

# Symmetries of Codeword Stabilized Quantum Codes\*

Salman Beigi<sup>1</sup>, Jianxin Chen<sup>2,3</sup>, Markus Grassl<sup>4</sup>, Zhengfeng Ji<sup>3</sup>,  
Qiang Wang<sup>5</sup>, and Bei Zeng<sup>2,3</sup>

- 1 School of Mathematics, Institute for Research in Fundamental Sciences (IPM)  
Niavaran Square, Tehran, Iran  
salman.beigi@gmail.com
- 2 Department of Mathematics & Statistics, University of Guelph  
50 Stone Road East, Guelph, Ontario, Canada  
{chenkenshin,zengbei}@gmail.com
- 3 Institute for Quantum Computing  
200 University Avenue West, Waterloo, Ontario, Canada  
jizhengfeng@gmail.com
- 4 Centre for Quantum Technologies, National University of Singapore  
3 Science Drive 2, Singapore 117543  
Markus.Grassl@nus.edu.sg
- 5 School of Mathematics and Statistics, Carleton University  
1125 Colonel By Drive, Ottawa, Ontario, Canada  
wang@math.carleton.ca

---

## Abstract

Symmetry is at the heart of coding theory. Codes with symmetry, especially cyclic codes, play an essential role in both theory and practical applications of classical error-correcting codes. Here we examine symmetry properties for codeword stabilized (CWS) quantum codes, which is the most general framework for constructing quantum error-correcting codes known to date. A CWS code  $\mathcal{Q}$  can be represented by a self-dual additive code  $\mathcal{S}$  and a classical code  $\mathcal{C}$ , i. e.,  $\mathcal{Q} = (\mathcal{S}, \mathcal{C})$ , however this representation is in general not unique. We show that for any CWS code  $\mathcal{Q}$  with certain permutation symmetry, one can always find a self-dual additive code  $\mathcal{S}$  with the same permutation symmetry as  $\mathcal{Q}$  such that  $\mathcal{Q} = (\mathcal{S}, \mathcal{C})$ . As many good CWS codes have been found by starting from a chosen  $\mathcal{S}$ , this ensures that when trying to find CWS codes with certain permutation symmetry, the choice of  $\mathcal{S}$  with the same symmetry will suffice. A key step for this result is a new canonical representation for CWS codes, which is given in terms of a unique decomposition as union stabilizer codes. For CWS codes, so far mainly the standard form  $(\mathcal{G}, \mathcal{C})$  has been considered, where  $\mathcal{G}$  is a graph state. We analyze the symmetry of the corresponding graph of  $\mathcal{G}$ , which in general cannot possess the same permutation symmetry as  $\mathcal{Q}$ . We show that it is indeed the case for the toric code on a square lattice with translational symmetry, even if its encoding graph can be chosen to be translational invariant.

**1998 ACM Subject Classification** E.4 Coding and Information Theory

**Keywords and phrases** CWS Codes, Union Stabilizer Codes, Permutation Symmetry, Toric Code

**Digital Object Identifier** 10.4230/LIPIcs.TQC.2013.192


---

\* This work was partially supported by NSERC, CIFAR, and IARPA.

 © Salman Beigi, Jianxin Chen, Markus Grassl, Zhengfeng Ji, Qiang Wang, and Bei Zeng;  
licensed under Creative Commons License CC-BY

8th Conference on Theory of Quantum Computation, Communication and Cryptography.

Editors: Simone Severini and Fernando Brandao; pp. 192–206

 Leibniz International Proceedings in Informatics

LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany



## 1 Introduction

Coding theory is an important component of information theory having a long history dating back to Shannon's seminal 1948 paper that laid the ground for information theory [21]. Coding theory is at the heart of reliable communication, where codes with symmetry, especially cyclic codes, such as the Reed-Solomon codes, are among the most widely used codes in practice [19].

In recent years, it has become evident that quantum communication and computation offer the possibility of secure and high rate information transmission, fast computational solution of certain important problems, and efficient physical simulation of quantum phenomena. However, quantum information processing depends on the identification of suitable quantum error-correcting codes (QECC) to make such processes and machines robust against faults due to decoherence, ubiquitous in quantum systems. Quantum coding theory has hence been extensively developed during the past 15 years [3, 9, 20].

