(N^2)$ Hadamard gates. Compared with the CWS code, our CSS code reduces G for encoding from $O(N^3)$ to $O(N^2)$.

Our protocol employs a CSS code to summon quantum information in any valid configuration. The CSS code can correct the erasure errors that occur in the quantum summoning task. The encoding and the decoding methods for this CSS code have been presented. Finally, we have compared the complexity of the encoding of the CSS code with the encoding of the CWS code and found that our CSS code is more efficient.

V. DISCUSSION

We have presented a protocol to summon quantum information efficiently in any valid configuration of causal diamonds. Central to our protocol is a CSS code that encodes one logical qubit into $O(N^2)$ physical qubits, where each physical qubit is assigned to an edge of a complete graph whose vertices correspond to causal diamonds. This code is a qubit version of the homological continuous-variable quantum error correcting code [3]. The CSS code is designed using the fact that the power set of edges of a complete graph can be cast as a vector space. The stabilizer generators of the CSS code correspond to triangle graphs and sums of star graphs.

The properties of these graphs are used to show that the logical qubit can be decoded from the subset of physical qubits that are assigned to edges adjacent to any vertex. In order to employ this code for summoning, the physical qubits are sent to the request points in such a way that the past of every reveal point contains enough physical qubits to decode the original qubit. Our protocol design, similar to one used previously [3], ensures that whenever a request agent receives the request the associated reveal agent receives all physical qubits required to decode the original qubit.

We also present procedures to design the encoding and decoding circuits for the CSS code. We show that our protocol is less resource-intensive than the protocol based on the CWS code [2] which uses circuits that are $O(N^2)$ wide and $O(N^3)$ deep. The circuits for the CSS code have width that is also $O(N^2)$ but half that of the CWS code and require only $O(N^2)$ gates.

VI. CONCLUSION

Our protocol for summoning is designed to work for any valid configuration of causal diamonds, where the underlying CSS code depends only on the number of causal

diamonds. It is likely that codes can be designed that reduce resource usage by exploiting the structure of causal connections between the causal diamonds, examples being when a single causal curve connects multiple causal diamonds [3] or when the graph representing causal connections is acyclic [4].

While any given configuration of causal diamonds may be realized in man-made quantum networks, a useful avenue of research would be to classify the configurations that can occur naturally in flat or curved spacetimes. Our codes as well as other codes for quantum summoning assume that entangled states may be transferred without decoherence in spacetime. Quantum summoning in curved spacetime or Rindler coordinates might require the usage of codes that protect against decoherence caused due to gravity or acceleration [30–32].

Acknowledgments

We thank Dominic Berry, Dong-Xiao Quan, Masoud Habibi Davijani, Yun-Jiang Wang and Wei-Wei Zhang for helpful discussions and acknowledge funding from Alberta Innovates, NSERC, China's 1000 Talent Plan, and the Institute for Quantum Information and Matter, an NSF Physics Frontiers Center (NSF Grant PHY-1125565) with support of the Gordon and Betty Moore Foundation (GBMF-2644).

Appendix A: Proof of Lemma 3

Proof. Denote \mathcal{E}_r as the set of Pauli operators at qubits q_{ij} for $i, j \in [\tilde{N}] \setminus \{r\}$. For any Pauli operator $P \in \mathcal{E}_r$, its vector representation (6) is denoted

$$P = \begin{bmatrix} \mathbf{P}_Z & \mathbf{P}_X \end{bmatrix}. \quad (\text{A1})$$

As P acts nontrivially only at qubits q_{ij} for $i, j \in [\tilde{N}] \setminus \{r\}$,

$$\forall k \in [\tilde{N}] \setminus \{r\}, \mathbf{P}_Z \cdot \mathbf{e}_{rk} = \mathbf{P}_X \cdot \mathbf{e}_{rk} = 0. \quad (\text{A2})$$

