

# Transversal Toffoli-gate in Hybrid-code System

Dawei Jiao<sup>1</sup>, Mahdi Bayanifar<sup>1</sup>, Alexei Ashikhmin<sup>2</sup>, Olav Tirkkonen<sup>1</sup>

<sup>1</sup>*Department of Communications and Networking, Aalto University, Finland*

<sup>2</sup>*Nokia Bell Labs, Murray Hill, New Jersey, USA*

*Email: {dawei.jiao, mahdi.bayanifar, olav.tirkkonen}@aalto.fi  
alexei.ashikhmin@nokia-bell-labs.com*

**Abstract**—We study the transversality of the Toffoli gate in a hybrid-code system that employs two quantum error correction codes with special structure. We find that a system using a tri-orthogonal code with its paired code supports a fully transversal implementation of the Toffoli gate. Through circuit-level analysis, we prove the transversality of the Toffoli operation in this system. Based on this hybrid-code framework, we propose a Toffoli state distillation protocol that does not rely on pre-distilled T-gate magic states. In our approach, the Toffoli state is directly distilled layer by layer within the hybrid-code system using only transversal operations. Numerical simulations demonstrate that our method uses approximately 50% fewer qubit resources than previously reported protocols.

## I. INTRODUCTION

Fault-tolerant quantum computation relies on carefully designed circuits to prevent the propagation of errors during quantum operations [1], [2]. Transversal gates play an important role in this process, as they act in parallel on each qubit of encoded blocks, thereby naturally preserving the fault-tolerance. Compared with other fault-tolerant approaches, such as magic state and gauge fixing, the transversal gates approach does not require any additional resource costs [3]–[5]. Every quantum error correction code (QECC) supports a gate set that can be applied transversally. However, according to the Easting-Knill theorem, it is not possible to have a universal and transversal set of gates simultaneously for a given QECC [2]. Some conventional QECCs, such as surface code and Steane code, support the Clifford gate set transversal realizations, but universal quantum computation additionally requires the inclusion of non-Clifford gates such as the T-gate or the controlled-controlled-phase (CCZ) gate [6].

The transversality of some non-Clifford gates, such as T-gate and CCZ gate, have been extensively studied [4], [7], [8]. In particular, triorthogonal codes have been shown to admit transversal T and CCZ gates under certain constraints on their logical operators [4], [7]. Besides these gates, there is another well-known non-Clifford gate, called Toffoli-gate. It is a three-qubit gate that performs a controlled-NOT operation on a target qubit condition on the state of two control qubits. The Toffoli gate is frequently used in both reversible classical computation [9] and more complex algorithms, such as Shor’s algorithm [10]. The complexity of implementing Toffoli gate highly depends on the overall complexity of the algorithm. However, the transversality of the Toffoli gate has rarely been discussed. Even it is shown that no single QECC can support a

transversal Toffoli gate [8]. The use of multiple QECCs in one quantum system in a transversal manner is investigated in [11], where the authors introduced a mirrored code design that enables a transversal CZ gate between two different QECCs.

Motivated by these observations, in this paper we study the transversality of the Toffoli gate using different QECCs. In particular, we identify a scheme that employs two distinct QECCs, enabling a fully transversal implementation of the Toffoli gate. To support this approach, we introduce the concept of a *hybrid-code system*, in which multiple QECCs coexist and interact within the same quantum system. In the context of the logical Toffoli-gate, we construct such a system by encoding the control and target qubits using distinct, but structural-related codes. Specifically, we show that combining a triorthogonal code with its mirrored code enables a transversal realization of the Toffoli-gate.

Furthermore, this hybrid-code system can be used as distillation protocol to prepare high-fidelity Toffoli magic state, which is used to realize high-fidelity Toffoli gates. Since magic states are key resources in fault-tolerant quantum computation, minimizing the cost of their preparation is crucial. There exist several different Toffoli state distillation protocols [12]–[14], each using different circuit decompositions of Toffoli gate into T and Clifford gates. In these approaches, the T-gate is implemented using distilled magic states, and the final Toffoli state is obtained by using a large number of magic states. In contrast, our distillation protocol is implemented entirely in a transversal manner, eliminating the need for magic states. The Toffoli state is directly distilled layer by layer within the hybrid-code system. Using this approach, we achieve approximately a 50% reduction in qubit resources compared to existing protocols.

The rest of the paper is organized as follows: Sec. II introduces preliminaries on Calderbank-Shor-Steane (CSS) code, transversality and triorthogonal codes. In Sec. III we show the structure of our hybrid-code system and prove the Toffoli gate transversality. Our new proposed Toffoli state distillation procedure is mentioned in Sec. IV. Finally, in Sec. V using numerical simulations, we demonstrate that our proposed protocol reduces the qubit number cost compared to other Toffoli state distillation protocols.

## II. PRELIMINARIES

### A. CSS Codes

CSS quantum error correction codes are a special case of stabilizer codes. They can be constructed based on two classical linear codes  $\mathcal{C}_1(n, k_1, d_1)$  and  $\mathcal{C}_2(n, k_2, d_2)$ , such that  $\mathcal{C}_2^\perp \subset \mathcal{C}_1$ , with  $\mathcal{C}_2^\perp$  the dual space of  $\mathcal{C}_2$ . A quantum  $[[n, k, d]]$  CSS code  $\mathcal{Q} = \text{CSS}(\mathcal{C}_1, \mathcal{C}_2)$ , is defined as a  $2^k$ -dimensional linear subspace of  $\mathbb{C}^{2^n}$  with orthonormal basis [15]:

$$|\psi\rangle_L = \frac{1}{\sqrt{|\mathcal{C}_2^\perp|}} \sum_{\mathbf{y} \in \mathcal{C}_2^\perp} |\mathbf{x}_\psi + \mathbf{y}\rangle, \quad (1)$$

where  $\psi \in \mathbb{F}_2^k$  and  $\mathbf{x}_\psi = \psi \mathbf{A}$ , where  $\mathbf{A} \in \mathbb{F}_2^{k \times n}$  is a full-rank mapping matrix which is the generator of the quotient group  $\mathcal{C}_1/\mathcal{C}_2^\perp$ , i.e.,  $\mathbf{A} \cong \mathcal{C}_1/\mathcal{C}_2^\perp$ . Note that  $k = k_1 + k_2 - n$  and the code minimum distance is  $d = \min(d_1, d_2^\perp)$ . The generator matrix of  $\text{CSS}(\mathcal{C}_1, \mathcal{C}_2)$  is:

$$\mathbf{G}^{\mathcal{Q}} = \begin{bmatrix} \mathbf{H}(\mathcal{C}_2) & \mathbf{0} \\ \mathbf{0} & \mathbf{H}(\mathcal{C}_1) \end{bmatrix}. \quad (2)$$

The dimension of  $\mathbf{G}^{\mathcal{Q}}$  is  $(n - k) \times 2n$ . Thus, with  $n$  qubits and  $n - k$  generators,  $\mathcal{Q}$  encodes  $k$  logical qubits. If  $\mathcal{C}_1 = \mathcal{C}_2 = \mathcal{C}$ , we have a symmetric CSS code  $\text{CSS}(\mathcal{C}, \mathcal{C})$ .