Codeword stabilized (CWS) quantum codes are by far the most general construction of QECC [6]. A CWS code  $\mathcal{Q}$  can be represented by a stabilizer state (i.e. a self-dual additive code)  $\mathcal{S}$  and a classical code  $\mathcal{C}$ , i.e.  $\mathcal{Q} = (\mathcal{S}, \mathcal{C})$ . When  $\mathcal{C}$  is a linear code, the corresponding CWS code  $\mathcal{Q}$  is actually a stabilizer code. Also, any CWS code is local Clifford equivalent to a standard form  $(\mathcal{G}, \mathcal{C})$ , where  $\mathcal{G}$  is a graph state [6].

The CWS construction encompasses stabilizer (additive) codes and all the known non-additive codes with good parameters. It also leads to many new codes with good parameters, or good algebraic/combinatorial properties, through both analytical and numerical methods. Alternative perspectives of CWS codes have also been analyzed, including the union stabilizer codes (USt) method [11, 12], and the codes based on graphs [18, 23]. Concatenated codes and their generalizations using CWS codes have been developed [1], and decoding methods for CWS codes have been studied as well [17].

Given all the evidence that the CWS framework is a powerful method to construct and analyze QECC, it remains unclear to what extent the stabilizer state  $\mathcal{S}$  and the classical code  $\mathcal{C}$  can represent the symmetry of the CWS code  $\mathcal{Q} = (\mathcal{S}, \mathcal{C})$  in general. Given the vital importance that the code symmetry plays in coding theory, this understanding becomes crucial since if such a correspondence exists, it can provide practical methods for constructing CWS codes with desired symmetry from  $\mathcal{S}$  and/or  $\mathcal{C}$  with corresponding symmetry.

Unfortunately, there is no immediate clue what answer one can hope for. First of all, the representation  $\mathcal{Q} = (\mathcal{S}, \mathcal{C})$  is not unique. So for a given CWS code  $\mathcal{Q}$ , there might be some stabilizer states  $\mathcal{S}$  and/or classical codes  $\mathcal{C}$  which are more symmetric than others. Perhaps the best known example is the CWS representation for the five-qubit code  $\mathcal{Q}_5$ , where in the ideal case  $\mathcal{S}$  can be chosen as a graph state corresponding to the pentagon graph, and the classical code  $\mathcal{C}$  is chosen as the repetition code  $\{00000, 11111\}$ . In this case, both  $\mathcal{S}$  and  $\mathcal{C}$  nicely represent the cyclic symmetry of the five-qubit code.

However, there are known 'bad cases', too. One example is the seven-qubit Steane code  $\mathcal{Q}_7$ , where although the code itself is cyclic, one cannot find any  $\mathcal{S}$  corresponding to a cyclic graph, even if local Clifford operations are allowed [10]. Nonetheless, we know that the stabilizer group for this code  $\mathcal{Q}_7$  is invariant under cyclic shifts, and the logical  $Z$  operator can be chosen as  $Z_L = Z^{\otimes 7}$ , therefore the logical  $|0\rangle_L$  can be chosen as a cyclic stabilizer code. This is to say, there exists a representation for  $\mathcal{Q}_7 = (\mathcal{S}, \mathcal{C})$  such that  $\mathcal{S}$  is cyclic. In general it remains unclear under which conditions a representation for cyclic CWS code with a cyclic stabilizer state  $\mathcal{S}$  exists.

In this work, we address the symmetry properties of CWS codes. We are interested in

the permutation symmetry of CWS codes, which includes the important category of cyclic codes. Our main question is, to which extent can the representation  $(\mathcal{S}, \mathcal{C})$  and the standard form  $(\mathcal{G}, \mathcal{C})$  reflect the symmetry of the corresponding CWS code  $\mathcal{Q}$ . We show that for any CWS code  $\mathcal{Q}$  with permutation symmetry, one can always find a stabilizer state  $\mathcal{S}$  with the same permutation symmetry as  $\mathcal{Q}$  such that  $\mathcal{Q} = (\mathcal{S}, \mathcal{C})$ . As many good CWS codes are found by starting from a chosen  $\mathcal{S}$ , this ensures that when trying to find CWS codes with certain permutation symmetry, the choice of  $\mathcal{S}$  with the same symmetry will suffice. A key step to reach this main result is to obtain a canonical representation for CWS codes, which is in terms of a unique decomposition as union stabilizer codes.