To show that the stabilizer code in Theorem 1 can correct any error in \mathcal{E}_r for every r , it is sufficient to prove that [21]

$$\forall P \in \mathcal{E}_r, P \in C(\mathcal{S}) \Rightarrow P \in \mathcal{S}, \quad (\text{A3})$$

where \mathcal{S} is the stabilizer group generated by the stabilizer generators in $H_{\tilde{N}}$ (56) and $C(\mathcal{S})$ is the centralizer of \mathcal{S} in $\mathcal{G}_{\binom{\tilde{N}}{2}}$, i.e. the group of the Pauli operators commuting with all the elements of \mathcal{S} . Using Eq. (8), we know that $P \in C(\mathcal{S})$ if and only if

$$\forall \mathbf{v} \in \mathcal{C}_1^\perp, \mathbf{P}_X \cdot \mathbf{v} = 0, \quad (\text{A4})$$

and

$$\forall \mathbf{u} \in \mathcal{C}_2, \mathbf{P}_Z \cdot \mathbf{u} = 0. \quad (\text{A5})$$

From $\mathbf{T}_{rij} \in \mathcal{C}_1^\perp$ and Eq. (A4),

$$\mathbf{P}_X \cdot \mathbf{T}_{rij} = 0. \quad (\text{A6})$$

It implies that

$$\mathbf{P}_X \cdot (\mathbf{e}_{ri} + \mathbf{e}_{rj} + \mathbf{e}_{ij}) = 0. \quad (\text{A7})$$

Using Eq. (A2), we know that

$$\mathbf{P}_X \cdot \mathbf{e}_{ij} = 0. \quad (\text{A8})$$

Equation (A8), together with Eq. (A2), implies that $\mathbf{P}_X = \mathbf{0}$.

Next we prove that Eq. (A5) implies that $\mathbf{P}_Z \in \mathcal{C}_1^\perp$. Suppose

$$\mathbf{P}_Z \cdot \mathbf{A}_1 = 1. \quad (\text{A9})$$

Then Eq. (A5) implies that for $2 \leq l \leq \tilde{N} - 1$,

$$\mathbf{P}_Z \cdot \mathbf{A}_l = 1. \quad (\text{A10})$$

As \tilde{N} is even,

$$\sum_{m=1}^{\tilde{N}-1} \mathbf{P}_Z \cdot \mathbf{A}_m = 1. \quad (\text{A11})$$

As

$$\sum_{m=1}^{\tilde{N}} \mathbf{P}_Z \cdot \mathbf{A}_m = \mathbf{P}_Z \cdot \sum_{m=1}^{\tilde{N}} \mathbf{A}_m = 0, \quad (\text{A12})$$

we have

$$\mathbf{P}_Z \cdot \mathbf{A}_{\tilde{N}} = 1. \quad (\text{A13})$$

Hence,

$$\forall k \in [\tilde{N}], \mathbf{P}_Z \cdot \mathbf{A}_k = 1. \quad (\text{A14})$$

Equation (A14) contradicts Eq. (A2) because Eq. (A2) implies that

$$\mathbf{P}_Z \cdot \mathbf{A}_r = 0. \quad (\text{A15})$$

Thus, (A9) is false and

$$\mathbf{P}_Z \cdot \mathbf{A}_1 = 0. \quad (\text{A16})$$

Then Eq. (A5) indicates that for $2 \leq l \leq \tilde{N} - 1$,

$$\mathbf{P}_Z \cdot \mathbf{A}_l = 0. \quad (\text{A17})$$

Hence

$$\sum_{m=1}^{\tilde{N}-1} \mathbf{P}_Z \cdot \mathbf{A}_m = 0. \quad (\text{A18})$$

From Eq. (A12), we know that

$$\mathbf{P}_Z \cdot \mathbf{A}_{\tilde{N}} = 0. \quad (\text{A19})$$

Thus,

$$\forall k \in [\tilde{N}], \mathbf{P}_Z \cdot \mathbf{A}_k = 0, \quad (\text{A20})$$

which indicates that $\mathbf{P}_Z \in \mathcal{C}_1^\perp$. Since $\mathbf{P}_X = \mathbf{0}$, we know that P is a Z -type stabilizer in \mathcal{S} . \square

Appendix B: Proof of Lemma 4

Proof. The distance (10) of the stabilizer code in Theorem 1 equals to the minimum weight of the Pauli operators in $C(\mathcal{S}) \setminus \mathcal{S}$ [21]. To prove the minimum weight of the Pauli operators in $C(\mathcal{S}) \setminus \mathcal{S}$ is $\tilde{N}/2$, we first show that there exists a Pauli operator

$$P := \bigotimes_{i=1}^{\tilde{N}/2} Z_{q_{2i-1}, 2i} \quad (\text{B1})$$

with weight $\tilde{N}/2$ such that $P \in C(\mathcal{S}) \setminus \mathcal{S}$. Then we show that no Pauli operator with weight less than $\tilde{N}/2$ lies in $C(\mathcal{S}) \setminus \mathcal{S}$.