### B. Transversality

Each QECC has its transversal gate set. The  $\mathbf{U}$  gate transversality for a  $[[n, k, d]]$  code is defined as:

$$\mathbf{U}^{\otimes n} |\psi\rangle = \mathbf{U}_L^{\otimes k} |\psi\rangle, \quad (3)$$

where  $\mathbf{U}_L$  is the logical  $\mathbf{U}$  gate, and  $|\psi\rangle$  is arbitrary logical state.

Let  $\mathbf{U}$  be a  $2^m \times 2^m$  operator acting on  $m$  qubits. The concept of a code allowing a transversal implementation of  $\mathbf{U}$  can be formalized as a definition of a *U-transversal code* as follows. Let  $\hat{\mathbf{U}}_i$  be the  $2^{mn} \times 2^{mn}$  operator that applies  $\mathbf{U}$  to qubits with indices  $\{i + ln : 0 \leq l \leq m - 1\}$  among  $mn$  qubits. Assume that we have an  $[[n, k]]$  stabilizer code  $\mathcal{Q}$  and that  $\mathbf{E}$  is an encoding operator of  $\mathcal{Q}$ .  $\mathcal{Q}$  is  $\mathbf{U}$ -transversal if:

$$\begin{aligned} & \left( \prod_{i=1}^n \hat{\mathbf{U}}_i \right) \bigotimes_{j=1}^m (\mathbf{E} |\psi_j\rangle |0 \dots 0\rangle) \\ &= \mathbf{E}^{\otimes m} \left( \prod_{i=1}^k \hat{\mathbf{U}}_i \right) \bigotimes_{j=1}^m (|\psi_j\rangle |0 \dots 0\rangle), \end{aligned} \quad (4)$$

where  $|\psi_j\rangle \in \mathbb{C}^{2^k}$  are logical states before encoding, and the  $|0 \dots 0\rangle$  state corresponds to the  $n - k$  physical qubits initialized in the  $|0\rangle$  state for the encoding process.

All CSS codes have CNOT transversality. Symmetric CSS codes have in addition complete Clifford gate transversality. For non-Clifford gate transversality, the most commonly considered one is  $\mathbf{T} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$  gate transversality. Certain CSS codes belonging to a family known as triorthogonal codes have  $T$ -transversality [4]. This comes at the cost of losing the transversality of some Clifford gates.

In addition to transversality within the same code, we can also define transversality between different codes. We can extend the notion of transversality to hold across two distinct codes. Expanding on this, the standard definition (4) of transversality within the same code can be generalized to an ordered set of  $m$   $[[n, k]]$  stabilizer codes  $\mathcal{Q}_j$ ,  $j = 1, \dots, m$  with encoding operators  $\mathbf{E}_j$  as follows. The set of codes  $\mathcal{Q}_1, \dots, \mathcal{Q}_m$  are  $\mathbf{U}$ -transversal if:

$$\begin{aligned} & \left( \prod_{i=1}^n \hat{\mathbf{U}}_i \right) \bigotimes_{j=1}^m (\mathbf{E}_j |\psi_j\rangle |0 \dots 0\rangle) \\ &= \left( \bigotimes_{s=1}^m \mathbf{E}_s \right) \left( \prod_{i=1}^k \hat{\mathbf{U}}_i \right) \bigotimes_{j=1}^m (|\psi_j\rangle |0 \dots 0\rangle). \end{aligned} \quad (5)$$

In [11], authors found that the restrictions for having transversal logical CNOT from CSS code  $\text{CSS}(\mathcal{C}_1, \mathcal{C}_2)$  to  $\text{CSS}(\mathcal{C}_3, \mathcal{C}_4)$  are:

$$\mathcal{C}_1/\mathcal{C}_2^\perp \cong \mathcal{C}_3/\mathcal{C}_4^\perp, \quad \mathcal{C}_2^\perp \subseteq \mathcal{C}_4^\perp. \quad (6)$$

Also, the sufficient conditions for two CSS code  $\text{CSS}(\mathcal{C}_1, \mathcal{C}_2)$  and  $\text{CSS}(\mathcal{C}_3, \mathcal{C}_4)$  to have a transversal logical CZ gate are:

$$\mathcal{C}_1/\mathcal{C}_2^\perp \subseteq \mathcal{C}_4, \quad \mathcal{C}_3 \subseteq \mathcal{C}_2, \quad \mathbf{A}\mathbf{B}^T = \mathbf{I}, \quad (7)$$

where  $\mathbf{A}, \mathbf{B} \in \mathbb{F}_2^{k \times n}$ ,  $\mathbf{A} \cong \mathcal{C}_1/\mathcal{C}_2^\perp$ ,  $\mathbf{B} \cong \mathcal{C}_3/\mathcal{C}_4^\perp$  are two mapping matrices, of the kind discussed after (1).

If a QECC system is both  $\mathbf{U}_a$  and  $\mathbf{U}_b$  transversal, it is also  $\mathbf{U}_c = \mathbf{U}_a \mathbf{U}_b$  transversal. From the definition of transversality, we can say if  $\mathbf{U}_a$  and  $\mathbf{U}_b$  both fulfill the (5), we can have:

$$\begin{aligned} & \left( \prod_{i=1}^n \hat{\mathbf{U}}_{a_i} \right) \left( \prod_{i=1}^n \hat{\mathbf{U}}_{b_i} \right) \bigotimes_{j=1}^m (\mathbf{E}_j |\psi_j\rangle |0 \dots 0\rangle) \\ &= \left( \bigotimes_{s=1}^m \mathbf{E}_s \right) \left( \prod_{i=1}^k \hat{\mathbf{U}}_{a_i} \hat{\mathbf{U}}_{b_i} \right) \bigotimes_{j=1}^m (|\psi_j\rangle |0 \dots 0\rangle), \end{aligned} \quad (8)$$

thus we have  $\mathbf{U}_c$  transversality.