We know that for the standard form of CWS codes using graph states, it is not always possible to find a graph with the same permutation symmetry. This is partially due to the fact that the local Clifford operations transforming the CWS code into the standard form may break the permutation symmetry of the original code. Also, the graphs usually can only represent the symmetry of the stabilizer generators of the stabilizer state, but not the symmetry of the stabilizer state in general. We show that this is indeed the case for the toric code on a two-dimensional square lattice with translational symmetry, even if its encoding graph can be chosen to be translational invariant.

However, we show that the converse always holds, i. e., any graph  $\mathcal{G}$  and classical code  $\mathcal{C}$  with certain permutation symmetry yields a CWS code  $\mathcal{Q} = (\mathcal{G}, \mathcal{C})$  with the same symmetry.

## 2 Preliminaries

The single-qudit (generalized) Pauli group is generated by the operators  $X$  and  $Z$  acting on the qudit Hilbert space  $\mathbb{C}^p$ , satisfying  $ZX = \omega XZ$ , where  $\omega = \omega_p = \exp 2i\pi/p$ . For simplicity, throughout the paper, we assume that  $p$  is a prime, although our results naturally extend to prime powers. Denote the computational basis of  $\mathbb{C}^p$  by  $\{|j\rangle : j = 0, 1, \dots, p-1\}$ . Then, without loss of generality, we can fix the operators  $X$  and  $Z$  such that  $X|j\rangle = |j+1\rangle$  and  $Z|j\rangle = \omega^j|j\rangle$ , respectively. Let  $I$  be the identity operator. The set  $\{X^a Z^b : a, b = 0, \dots, p-1\}$  of  $p^2$  operators forms a so-called nice unitary error basis which is a particular basis for the vector space of  $p \times p$  matrices [15, 16].

The  $n$ -qudit Pauli group  $\mathcal{P}_n$  consists of all local operators of the form  $\mathbf{M} = \alpha_{\mathbf{M}} M_1 \otimes \dots \otimes M_n$ , where  $\alpha_{\mathbf{M}} = \omega^k$  for some integer  $k$  is an overall phase factor, and  $M_i = X_i^a Z_i^b$  for some  $a, b \in \{0, 1, \dots, p-1\}$ , is an element of the single-qudit Pauli group of qudit  $i$ . We can write  $\mathbf{M}$  as  $\alpha_{\mathbf{M}} (M_1)_1 (M_2)_2 \dots (M_n)_n$  or  $\alpha_{\mathbf{M}} M_1 M_2 \dots M_n$  when it is clear what the qudit labels are. The weight of an operator  $\mathbf{M}$  is the number of tensor factors  $M_i$  that differ from identity.

The  $n$ -qudit Clifford group  $\mathcal{L}_n$  is the group of  $p^n \times p^n$  unitary matrices that map  $\mathcal{P}_n$  to itself under conjugation. The  $n$ -qudit local Clifford group is a subgroup in  $\mathcal{L}_n$  containing elements of the form  $M_1 \otimes \dots \otimes M_n$ , where each  $M_i$  is a single qudit Clifford operation, i. e.,  $M_i \in \mathcal{L}_1$ .

A stabilizer group  $\mathcal{S}$  in the Pauli group  $\mathcal{P}_n$  is defined as an abelian subgroup of  $\mathcal{P}_n$  which does not contain  $\omega I$ . A stabilizer consists of  $p^m$  Pauli operators for some  $m \leq n$ . As the operators in a stabilizer commute with each other, they can be simultaneously diagonalized. The common eigenspace of eigenvalue 1 is a stabilizer quantum code  $\mathcal{Q} = ((n, K, d))_p$  with length  $n$ , dimension  $K = p^{n-m}$ , and minimum distance  $d$ . The projection  $P_{\mathcal{Q}}$  onto the code  $\mathcal{Q}$  can be expressed as

$$P_{\mathcal{Q}} = \frac{1}{|\mathcal{S}|} \sum_{M \in \mathcal{S}} M. \quad (1)$$

The centralizer  $C(\mathcal{S})$  of the stabilizer  $\mathcal{S}$  is given by the elements in  $\mathcal{P}_n$  which commute with all elements in  $\mathcal{S}$ . For  $m < n$ , the minimum distance  $d$  of the code  $\mathcal{Q}$  is the minimum weight of all elements in  $C(\mathcal{S}) \setminus \mathcal{S}$ .