From Eq (B1), we know that

$$\mathbf{P}_Z = \sum_{i=1}^{\tilde{N}/2} \mathbf{e}_{2i-1, 2i}, \mathbf{P}_X = \mathbf{0}. \quad (\text{B2})$$

From Eq. (B2), we find that

$$\forall l \in [\tilde{N}], \mathbf{P}_Z \cdot \mathbf{A}_l = 1. \quad (\text{B3})$$

Hence,

$$\forall \mathbf{v} \in \mathcal{C}_2, \mathbf{P}_Z \cdot \mathbf{v} = 0. \quad (\text{B4})$$

From the fact that $\mathbf{P}_X = \mathbf{0}$, we know that P (B1) commutes with all the stabilizers in \mathcal{S} , i.e., $P \in C(\mathcal{S})$. As \mathbf{P}_Z cannot be represented by an Euclidean cycle,

$$\mathbf{P}_Z \notin \mathcal{C}_1^\perp. \quad (\text{B5})$$

Thus, $P \notin \mathcal{S}$, and hence

$$P \in C(\mathcal{S}) \setminus \mathcal{S}. \quad (\text{B6})$$

For any Pauli operator P' with weight less than $\tilde{N}/2$, there exists an $r \in [\tilde{N}]$ such that

$$\forall k \in [\tilde{N}] \setminus \{r\}, \mathbf{P}'_Z \cdot \mathbf{e}_{rk} = \mathbf{P}'_X \cdot \mathbf{e}_{rk} = 0. \quad (\text{B7})$$

From the discussion in Appendix A, we know that

$$P' \in C(\mathcal{S}) \Rightarrow P' \in \mathcal{S}. \quad (\text{B8})$$

It implies that

$$P' \notin C(\mathcal{S}) \setminus \mathcal{S}. \quad (\text{B9})$$

Thus, no Pauli operator with weight less than $\tilde{N}/2$ lies in $C(\mathcal{S}) \setminus \mathcal{S}$. \square

Appendix C: Reduced density matrix

In this appendix, we calculate the reduced density matrix ρ_r and show the state after the measurements of the operators in Eq. (66).

From Eqs. (14) and (15),

$$|0\rangle_L = \frac{1}{\sqrt{2^{\tilde{N}-2}}} \sum_{\mathbf{x} \in \mathcal{C}_2} |\mathbf{x}\rangle, \quad (\text{C1})$$

$$|1\rangle_L = \frac{1}{\sqrt{2^{\tilde{N}-2}}} \sum_{\mathbf{x} \in \mathcal{C}_2} |\mathbf{A}_1 + \mathbf{x}\rangle, \quad (\text{C2})$$

form a basis of the CSS code in Theorem 1. Hence, the density matrix of the $\binom{\tilde{N}}{2}$ physical qubits encoding $|\psi\rangle$ (47) is

$$\begin{aligned} \rho &= \frac{1}{2^{\tilde{N}-2}} \sum_{\mathbf{x} \in \mathcal{C}_2} (\alpha |\mathbf{x}\rangle + \beta |\mathbf{A}_1 + \mathbf{x}\rangle) \\ &\quad \times \sum_{\mathbf{y} \in \mathcal{C}_2} (\alpha^* \langle \mathbf{y} | + \beta^* \langle \mathbf{A}_1 + \mathbf{y} |). \end{aligned} \quad (\text{C3})$$