### C. Triorthogonal code

Triorthogonal codes are special type of CSS code, which are generated by triorthogonal matrices [16]. A binary matrix  $\mathbf{G}$  of size  $m$ -by- $n$  is triorthogonal if

1) for all pairs  $(a, b)$  that satisfy  $1 \leq a < b \leq m$ , we have

$$\sum_{i=1}^n G_{ai} G_{bi} = 0 \pmod{2} \quad (9)$$

2) for all triples  $(a, b, c)$  that satisfy  $1 \leq a < b < c \leq m$ , we have

$$\sum_{i=1}^n G_{ai} G_{bi} G_{ci} = 0 \pmod{2} \quad (10)$$

where  $G_{ij}$  indicates the  $j$ th element in  $i$ th row of  $\mathbf{G}$  [17]. A triorthogonal matrix  $\mathbf{G}$  can be written as:

$$\mathbf{G} = \begin{bmatrix} \mathbf{G}_1 \\ \mathbf{G}_0 \end{bmatrix} \quad (11)$$

where all rows in  $\mathbf{G}_1$  have odd weight, while rows in  $\mathbf{G}_0$  have even weight.

A triorthogonal  $[[n, k, d]]$  CSS code  $\mathcal{Q}^T = \text{CSS}(\mathcal{C}_1, \mathcal{C}_2)$  is generated by triorthogonal matrix  $\mathbf{G}$  of the form (11), such that  $\mathbf{G}$  and  $\mathbf{G}_0^\perp$  are the generators of  $\mathcal{C}_1$  and  $\mathcal{C}_2$ , respectively. The generator matrix of the triorthogonal CSS code thus is:

$$\mathbf{G}^{\mathcal{Q}^T} = \begin{bmatrix} \mathbf{G}_0 & \mathbf{0} \\ \mathbf{0} & \mathbf{G}^\perp \end{bmatrix}. \quad (12)$$

Transversal action of  $\mathbf{T}$  gates realize logical  $\mathbf{T}$ -gates in the triorthogonal codes if certain additional constraints on logical  $\mathbf{X}$  operators hold [7]. Triorthogonal codes that support transversal  $\mathbf{T}$ -gates are referred to as  $\mathbf{T}$ -transversal triorthogonal codes. In this paper, we use the term *T-triorthogonal codes* for these codes.

### III. TRANSVERSAL TOFFOLI-GATE

In this section, we construct a hybrid-code system that has a transversal logical Toffoli-gate. This *hybrid-code system* defined as follows: A system of  $k$  parallel logical Toffoli-gates are realized across three code blocks, each protecting  $k$  logical qubits. The gate acts in parallel on  $k$  triplets of qubits, with one qubit from each block in each triplet. The first and second block are encoded in T-triorthogonal code  $\mathcal{Q}^T$ . We denote mirrored code of  $\mathcal{Q}^T$  by  $\mathcal{Q}^{\text{T}^\times}$  and use it for the third code block. The concept of mirrored CSS code is defined in [11]. Below, we discuss this concept, and show that this system can achieve transversal Toffoli-gate.

#### A. Mirrored code $\mathcal{Q}^{\text{T}^\times}$

To start with, we focus on the mirrored code  $\mathcal{Q}^{\text{T}^\times}$ , emphasizing its features that can be used for providing Toffoli-gate transversality.

Consider T-triorthogonal code  $\mathcal{Q}^T = \text{CSS}(\mathcal{C}_1, \mathcal{C}_2)$  with generator matrix (12). The corresponding mirrored code  $\mathcal{Q}^{\text{T}^\times} = \text{CSS}(\mathcal{C}_2, \mathcal{C}_1)$  has the generator matrix:

$$\mathbf{G}^{\mathcal{Q}^{\text{T}^\times}} = \begin{bmatrix} \mathbf{G}_0^\perp & \mathbf{0} \\ \mathbf{0} & \mathbf{G}_1 \end{bmatrix}, \quad (13)$$

which can be considered as conjugating all the generators in  $\mathcal{Q}^T$  with Hadamard operations, exchanging the  $\mathbf{X}$  and  $\mathbf{Z}$  parts of the generators.

Defining the transformed gate  $\mathbf{T}_X = \mathbf{HTH}$ , we have:

**Lemma 1.** *If triorthogonal code  $\mathcal{Q}^T$  has  $\mathbf{T}$ -gate transversality, its mirrored code  $\mathcal{Q}^{\text{T}^\times}$  has  $\mathbf{T}_X$  gate transversality.*

*Proof.* For a T-triorthogonal code  $\mathcal{Q}^T = \text{CSS}(\mathcal{C}_1, \mathcal{C}_2)$ , it has  $\mathbf{T}$ -gate transversality, then we can write:

$$\mathbf{T}^{\otimes n} \frac{1}{\sqrt{|\mathcal{C}_2^\perp|}} \sum_{\mathbf{y} \in \mathcal{C}_2^\perp} |\boldsymbol{\psi}\mathbf{A} + \mathbf{y}\rangle = \mathbf{T}_L^{\otimes k} |\boldsymbol{\psi}\rangle_L, \quad (14)$$

where  $\boldsymbol{\psi} \in \mathbb{F}_2^k$  is arbitrary logical state, and  $\mathbf{A} \in \mathcal{C}_1/\mathcal{C}_2^\perp$  is a mapping matrix from logical state to physical state. Since  $\mathbf{T}|\boldsymbol{\psi}\rangle = e^{\frac{i\pi \text{wt}(\boldsymbol{\psi})}{4}} |\boldsymbol{\psi}\rangle$ , we can rewrite the equation as:

$$\beta \sum_{\mathbf{y} \in \mathcal{C}_2^\perp} e^{\frac{i\pi}{4} \text{wt}(\boldsymbol{\psi}\mathbf{A} + \mathbf{y})} |\boldsymbol{\psi}\mathbf{A} + \mathbf{y}\rangle = \beta e^{\frac{i\pi}{4} \text{wt}(\boldsymbol{\psi})} \sum_{\mathbf{y} \in \mathcal{C}_2^\perp} |\boldsymbol{\psi}\mathbf{A} + \mathbf{y}\rangle, \quad (15)$$

where  $\beta = \frac{1}{\sqrt{|\mathcal{C}_2^\perp|}}$ .