If  $m = n$ , then there exists a unique  $n$ -qudit state  $|\psi\rangle$  such that  $\mathbf{M}|\psi\rangle = |\psi\rangle$  for every  $\mathbf{M} \in \mathcal{S}$ . Such a state  $|\psi\rangle$  is called a stabilizer state, and the group  $\mathcal{S} = \mathcal{S}(|\psi\rangle)$  is called the stabilizer of  $|\psi\rangle$ . A stabilizer state can also be viewed as a self-dual code over the finite field  $\mathbb{F}_{p^2}$  under the trace inner product [7]. For a stabilizer state, the minimum distance is defined as the minimum weight of the non-trivial elements in  $\mathcal{S}(|\psi\rangle)$  [7].

A union stabilizer (USt) code of length  $n$  is characterized by a stabilizer code with stabilizer  $\mathcal{S} = \langle \mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_m \rangle$ , where  $\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_m$  are  $m$  independent generators, and a classical code  $\mathcal{C}$  over  $\mathbb{F}_p$  of length  $m$ . Note that for a given  $\mathcal{S}$ , the choice of the  $m$  generators  $\mathbf{g}_j$  is not unique. Now for a classical code  $\mathcal{C}$  of length  $m$  with  $K$  codewords, for each codeword  $\mathbf{c} = (c_1, c_2, \dots, c_m) \in \mathcal{C}$ , the corresponding quantum code is given by the subspace  $V_{\mathbf{c}}$  stabilized by  $\omega^{c_1} \mathbf{g}_1, \omega^{c_2} \mathbf{g}_2, \dots, \omega^{c_m} \mathbf{g}_m$ . Note that for  $\mathbf{c} \neq \mathbf{c}' \in \mathcal{C}$ , the subspaces  $V_{\mathbf{c}}$  and  $V_{\mathbf{c}'}$  are mutually orthogonal. The corresponding USt code is then given by the subspace  $\bigoplus_{\mathbf{c}} V_{\mathbf{c}}$ .

Therefore, the combination of  $\mathcal{S}$  (more precisely, the generators of  $\mathcal{S}$ ) and  $\mathcal{C}$  gives an  $((n, 2^{n-m}K))_p$  USt quantum code  $\mathcal{Q}$ . Hence we denote a USt code  $\mathcal{Q}$  by  $\mathcal{Q} = (\mathcal{S}, \mathcal{C})$ . The projection onto  $\mathcal{Q}$  can be expressed as

$$P_{\mathcal{Q}} = \sum_{\mathbf{c} \in \mathcal{C}} \frac{1}{p^m} \sum_{\mathbf{y} \in \mathbb{F}_p^m} \omega^{\mathbf{c} \cdot \mathbf{y}} \mathbf{g}_1^{y_1} \dots \mathbf{g}_m^{y_m}, \quad (2)$$

where we identify the elements  $y_i$  of the finite field with integers modulo  $p$ .

A CWS code  $\mathcal{Q}$  of length  $n$  is a USt code with  $m = n$ . That is, it is characterized by a stabilizer state with stabilizer  $\mathcal{S}$  and a classical code  $\mathcal{C}$  of length  $n$ . For a CWS code  $\mathcal{Q}$  given by  $\mathcal{Q} = (\mathcal{S}, \mathcal{C})$ , the stabilizer  $\mathcal{S}$  always corresponds to a unique stabilizer state. We will then refer to  $\mathcal{S}$  as the stabilizer state when no confusion arises.

For a CWS code, the projection  $P_{\mathcal{Q}}$  onto the code space is given by

$$P_{\mathcal{Q}} = \sum_{\mathbf{t} \in \mathcal{C}} \frac{1}{p^n} \sum_{\mathbf{x} \in \mathbb{F}_p^n} \omega^{\mathbf{t} \cdot \mathbf{x}} \mathbf{g}_1^{x_1} \dots \mathbf{g}_n^{x_n}, \quad (3)$$

where we again identify the elements  $x_i$  of the finite field with integers modulo  $p$ .