To express the reduced density matrix, we give the following notations. The subset of edges connected to \diamond_r in $K_{\tilde{N}}$ is denoted by E_r and the complement of E_r in E ,

i.e. the subset of edges not connected to \diamond_r , is denoted by E_r^c . In the same way as 2^{E_K} forms a linear space

$$\mathcal{E} \cong \mathbb{Z}_2^{\binom{\tilde{N}}{2}},$$

the power set 2^{E_r} forms a linear subspace

$$\mathcal{E}_r \cong \mathbb{Z}_2^{\tilde{N}-1} \quad (\text{C4})$$

and the power set $2^{E_r^c}$ forms the orthogonal complement of \mathcal{E}_r in \mathcal{E} , denoted by

$$\mathcal{E}_r^\perp \cong \mathbb{Z}_2^{\binom{\tilde{N}-1}{2}}. \quad (\text{C5})$$

For a vector $\mathbf{v} \in \mathcal{E}$, we use \mathbf{v}_r to denote the projection of \mathbf{v} onto \mathcal{E}_r , and \mathbf{v}_r^\perp to denote the projection of \mathbf{v} onto \mathcal{E}_r^\perp .

Now we calculate the reduced density matrix ρ_r of the $\tilde{N} - 1$ qubits $\{q_{rk}; k \in [\tilde{N}] \setminus \{r\}\}$. As

$$\forall r \in [\tilde{N}], \sum_{\mathbf{x} \in \mathcal{C}_2} |\mathbf{A}_r + \mathbf{x}\rangle = \sum_{\mathbf{x} \in \mathcal{C}_2} |\mathbf{A}_1 + \mathbf{x}\rangle, \quad (\text{C6})$$

$$\rho_r = \frac{1}{2^{\tilde{N}-2}} \text{tr}_{E_r^c} \left[\sum_{\mathbf{x} \in \mathcal{C}_2} (\alpha |\mathbf{x}\rangle + \beta |\mathbf{A}_r + \mathbf{x}\rangle) \sum_{\mathbf{y} \in \mathcal{C}_2} (\alpha^* \langle \mathbf{y} | + \beta^* \langle \mathbf{A}_r + \mathbf{y} |) \right], \quad (\text{C7})$$

where $\text{tr}_{E_r^c}$ denotes the partial trace over the qubits $\{q_{ij}; i, j \in [\tilde{N}] \setminus \{r\}\}$. From the definition of partial trace [33],

$$\rho_r = \frac{1}{2^{\tilde{N}-2}} \sum_{\mathbf{v} \in \mathcal{E}_r^\perp} \left\langle \mathbf{v} \left| \sum_{\mathbf{x} \in \mathcal{C}_2} (\alpha |\mathbf{x}\rangle + \beta |\mathbf{A}_r + \mathbf{x}\rangle) \sum_{\mathbf{y} \in \mathcal{C}_2} (\alpha^* \langle \mathbf{y} | + \beta^* \langle \mathbf{A}_r + \mathbf{y} |) \right| \mathbf{v} \right\rangle. \quad (\text{C8})$$

For each $\mathbf{v} \in \mathcal{E}_r^\perp$, there is at most one $\mathbf{x} \in \mathcal{C}_2$ such that

$$\mathbf{x}_r^\perp = \mathbf{v}. \quad (\text{C9})$$

Hence, we get

$$\rho_r = \frac{1}{2^{\tilde{N}-2}} \sum_{\mathbf{x} \in \mathcal{C}_2} \langle \mathbf{x}_r^\perp | (\alpha |\mathbf{x}\rangle + \beta |\mathbf{A}_r + \mathbf{x}\rangle) (\alpha^* \langle \mathbf{x} | + \beta^* \langle \mathbf{A}_r + \mathbf{x} |) | \mathbf{x}_r^\perp \rangle. \quad (\text{C10})$$

As

$$\langle \mathbf{x}_r^\perp | \mathbf{x} \rangle = |\mathbf{x}_r\rangle \quad \text{and} \quad \langle \mathbf{x}_r^\perp | \mathbf{A}_r + \mathbf{x} \rangle = |\mathbf{1} + \mathbf{x}_r\rangle, \quad (\text{C11})$$

where $\mathbf{1}$ is an $(\tilde{N} - 1)$ -dimensional vector with all the entries equal to 1,

$$\rho_r = \frac{1}{2^{\tilde{N}-2}} \sum_{\mathbf{x} \in \mathcal{C}_2} (\alpha |\mathbf{x}_r\rangle + \beta |\mathbf{1} + \mathbf{x}_r\rangle) (\alpha^* \langle \mathbf{x}_r | + \beta^* \langle \mathbf{1} + \mathbf{x}_r |). \quad (\text{C12})$$