Now we consider the mirrored code  $\mathcal{Q}^{\text{T}^\times} = \text{CSS}(\mathcal{C}_2, \mathcal{C}_1)$  and apply  $n$  transversal physical  $\mathbf{T}_X = \mathbf{HTH}$  gates, we have:

$$\begin{aligned} & \mathbf{H}^{\otimes n} \mathbf{T}^{\otimes n} \mathbf{H}^{\otimes n} \frac{1}{\sqrt{|\mathcal{C}_1^\perp|}} \sum_{\mathbf{z} \in \mathcal{C}_1^\perp} |\boldsymbol{\psi}\mathbf{B} + \mathbf{z}\rangle \\ &= \mathbf{H}^{\otimes n} \mathbf{T}^{\otimes n} \frac{\sqrt{|\mathcal{C}_1^\perp|}}{\sqrt{2^n}} \sum_{\mathbf{x}_a \in \mathcal{C}_1} (-1)^{\boldsymbol{\psi}\mathbf{B}\mathbf{x}_a^T} |\mathbf{x}_a\rangle, \end{aligned}$$

where  $\mathbf{B} \cong \mathcal{C}_2/\mathcal{C}_1^\perp$ . Since  $\mathcal{C}_2^\perp \subset \mathcal{C}_1$ , we can rewrite  $\mathbf{x}_a = \boldsymbol{\psi}'\mathbf{A} + \mathbf{I}$ , where  $\boldsymbol{\psi}' \in \mathbb{F}_2^k$  and  $\mathbf{I} \in \mathcal{C}_2^\perp$ . Also combining with (15), the above equation can be rewritten as:

$$\begin{aligned} & \frac{\sqrt{|\mathcal{C}_1^\perp|}}{\sqrt{2^n}} \mathbf{H}^{\otimes n} \mathbf{T}^{\otimes n} \sum_{\mathbf{I} \in \mathcal{C}_2^\perp, \boldsymbol{\psi}' \in \mathbb{F}_2^k} (-1)^{\boldsymbol{\psi}\mathbf{B}(\boldsymbol{\psi}'\mathbf{A} + \mathbf{I})^T} |\boldsymbol{\psi}'\mathbf{A} + \mathbf{I}\rangle \\ &= \frac{\sqrt{|\mathcal{C}_1^\perp|}}{\sqrt{2^n}} \mathbf{H}^{\otimes n} \sum_{\mathbf{I} \in \mathcal{C}_2^\perp, \boldsymbol{\psi}' \in \mathbb{F}_2^k} (-1)^{\boldsymbol{\psi}\mathbf{B}(\boldsymbol{\psi}'\mathbf{A})^T} e^{\frac{i\pi}{4} \text{wt}(\boldsymbol{\psi}')} |\boldsymbol{\psi}'\mathbf{A} + \mathbf{I}\rangle \\ &= \alpha \sum_{\boldsymbol{\psi}' \in \mathbb{F}_2^k} (-1)^{\boldsymbol{\psi}\mathbf{B}(\boldsymbol{\psi}'\mathbf{A})^T} e^{\frac{i\pi}{4} \text{wt}(\boldsymbol{\psi}')} \sum_{\mathbf{x}_b \in \mathcal{C}_2} (-1)^{\boldsymbol{\psi}'\mathbf{A}\mathbf{x}_b^T} |\mathbf{x}_b\rangle, \end{aligned}$$

where  $\alpha = \frac{\sqrt{|\mathcal{C}_1^\perp|}|\mathcal{C}_2^\perp|}{2^n} = \frac{\sqrt{|\mathcal{C}_1^\perp|}}{2^k \sqrt{|\mathcal{C}_1^\perp|}}$ . With a similar approach, we can rewrite  $\mathbf{x}_b = \boldsymbol{\psi}''\mathbf{B} + \mathbf{j}$ . Then outcome state of transversal  $\mathbf{T}_X$  gates is:

$$\begin{aligned} & \alpha \sum_{\boldsymbol{\psi}' \in \mathbb{F}_2^k} (-1)^{\boldsymbol{\psi}\mathbf{B}(\boldsymbol{\psi}'\mathbf{A})^T} e^{\frac{i\pi}{4} \text{wt}(\boldsymbol{\psi}')} \\ & \sum_{\boldsymbol{\psi}'' \in \mathbb{F}_2^k, \mathbf{j} \in \mathcal{C}_1^\perp} (-1)^{\boldsymbol{\psi}'\mathbf{A}(\boldsymbol{\psi}''\mathbf{B})^T} |\boldsymbol{\psi}''\mathbf{B} + \mathbf{j}\rangle. \quad (16) \end{aligned}$$

For the  $k$  parallel logical  $\mathbf{T}_{XL}$  operators acting on logical state  $|\boldsymbol{\psi}\rangle_L$ , we have:

$$\begin{aligned} & \mathbf{H}_L^{\otimes k} \mathbf{T}_L^{\otimes k} \mathbf{H}_L^{\otimes k} |\boldsymbol{\psi}\rangle_L = \frac{1}{\sqrt{2^k}} \mathbf{H}_L^{\otimes k} \mathbf{T}_L^{\otimes k} \sum_{\boldsymbol{\psi}_b \in \mathbb{F}_2^k} (-1)^{\boldsymbol{\psi}\boldsymbol{\psi}_b^T} |\boldsymbol{\psi}_b\rangle_L \\ &= \frac{1}{\sqrt{2^k}} \mathbf{H}_L^{\otimes k} \sum_{\boldsymbol{\psi}_b \in \mathbb{F}_2^k} (-1)^{\boldsymbol{\psi}\boldsymbol{\psi}_b^T} e^{\frac{i\pi}{4} \text{wt}(\boldsymbol{\psi}_b)} |\boldsymbol{\psi}_b\rangle_L \\ &= \frac{1}{2^k} \sum_{\boldsymbol{\psi}_b \in \mathbb{F}_2^k} (-1)^{\boldsymbol{\psi}\boldsymbol{\psi}_b^T} e^{\frac{i\pi}{4} \text{wt}(\boldsymbol{\psi}_b)} \sum_{\boldsymbol{\psi}_c \in \mathbb{F}_2^k} (-1)^{\boldsymbol{\psi}_b\boldsymbol{\psi}_c^T} |\boldsymbol{\psi}_c\rangle_L \\ &= \alpha \sum_{\boldsymbol{\psi}_b \in \mathbb{F}_2^k} (-1)^{\boldsymbol{\psi}\boldsymbol{\psi}_b^T} e^{\frac{i\pi}{4} \text{wt}(\boldsymbol{\psi}_b)} \sum_{\substack{\boldsymbol{\psi}_c \in \mathbb{F}_2^k \\ \mathbf{j} \in \mathcal{C}_1^\perp}} (-1)^{\boldsymbol{\psi}_b\boldsymbol{\psi}_c^T} |\boldsymbol{\psi}_c\mathbf{B} + \mathbf{j}\rangle. \quad (17) \end{aligned}$$

We can notice that when  $\mathbf{A}\mathbf{B}^T = \mathbf{I}$ , we have (16) equals to (17), implying that the  $n$  transversal physical  $\mathbf{T}_X$  gates are