A CWS code has a permutation symmetry  $\sigma$  if

$$P_{\mathcal{Q}}^{\sigma} = P_{\mathcal{Q}}, \quad (4)$$

where  $P_{\mathcal{Q}}^{\sigma}$  is the projection onto the space obtained by permuting the qudits of the code  $\mathcal{Q}$  according to  $\sigma$ .

### 3 Canonical form of CWS codes

For a given a CWS code  $\mathcal{Q} = (\mathcal{S}, \mathcal{C})$ , there might exist another stabilizer state  $\mathcal{S}'$  and another classical code  $\mathcal{C}'$  such that  $\mathcal{Q} = (\mathcal{S}', \mathcal{C}')$ . In other words, the representation of a CWS code by the stabilizer state  $\mathcal{S}$  and the classical code  $\mathcal{C}$  is non-unique.

In order to discuss the relationship between the symmetry of the CWS code  $\mathcal{Q}$  and that of the stabilizer state  $\mathcal{S}$ , we first need to explore the relationship between the different representations of  $\mathcal{Q}$  (i. e., the relationship between  $\mathcal{S}$  and  $\mathcal{S}'$ , as well as the relationship between  $\mathcal{C}$  and  $\mathcal{C}'$ ).

Let us start by recalling that a stabilizer code can be viewed as a CWS code where the classical code is a linear code [6]. A simple way to see this is that for a given stabilizer code  $\mathcal{Q}_s$  with stabilizer generated by  $\mathcal{S} = \langle \mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_m \rangle$ , which is a code of dimension  $p^{n-m}$ , we can choose the larger stabilizer  $\mathcal{S}' = \langle \mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_m, \bar{Z}_1, \dots, \bar{Z}_{n-m} \rangle$ , where  $\bar{Z}_1, \dots, \bar{Z}_{n-m} \in C(\mathcal{S})$  mutually commute. Now choose the classical code  $\mathcal{C}' = \{(0, \dots, 0, x_{m+1}, \dots, x_n) : x_j \in \{0, \dots, p-1\}\}$  of length  $n$  with  $p^{n-m}$  codewords, where the first  $m$  coordinates of each codeword are zero. Then we have  $\mathcal{Q}_s = (\mathcal{S}', \mathcal{C}')$ , i. e., the stabilizer code  $\mathcal{Q}_s$  can then be viewed as a CWS code with stabilizer state  $\mathcal{S}'$  and classical code  $\mathcal{C}'$ . However, note that the choice of  $\mathcal{S}'$  (and hence  $\mathcal{C}'$ ) is non-unique, as in particular the choice of  $\bar{Z}_1, \dots, \bar{Z}_{n-m} \in C(\mathcal{S})$  is non-unique.

► **Example 1.** As an example, consider the five-qubit code with stabilizer

$$\mathbf{g}_1 = XZZXI, \quad \mathbf{g}_2 = IXZZX, \quad \mathbf{g}_3 = XIXZZ, \quad \mathbf{g}_4 = ZXIXZ. \quad (5)$$

In the CWS picture, the stabilizer state can be chosen as

$$\mathcal{S} = \langle \mathbf{g}_1, \mathbf{g}_2, \mathbf{g}_3, \mathbf{g}_4, \mathbf{Z}_L \rangle, \quad (6)$$

where  $\mathbf{Z}_L = Z^{\otimes 5}$  is the logical  $Z$  operator. Alternatively, one can choose the stabilizer state

$$\mathcal{S}' = \langle \mathbf{g}_1, \mathbf{g}_2, \mathbf{g}_3, \mathbf{g}_4, \mathbf{X}_L \rangle, \quad (7)$$

where  $\mathbf{X}_L = X^{\otimes 5}$  is the logical  $X$  operator. For both  $\mathcal{S}$  and  $\mathcal{S}'$ , the classical code can be chosen as  $\mathcal{C} = \{00000, 00001\}$ .