Consider the set of mutually commutative Hermitian operators in (66)

$$\{Z_{q_{rk}} Z_{q_{r,k+1}}; k \in [\tilde{N} - 1] \setminus \{r\}\}.$$

$\forall \mathbf{x} \in \mathcal{C}_2$, $|\mathbf{x}_r\rangle$ and $|\mathbf{1} + \mathbf{x}_r\rangle$ are the eigenstates of each Hermitian operator in (66) with same eigenvalue, so any linear combination

$$\alpha |\mathbf{x}_r\rangle + \beta |\mathbf{1} + \mathbf{x}_r\rangle$$

is a common eigenstate of the Hermitian operators (66), with the eigenvalues forming a vector consisting of ± 1 . For

$$\forall \mathbf{x}, \mathbf{z} \in \mathcal{C}_2 \text{ and } \mathbf{x} \neq \mathbf{z}, \quad (\text{C13})$$

the two eigenstates

$$\alpha |\mathbf{x}_r\rangle + \beta |\mathbf{1} + \mathbf{x}_r\rangle \quad (\text{C14})$$

and

$$\alpha |\mathbf{z}_r\rangle + \beta |\mathbf{1} + \mathbf{z}_r\rangle \quad (\text{C15})$$

have different eigenvalue vectors. This is because if (C14) and (C15) have the same eigenvalues, then either $\mathbf{x}_r = \mathbf{z}_r$ or $\mathbf{x}_r = \mathbf{z}_r + \mathbf{1}$, both of which contradict condition (C13). Thus, ρ_r in Eq. (C12) is an equally weighted mixture of the common eigenstates of the Hermitian operators (66) with different eigenvalue vectors.

After the projective measurements on all the Hermitian operators (66), the reduced state is projected onto

$$\alpha |\mathbf{y}_r\rangle + \beta |\mathbf{1} + \mathbf{y}_r\rangle, \quad (\text{C16})$$

where $\mathbf{y} \in \mathcal{C}_2$ and \mathbf{y}_r is the projection of \mathbf{y} onto \mathcal{E}_r . The corresponding measurement outcomes are $\left\{ (-1)^{\mathbf{y}_r^{(i)} + \mathbf{y}_r^{(i+1)}}; i \in [\tilde{N} - 2] \right\}$, where $\mathbf{y}_r^{(i)}$ is the i -th component in \mathbf{y}_r . (C16) is the state after the measurements of the Hermitian operators in (66).