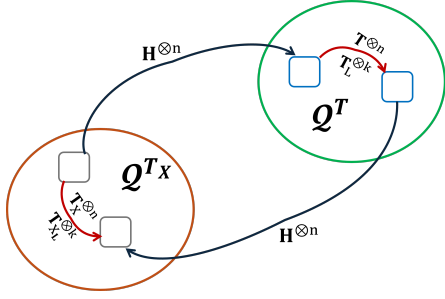


Fig. 1. Applying transversal  $\mathbf{T}_X = \mathbf{HTH}$  gates on mirrored code  $Q^{T_x}$  results in transversal logical  $\mathbf{T}_X$  gates. While transversal Hadamard gates do not preserve the code space, they instead map the logical state between the code space of the mirrored code  $Q^{T_x}$  and its original code  $Q^T$ . The red curves indicate that the corresponding transversal operators act as logical operators within each respective code space.

equivalent to  $k$  logical  $\mathbf{T}_X$  gates. In paper [11], we showed that for any CSS codes, one can always construct mapping matrices  $\mathbf{A}$  and  $\mathbf{B}$  that satisfy this condition. We therefore conclude that mirrored T-triorthogonal codes admit transversal  $\mathbf{T}_X$  gate.  $\square$

It is worth noting that, in our computation, the transversal  $\mathbf{T}_X$  gates are implemented via the decomposition  $\mathbf{HTH}$ . While the  $\mathbf{T}_X$  gate is transversal, neither the Hadamard nor the  $\mathbf{T}$  gates are transversal in  $Q^{T_x}$ . Consequently, the logical information encoded in the mirrored code transitions between the mirrored code space and the original  $Q^T$  code space during the computation, as illustrated in Fig. 1.

### B. CZ and CNOT Transversality Between $Q^T$ and $Q^{T_x}$

As a consequence of the concept of transversal gates between different codes [11], we can show that there exists CZ and one-direction CNOT gate transversality between the codes  $Q^T$  and  $Q^{T_x}$ .

From [11], it follows that for a pair of codes with mirrored structure, they satisfy the CZ transversal conditions (7). Thus,  $Q^T$  and its mirrored code  $Q^{T_x}$  fulfill this condition, they have CZ transversality.

**Lemma 2.** *If  $Q^T$  is triorthogonal code and  $Q^{T_x}$  is its mirrored code, the CNOT gate, controlled by  $Q^T$  and  $Q^{T_x}$  as target, is transversal.*

*Proof.* Consider the transversal CNOT gate conditions (6) for the codes  $Q^T = \text{CSS}(\mathcal{C}_1, \mathcal{C}_2)$  and  $Q^{T_x} = \text{CSS}(\mathcal{C}_2, \mathcal{C}_1)$ . Since  $Q^T$  a triorthogonal code with generator (12), the classical codes  $\mathcal{C}_1$  and  $\mathcal{C}_2$  are generated by  $\mathbf{G}$  and  $\mathbf{G}_0^\perp$ , respectively. As  $\mathbf{G}$  can be written as (11), and  $\mathbf{G}_0$  is the generator of  $\mathcal{C}_2^\perp$ . Thus, we have  $\mathcal{C}_1/\mathcal{C}_2^\perp \cong \mathbf{G}_1$ .

A similar analysis applies to the coset  $\mathcal{C}_2/\mathcal{C}_1^\perp$ , which corresponds to codewords in  $\mathbf{G}_0^\perp$  that are not in  $\mathbf{G}^\perp$ . By the triorthogonality condition in (9),  $\mathbf{G}_0$  is a self-orthogonal matrix, and that each row of  $\mathbf{G}_1$  is in  $\mathbf{G}_0^\perp$ , and  $\mathbf{G}_1$  is orthogonal to  $\mathbf{G}_0$ . All  $2^k$  codewords generated by  $\mathbf{G}_1$  are in the coset space  $\mathcal{C}_2/\mathcal{C}_1^\perp$ . Note that the size of the space generated by  $\mathbf{G}_0^\perp$  and  $\mathbf{G}^\perp$  are  $2^{n-\text{rank}(\mathbf{G}_0)}$  and  $2^{n-\text{rank}(\mathbf{G}_0)-\text{rank}(\mathbf{G}_1)}$ , respectively. In addition, the coset  $\mathcal{C}_2/\mathcal{C}_1^\perp$  has size  $2^{\text{rank}(\mathbf{G}_1)}$ . This shows

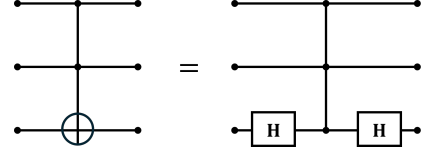


Fig. 2. A Toffoli-gate is equivalent to a CCZ gate with target qubit conjugated by Hadamard gates.

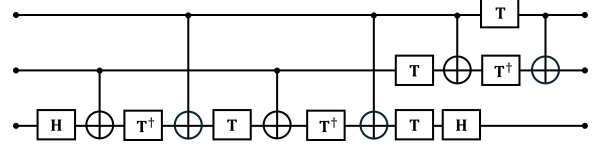


Fig. 3. Decomposition of a Toffoli-gate into 6 CNOT gates, 2 Hadamard gates and 7  $\mathbf{T}$  (or  $\mathbf{T}^\dagger$ ) gates.

that it is exactly the space generated by  $\mathbf{G}_1$ . Thus, we can conclude:

$$\mathcal{C}_2^\perp \subseteq \mathcal{C}_1^\perp \text{ and } \mathcal{C}_1/\mathcal{C}_2^\perp \cong \mathcal{C}_2/\mathcal{C}_1^\perp = \mathbf{G}_1.$$

This mirrored design thus fulfills the CNOT-transversality conditions (6), with  $Q^T$  as control and  $Q^{T_x}$  as target.  $\square$

Note that, this lemma holds due to the triorthogonality conditions and therefore applies to all triorthogonal codes, regardless of whether they are T-transversal.

### C. Toffoli-gate decomposition

A logical Toffoli-gate can be realized by using a logical CCZ gate and conjugating the target qubit with logical Hadamard gates, as depicted in Fig. 2. The CCZ gate itself can be decomposed into a sequence of  $\mathbf{T}$ -gates and CNOT gates, leading to a full decomposition of the logical Toffoli-gate into  $\mathbf{T}$ -gates and logical Clifford gates, shown in Fig. 3 [15]. If T-triorthogonal codes are used, only the CNOT and  $\mathbf{T}$ -gates can be implemented transversally. The logical Hadamard gates cannot be realized in a transversal manner.