Similarly, a USt code  $(\mathcal{S}, \mathcal{C})$  can be viewed as a CWS code  $(\mathcal{S}', \mathcal{C}')$  with the classical code  $\mathcal{C}'$  of length  $n$  possessing some coset structure, i. e.,  $\mathcal{C}' = \bigcup_{\mathbf{t}_i \in \bar{\mathcal{C}}} \mathcal{C}_0 + \mathbf{t}_i$ , where  $\mathcal{C}_0$  is a linear code. This linear code  $\mathcal{C}_0$  of length  $n$  can be readily chosen as the classical code for the CWS representation of the stabilizer code  $\mathcal{S}$ . The code  $\bar{\mathcal{C}}$  of length  $n$  can be derived from  $\mathcal{C}$  of length  $m$  by appending  $n - m$  zero coordinates. However, again, the choices of  $\mathcal{S}'$  and  $\mathcal{C}'$  are non-unique.

In the general situation, we have some freedom in choosing the stabilizer state when representing a stabilizer code or a USt code in the CWS framework. Consequently, for a given CWS code  $\mathcal{Q}$ , there are also many different ways to write it in terms of a USt code in general. We will show, however, that we can always obtain a unique stabilizer  $\mathcal{S}$ , when expressing a given CWS code as a USt code. The following theorem gives a canonical form for any CWS code.

► **Theorem 2.** *Every CWS code has a unique representation as a union stabilizer code.*

**Proof.** To prove this theorem, we will need some lemmas.

► **Lemma 3** (translational invariant codes). *Let  $\mathcal{C} \subset \mathbb{F}_p^n$  be a code over  $\mathbb{F}_p$  with  $|\mathcal{C}| = M$  and assume that for some non-zero  $\mathbf{s} \in \mathbb{F}_p^n$  we have  $\mathcal{C} = \mathcal{C} + \mathbf{s}$ , i. e., the code is invariant with respect to translation by  $\mathbf{s}$ . Then  $\mathcal{C}$  can be written as a disjoint union of cosets of the one-dimensional space  $\mathcal{C}_0 = \langle \mathbf{s} \rangle$  generated by  $\mathbf{s}$ , i. e.,*

$$\mathcal{C} = \bigcup_{\mathbf{t}_i \in \mathcal{C}'} \mathcal{C}_0 + \mathbf{t}_i,$$

where  $\mathcal{C}' \subset \mathbb{F}_p^n$  with  $|\mathcal{C}'| = M/p$ .

**Proof.** By assumption, for every  $\mathbf{x} \in \mathcal{C}$ , the vector  $\mathbf{x} + \mathbf{s}$  is in the code as well. Hence we can arrange the elements of  $\mathcal{C}$  as follows:

$\mathcal{C}'$	$\mathbf{t}_1$	$\mathbf{t}_2$	$\dots$	$\mathbf{t}_{M/p}$
$\mathcal{C}' + \mathbf{s}$	$\mathbf{t}_1 + \mathbf{s}$	$\mathbf{t}_2 + \mathbf{s}$	$\dots$	$\mathbf{t}_{M/p} + \mathbf{s}$
$\mathcal{C}' + 2\mathbf{s}$	$\mathbf{t}_1 + 2\mathbf{s}$	$\mathbf{t}_2 + 2\mathbf{s}$	$\dots$	$\mathbf{t}_{M/p} + 2\mathbf{s}$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$\mathcal{C}' + (p-1)\mathbf{s}$	$\mathbf{t}_1 + (p-1)\mathbf{s}$	$\mathbf{t}_2 + (p-1)\mathbf{s}$	$\dots$	$\mathbf{t}_{M/p} + (p-1)\mathbf{s}$

Every column in this arrangements is a coset  $\mathcal{C}_0 + \mathbf{t}_i$ . ◀

► **Lemma 4** (vanishing character sum). *Let  $\mathcal{C} \subset \mathbb{F}_p^n$  be an arbitrary code of length  $n$ . Assume that the function*

$$f: \mathbb{F}_p^n \rightarrow \mathbb{C}; \quad f(\mathbf{y}) = \sum_{\mathbf{c} \in \mathcal{C}} \omega^{\mathbf{c} \cdot \mathbf{y}},$$

where  $\omega = \exp(2\pi i/p)$ , vanishes outside a proper subspace  $V_0 < \mathbb{F}_p^n$ . Then there exists a non-zero vector  $\mathbf{s} \in \mathbb{F}_p^n$  such that  $\mathcal{C} = \mathcal{C} + \mathbf{s}$ . What is more, the code  $\mathcal{C}$  can be written as a union of cosets of the linear code  $\mathcal{C}_0 = V_0^\perp$ , i. e.,

$$\mathcal{C} = \bigcup_{\mathbf{t} \in \mathcal{C}'} \mathcal{C}_0 + \mathbf{t}. \quad (8)$$