-
- [1] A. Kent, *Quantum Inf. Process.* **12**, 1023 (2013), URL <http://dx.doi.org/10.1007/s11128-012-0431-6>.
- [2] P. Hayden and A. May, *J. Phys. A* **49**, 175304 (2016), URL <http://stacks.iop.org/1751-8121/49/i=17/a=175304>.
- [3] P. Hayden, S. Nezami, G. Salton, and B. C. Sanders, *New J. Phys.* **18**, 083043 (2016), URL <http://stacks.iop.org/1367-2630/18/i=8/a=083043>.
- [4] E. Adlam and A. Kent, *Phys. Rev. A* **93**, 062327 (2016), URL <http://link.aps.org/doi/10.1103/PhysRevA.93.062327>.
- [5] J. L. Park, *Found. Phys.* **1**, 23 (1970), URL <https://doi.org/10.1007/BF00708652>.
- [6] W. K. Wootters and W. H. Zurek, *Nature* **299**, 802 (1982), URL <http://dx.doi.org/10.1038/299802a0>.
- [7] D. Dieks, *Phys. Lett. A* **92**, 271 (1982), URL <http://www.sciencedirect.com/science/article/pii/0375960182900846>.
- [8] J. Ortigoso, arXiv:1707.06910 (2017).
- [9] R. Cleve, D. Gottesman, and H.-K. Lo, *Phys. Rev. Lett.* **83**, 648 (1999), URL <https://link.aps.org/doi/10.1103/PhysRevLett.83.648>.
- [10] D. Gottesman, *Phys. Rev. A* **61**, 042311 (2000), URL <http://link.aps.org/doi/10.1103/PhysRevA.61.042311>.
- [11] D. Markham and B. C. Sanders, *Phys. Rev. A* **78**, 042309 (2008), URL <https://link.aps.org/doi/10.1103/PhysRevA.78.042309>.
- [12] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, *Phys. Rev. Lett.* **70**, 1895 (1993), URL <https://link.aps.org/doi/10.1103/PhysRevLett.70.1895>.
- [13] R. F. Werner, *J. Phys. A* **34**, 7081 (2001), URL <http://stacks.iop.org/0305-4470/34/i=35/a=332>.
- [14] A. Cross, G. Smith, J. A. Smolin, and B. Zeng, *IEEE Trans. Inf. Theory* **55**, 433 (2009).
- [15] A. R. Calderbank and P. W. Shor, *Phys. Rev. A* **54**, 1098 (1996), URL <https://link.aps.org/doi/10.1103/PhysRevA.54.1098>.
- [16] A. Steane, *Proc. Royal Soc. A* **452**, 2551 (1996), URL <http://rspa.royalsocietypublishing.org/content/452/1954/2551>.
- [17] R. Diestel, *Graph Theory*, vol. 173 of *Graduate Texts in Mathematics* (Springer-Verlag, Heidelberg, 2016).
- [18] H. Bombin and M. A. Martin-Delgado, *J. Math. Phys.* **48**, 052105 (2007), URL <http://dx.doi.org/10.1063/1.2731356>.
- [19] P. W. Shor, *Phys. Rev. A* **52**, R2493 (1995), URL <https://link.aps.org/doi/10.1103/PhysRevA.52.R2493>.
- [20] A. M. Steane, *Phys. Rev. Lett.* **77**, 793 (1996), URL <https://link.aps.org/doi/10.1103/PhysRevLett.77.793>.
- [21] D. Gottesman, Ph.D. thesis, California Institute of Technology (1997).
- [22] P. Preskill, *Lecture Notes for Physics 229: Quantum Information and Computation* (CreateSpace Independent Publishing Platform, North Charleston, 2015).
- [23] M. Grassl, T. Beth, and T. Pellizzari, *Phys. Rev. A* **56**, 33 (1997), URL <https://link.aps.org/doi/10.1103/PhysRevA.56.33>.
- [24] S. Roman, *Advanced Linear Algebra*, vol. 135 of *Graduate Texts in Mathematics* (Springer Science+Business Media, New York, 2005).
- [25] R. Lidl and H. Niederreiter, *Finite Fields* (Cambridge university press, Cambridge, 1997).
- [26] R. Raussendorf, D. E. Browne, and H. J. Briegel, *Phys. Rev. A* **68**, 022312 (2003), URL <https://link.aps.org/doi/10.1103/PhysRevA.68.022312>.
- [27] E. F. Taylor and J. A. Wheeler, *Spacetime Physics: Introduction to Special Relativity* (W. H. Freeman, New York, 1992).
- [28] S. D. Bartlett, B. C. Sanders, S. L. Braunstein, and K. Nemoto, *Phys. Rev. Lett.* **88**, 097904 (2002), URL <https://link.aps.org/doi/10.1103/PhysRevLett.88.097904>.
- [29] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, *Rev. Mod. Phys.* **84**, 621 (2012), URL <http://link.aps.org/doi/10.1103/RevModPhys.84.621>.
- [30] P. M. Alsing and G. J. Milburn, *Phys. Rev. Lett.*

- 91**, 180404 (2003), URL <https://link.aps.org/doi/10.1103/PhysRevLett.91.180404>.
- [31] N. Friis, A. R. Lee, K. Truong, C. Sabín, E. Solano, G. Johansson, and I. Fuentes, Phys. Rev. Lett. **110**, 113602 (2013), URL <https://link.aps.org/doi/10.1103/PhysRevLett.110.113602>.
- [32] M. Ahmadi, Y.-D. Wu, and B. C. Sanders, Phys. Rev. D **96**, 065018 (2017), URL <https://link.aps.org/doi/10.1103/PhysRevD.96.065018>.
- [33] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, Cambridge, 2010).