By commuting the first Hadamard gate in Fig. 3 across all gates acting on the third qubit, each  $\mathbf{T}$  gate is transformed into a  $\mathbf{T}_X$  gate, and CNOT gates are converted into CZ gates. This Hadamard gate then cancels with the last one, yielding a new Toffoli gate decomposition shown in Fig. 4. Based on this circuit, we can implement the logical Toffoli gate by encoding the first and second qubits in  $Q^T$ , and the third qubit in  $Q^{T_x}$ . With this encoding, all logical gates in the circuit can be implemented transversally. Therefore, we have:

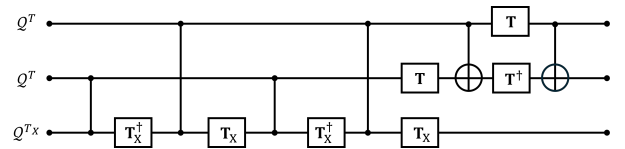


Fig. 4. Modified Toffoli-gate decomposition circuit. The first and second qubits encoded in  $Q^T$  and the last one encoded in  $Q^{T_x}$ .

**Theorem 1.** *A hybrid-code system with the first and second qubit encoded in  $\mathcal{Q}^T$  and third qubit encoded in  $\mathcal{Q}^{T^x}$  has Toffoli-gate transversality with the first and second qubit as control qubits and third as target qubit.*

*Proof.* Since  $\mathcal{Q}^T$  is a T-triorthogonal CSS code, the first and second qubits, encoded in  $\mathcal{Q}^T$ , have T-gate and CNOT gate transversalities. From Lemma 1, the third qubit, encoded in  $\mathcal{Q}^{T^x}$ , supports transversal  $\mathbf{T}_X$ . From [11, Example.2], it follows that CZ gates are transversal between qubits 1 or 2 and 3. In the Toffoli-gate decomposition circuit shown in Fig. 4, every operation can thus be applied transversally across three code blocks. Since each component of the circuit support the transversal conditions, from (8) it follows that the logical Toffoli-gate can be directly implemented in a transversal manner in this system.  $\square$

With such a hybrid-code system, two approaches can be used to achieve universal quantum computation. The first approach uses the T-triorthogonal code with its mirrored code. In this case, the system implements non-Clifford gate transversality, and universality can be achieved by applying the logical Hadamard gate through an ancilla block [18]. The second approach exploits the Toffoli gate transversality to perform Toffoli state distillation. Similar to magic state distillation, the distilled Toffoli states serve as ancilla states for implementing logical Toffoli gates in other code systems with transversal Clifford gate sets, such as surface codes or color codes. We will explain this distillation protocol in the following section.

#### IV. TOFFOLI-STATE DISTILLATION

As an example application for the proposed hybrid-code system with Toffoli gate transversality, we consider a Toffoli state distillation protocol. The Toffoli state  $|\psi_{\text{Tof}}\rangle$  is a three qubit magic state defined by the output of the Toffoli-gate acting on the initial state:

$$|\psi_{\text{Tof}}\rangle = \mathbf{CCX}|+\rangle|+\rangle|0\rangle, \quad (18)$$

where  $\mathbf{CCX}$  indicates Toffoli gate and with the third qubit,  $|0\rangle$ , as the target. It can be used to implement the action of a Toffoli-gate with a circuit shown as Fig. 5, as an assistant state. The lower three qubits in arbitrary state  $|a\rangle|b\rangle|c\rangle$  are the input state. With following three CNOT gates between Toffoli state and input state, the input state are measured in Pauli  $\mathbf{X}$  and  $\mathbf{Z}$  basis. According to the measurement outcome, the feedback operations, connected by solid lines, are applied. For example, if the measurement on  $|c\rangle$  is  $-1$ , then a Pauli  $\mathbf{Z}$  and CZ operators are applied simultaneously. The outcome of left circuit is  $|a\rangle|b\rangle|a \cdot b \oplus c\rangle$ , which is the same as the outcome of  $|a\rangle|b\rangle|c\rangle$  go through Toffoli-gate [12].

Our Toffoli state distillation protocol is based on the hybrid-code system, which takes low-fidelity Toffoli states as input and outputs distilled, high-fidelity physical Toffoli states. These high-fidelity states can then be fault-tolerantly encoded into any code used within the computational system. In cases where direct fault-tolerant encoding is not available, a concatenated

architecture can be employed, combining the computational code with the hybrid-code system. There are several ways to fault-tolerantly distill Toffoli-states [12]–[14]. These protocols use distilled magic states to implement logical T-gates, and through specific logical circuits, high-fidelity Toffoli states can be obtained. Our distillation method exploits Toffoli-gate transversality discussed above, and directly distill the Toffoli state for achieving high-fidelity state.

Our Toffoli-state distillation protocol is summarized in Algorithm 1. In Phase 1, we directly apply physical Toffoli gates and use error correction to improve the fidelity. After this phase, if the fidelity of the distilled Toffoli states meets the target threshold  $f_T$ , the protocol terminates. Otherwise, we proceed to iterative distillation, where the circuit shown in Fig. 5 is applied using the Toffoli states produced in the previous round. This iterative process continues until the fidelity reaches the required value  $f_T$ .

---

#### Algorithm 1 Toffoli state distillation protocol

---

**TARGET** Toffoli state with fidelity higher than  $f_T$ .

---

##### Phase 1 – Level-1 Distillation

---

**Input:** Logical qubits initialized in  $|+\rangle_L|+\rangle_L|0\rangle_L$  in  $\mathcal{Q}^T$ ,  $\mathcal{Q}^T$ , and  $\mathcal{Q}^{T^x}$ , respectively.  $\mathcal{Q}^T$  and  $\mathcal{Q}^{T^x}$  are  $[[n, k]]$  codes.

- 1: Implement  $n$  transversal physical Toffoli gates. Controlled by qubits in  $\mathcal{Q}^T$  and target qubit in  $\mathcal{Q}^{T^x}$ .
  - 2: Error correction: compute error syndrome vector  $\mathbf{s}$ .
  - 3: **if**  $\mathbf{s} \neq \mathbf{0}$  **then**
  - 4:     Discard states and start from the beginning.
  - 5: **end if**
  - 6: Decoding, outcome  $k$  physical  $|\psi_{\text{Tof}}\rangle_1$  states.
  - 7: The outcome fidelity  $f = {}_1\langle\psi_{\text{Tof}}|\psi_{\text{Tof}}\rangle_1$ .
- 

##### Phase 2 – Level- $m$ distillation, $m \geq 2$

---

**Input:** Three logical blocks in  $|+\rangle_L|+\rangle_L|0\rangle_L$  in  $\mathcal{Q}^T$ ,  $\mathcal{Q}^T$ , and  $\mathcal{Q}^{T^x}$ .  $n$  physical  $|\psi_{\text{Tof}}\rangle_{m-1}$  states.

- 8: **if**  $f < f_T$  **then**
- 9:     Transversal  $\mathbf{CCX}$  using  $n$  physical  $|\psi_{\text{Tof}}\rangle_{m-1}$  states.
- 10:     Error correction: compute error syndrome vector  $\mathbf{s}$ .
- 11:     **if**  $\mathbf{s} \neq \mathbf{0}$  **then**
- 12:         Discard states and restart from line 8.
- 13:     **end if**
- 14:     Decoding, outcome  $k$  physical  $|\psi_{\text{Tof}}\rangle_m$  states.
- 15:     The outcome fidelity  $f = {}_m\langle\psi_{\text{Tof}}|\psi_{\text{Tof}}\rangle_m$ .
- 16: **end if**

**Output:**  $k$  physical  $|\psi_{\text{Tof}}\rangle_m$  with required fidelity.

---

Notice, after repeated use of distilled Toffoli-states, we can achieve Toffoli-gates with arbitrarily high fidelity, as long as the physical error rate of initial physical Toffoli-gates is lower than a threshold.

Our Toffoli state distillation protocol can produce a high-fidelity Toffoli state without the need to generate seven magic states that are used to realize the circuit of Fig. 3. This not only reduces the overall resource overhead but also minimizes the number of encoding procedures, as each distilled physical

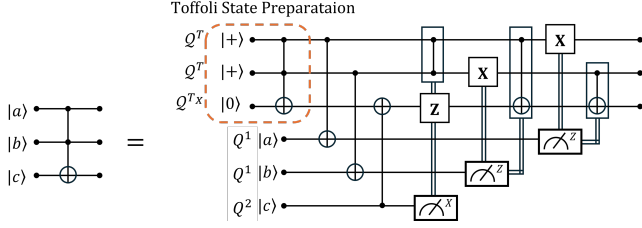


Fig. 5. Circuit for both Toffoli state distillation and Toffoli gate implementation. When the Toffoli state is used to perform a Toffoli gate,  $Q^1$  and  $Q^2$  correspond to the same code employed in the computational system, such as the surface code. In the Toffoli-state distillation process, the  $Q^1$  and  $Q^2$  are chosen as  $Q^T$  and  $Q^{T_x}$  respectively. The orange dashed box outputs an ancillary Toffoli-state. Using CNOTs and measurements, the Toffoli-gate action is teleported to the 3-qubit state  $|a\rangle|b\rangle|c\rangle$ .

magic state would need to be re-encoded into a different code system.

## V. NUMERICAL SIMULATION

As an example, consider using the  $[[15, 1, 3]]$  T-triorthogonal code and its mirrored code for Toffoli-state distillation. For performance evaluation, since the physical Toffoli gates are much erroneous than single and two-qubit gates [19], we assume noise on the physical Toffoli-gates as the only error source. For each code block, the main contribution to non-trivial syndromes are weight-1 and weight-2 errors. For simplicity we assume that after apply physical Toffoli gate, all qubits have the same error probability  $p$  to occur a  $Z$  error, the successful rate  $p_s$  to conduct distillation can be written as:

$$p_s = 1 - 15p - 105p^2 + O(p^3).$$

When we get trivial syndrome, the outcome state in each code block has error rate  $35p^3 + O(p^4)$ , which the factor 35 comes from the number of non-detectable weight-3 errors in  $[[15, 1, 3]]$  code. This performance is the same as using  $[[15, 1, 3]]$  code for magic state distillation, thus the threshold for  $p$  is 14.1%, the same as 15-to-1 distillation protocol [4]. Since Toffoli gate is a three qubit gate, and for each qubit it has error threshold  $p_\epsilon = 14.1\%$ , the threshold for Toffoli error rate should be  $p_{th} \approx 3p_\epsilon(1 - p_\epsilon)^2 = 31.8\%$ .

An alternative approach is using another set of T-triorthogonal codes with parameter  $[[3k + 8, k, 2]]$  [16]. By using this code, one can achieve successful error rate as:  $p_s = 1 - (3k + 8)p + O(p^2)$  and output error rate on any one qubit is  $(1 + 3k)p^2$ .

We can also estimate the qubit resource cost required to achieve a given level of distilled error rate. In Fig. 6, we compare the qubit overhead required to achieve a target-fidelity Toffoli gate between our direct Toffoli-state distillation protocol and conventional approaches that use magic states to construct Toffoli states. The physical Toffoli gate or magic state error rate is selected as  $10^{-2}$ , and for  $[[3k + 8, k, 2]]$  code we choose the optimized  $k$  for each target error rate. In our protocol, we directly distill a three-qubit Toffoli state, whereas other approaches use either seven magic states with

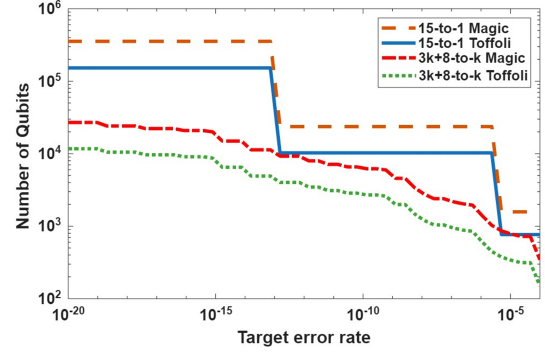


Fig. 6. Comparison of qubit resource costs for different Toffoli state distillation protocols. The 15-to-1 and  $3k + 8$ -to- $k$  Toffoli curves corresponding to our direct Toffoli state distillation protocols using the  $[[15, 1, 3]]$  and  $[[3k+8, k, 2]]$  codes, respectively. The corresponding 'Magic' curves represent the protocols that first distill seven magic states using the same codes to construct a Toffoli state. With the initial physical error rate selected as  $10^{-2}$ , our direct Toffoli-state distillation approach achieves the same target error rate with approximately 50% fewer qubits.

a 15-to-1 protocol or the more general  $3k + 8$ -to- $k$  distillation protocol. Because we directly distill the Toffoli state, our method requires only about half as many qubits. Specifically, the average qubit cost for achieving an  $m$ -level distilled Toffoli state via the 15-to-1 protocol is

$$\frac{3 \times 15^m + 45(m - 1)}{p_{suc}},$$

where  $p_{suc}$  is the overall successful probability. In contrast, using magic state distillation requires  $7 \times 15^m / p_{suc}$ , which the cost is around  $\times 2$  larger than our protocol. We can see the same reduce overhead in  $[[3k + 8, k, 2]]$  distillation protocol. Compare with  $[[15, 1, 3]]$  code,  $[[3k + 8, k, 2]]$  with optimized  $k$  uses less qubit to achieve target error rate.

The optimized value of  $k$  in the  $[[3k + 8, k, 2]]$  code can be carefully selected to achieve the best performance for a given target error rate. We numerical calculate the qubit number cost for  $k = 1$  to 50 with initial physical error rate selected as  $10^{-2}$ , and the results for  $k = 2$  to  $k = 13$  are shown in Fig. 7. Other values of  $k$  lead to substantially higher overhead within the considered target error-rate range, and therefore omitted. The logical qubit number  $k$  at each distillation layer can thus be optimized to minimize the overall qubit overhead.

In addition to reducing the overall resource overhead, our protocol avoids the repeated encoding steps required in other methods. Since conventional approaches rely on T-gate-based magic states to construct the Toffoli state, the distilled magic states must be encoded into the computational system for seven times. These encoding procedure may increase the total cost and the logical error rate. In contrast, our protocol requires only a single encoding step at the end of distillation procedure, making it potentially more robust against CNOT gate errors. A more detailed investigation of this aspect is left for future work.

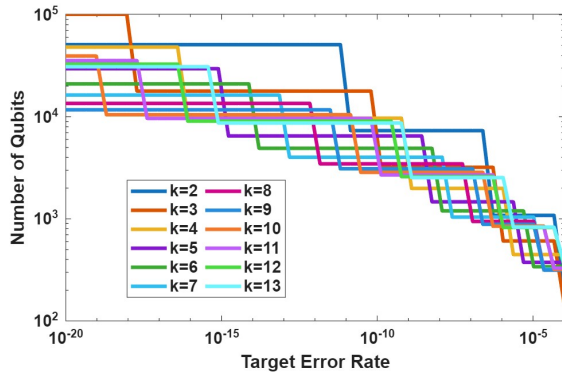


Fig. 7. Different values of  $k$  in the  $[[3k + 8, k, 2]]$  code. The optimal  $k$  is chosen as the value that minimizes the number of qubits required to achieve the target error rate.

## VI. CONCLUSION

In this paper, we investigated the transversality of the Toffoli gate within a hybrid-code framework. Through circuit-level analysis, we demonstrated that by employing a triorthogonal code and its paired mirrored code in a specific configuration, the Toffoli gate can be implemented transversally. Furthermore, based on this hybrid-code architecture, we proposed a Toffoli gate distillation protocol that does not require pre-distilled T gates. The numerical results indicate that the proposed method achieves a 50% reduction in the required qubit resources compared to existing approaches in the literature. This design serves as a concrete example of achieving a transversal Toffoli gate. In future work, we aim to establish necessary and/or sufficient conditions for transversality when employing three distinct quantum error correction codes.

## ACKNOWLEDGEMENTS

This work was funded in part by Nokia Industrial Doctoral School in Quantum Technology and Business Finland (grant 8264/31/2022).

## REFERENCES

[1] D. Gottesman, "Theory of fault-tolerant quantum computation," *Physical Review A*, vol. 57, no. 1, p. 127–137, Jan. 1998. [Online]. Available: <http://dx.doi.org/10.1103/PhysRevA.57.127>

[2] B. Eastin and E. Knill, "Restrictions on transversal encoded quantum gate sets," *Physical review letters*, vol. 102, no. 11, p. 110502, 2009.

[3] J. T. Anderson, G. Duclos-Cianci, and D. Poulin, "Fault-tolerant conversion between the steane and Reed-Muller quantum codes," *Physical review letters*, vol. 113, no. 8, p. 080501, 2014.

[4] S. Bravyi and A. Kitaev, "Universal quantum computation with ideal Clifford gates and noisy ancillas," *Physical Review A—Atomic, Molecular, and Optical Physics*, vol. 71, no. 2, p. 022316, 2005.

[5] D. Horsman, A. G. Fowler, S. Devitt, and R. Van Meter, "Surface code quantum computing by lattice surgery," *New Journal of Physics*, vol. 14, no. 12, p. 123011, 2012.

[6] T. J. Yoder, "Universal fault-tolerant quantum computation with Bacon-Shor codes," *arXiv preprint arXiv:1705.01686*, 2017.

[7] N. Rengaswamy, R. Calderbank, M. Newman, and H. D. Pfister, "On optimality of CSS codes for transversal T," *IEEE Journal on Selected Areas in Information Theory*, vol. 1, no. 2, pp. 499–514, 2020.

[8] M. Newman and Y. Shi, "Limitations on transversal computation through quantum homomorphic encryption," *arXiv preprint arXiv:1704.07798*, 2017.

[9] T. Toffoli, "Reversible computing," in *International colloquium on automata, languages, and programming*. Springer, 1980, pp. 632–644.

[10] L. M. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang, "Experimental realization of shor's quantum factoring algorithm using nuclear magnetic resonance," *Nature*, vol. 414, no. 6866, pp. 883–887, 2001.

[11] M. Bayanifar, A. Ashikhmin, D. Jiao, and O. Tirkkonen, "Transversality across two distinct quantum codes and its application to quantum repeaters," in *IEEE Internat. Conf. on Quantum Commun., Networking, and Computing (QCNC)*, 2025, pp. 17–23.

[12] B. Eastin, "Distilling one-qubit magic states into Toffoli states," *Physical Review A—Atomic, Molecular, and Optical Physics*, vol. 87, no. 3, p. 032321, 2013.

[13] C. Jones, "Low-overhead constructions for the fault-tolerant Toffoli gate," *Physical Review A—Atomic, Molecular, and Optical Physics*, vol. 87, no. 2, p. 022328, 2013.

[14] J. Haah and M. B. Hastings, "Codes and protocols for distilling  $T$ , controlled- $S$ , and Toffoli gates," *Quantum*, vol. 2, p. 71, 2018.

[15] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*. Cambridge university press, 2010.

[16] S. Bravyi and J. Haah, "Magic-state distillation with low overhead," *Physical Review A*, vol. 86, no. 5, Nov. 2012. [Online]. Available: <http://dx.doi.org/10.1103/PhysRevA.86.052329>

[17] M. Shi, H. Lu, J.-L. Kim, and P. Solé, "Triorthogonal codes and self-dual codes," *Quantum Information Processing*, vol. 23, no. 7, p. 280, 2024.

[18] A. Paetznick and B. W. Reichardt, "Universal fault-tolerant quantum computation with only transversal gates and error correction," *Physical review letters*, vol. 111, no. 9, p. 090505, 2013.

[19] Y. Kim, A. Morvan, L. B. Nguyen, R. K. Naik, C. Jünger, L. Chen, J. M. Kreikebaum, D. I. Santiago, and I. Siddiqi, "High-fidelity three-qubit toffoli gate for fixed-frequency superconducting qubits," *Nature Physics*, vol. 18, no. 7, p. 783–788, May 2022. [Online]. Available: <http://dx.doi.org/10.1038/s41567-022-01590-3>