**Proof.** Let  $\chi_{\mathcal{C}}(\mathbf{y})$  denote the characteristic function of the code  $\mathcal{C}$ , i. e.,  $\chi_{\mathcal{C}}(\mathbf{y}) \in \{0, 1\}$ , and  $\chi_{\mathcal{C}}(\mathbf{y}) = 1$  if and only if  $\mathbf{y} \in \mathcal{C}$ . Define  $g(\mathbf{y}) = 1 - (1 - \omega)\chi_{\mathcal{C}}(\mathbf{y})$ . Then  $g(\mathbf{y}) = \omega^{\chi_{\mathcal{C}}(\mathbf{y})}$ .

The Fourier transform of  $g(\mathbf{y})$  over  $\mathbb{F}_p^n$  reads

$$\begin{aligned} \hat{g}(\mathbf{y}) &= \frac{1}{\sqrt{p^n}} \sum_{\mathbf{x} \in \mathbb{F}_p^n} \omega^{\mathbf{x} \cdot \mathbf{y}} g(\mathbf{x}) \\ &= \frac{1}{\sqrt{p^n}} \sum_{\mathbf{x} \in \mathbb{F}_p^n} \omega^{\mathbf{x} \cdot \mathbf{y}} (1 - (1 - \omega)\chi_{\mathcal{C}}(\mathbf{x})) = \sqrt{p^n} \delta_{\mathbf{y}, \mathbf{0}} - \frac{1 - \omega}{\sqrt{p^n}} \sum_{\mathbf{x} \in \mathbb{F}_p^n} \omega^{\mathbf{x} \cdot \mathbf{y}} \chi_{\mathcal{C}}(\mathbf{x}) \\ &= \sqrt{p^n} \delta_{\mathbf{y}, \mathbf{0}} - \frac{1 - \omega}{\sqrt{p^n}} \sum_{\mathbf{c} \in \mathcal{C}} \omega^{\mathbf{c} \cdot \mathbf{y}} = \sqrt{p^n} \delta_{\mathbf{y}, \mathbf{0}} - \frac{1 - \omega}{\sqrt{p^n}} f(\mathbf{y}), \end{aligned}$$

where  $\delta_{\mathbf{y}, \mathbf{0}} = 1$  if  $\mathbf{y} = \mathbf{0}$ , and  $\delta_{\mathbf{y}, \mathbf{0}} = 0$  otherwise.

This shows that for  $\mathbf{y} \neq \mathbf{0}$ , the Fourier transform  $\hat{g}(\mathbf{y})$  is proportional to the function  $f(\mathbf{y})$ , and hence  $\hat{g}$  vanishes outside of  $V_0$  as well. Recall that  $\dim V_0 \leq n - 1$ , as  $V_0$  is a proper subspace by assumption. Let  $\mathbf{s} \in V_0^\perp$  be a non-zero vector that is orthogonal to all vectors in  $V_0$ . Furthermore, let  $V_0^c = \mathbb{F}_p^n \setminus V_0$  denote the set-complement of  $V_0$  in the full vector space.

We want to show that the code  $\mathcal{C}$  is invariant with respect to translations by  $\mathbf{s}$ , i. e.,  $\mathcal{C} = \mathcal{C} + \mathbf{s}$  or equivalently,  $\chi_{\mathcal{C}}(\mathbf{y} + \mathbf{s}) = \chi_{\mathcal{C}}(\mathbf{y})$ . This is in turn equivalent to showing that  $g(\mathbf{y}) = g(\mathbf{y} + \mathbf{s})$ . In the following,  $\mathcal{F}^{-1}$  denotes the inverse Fourier transform:

$$\begin{aligned} g(\mathbf{y} + \mathbf{s}) &= (\mathcal{F}^{-1} \hat{g})(\mathbf{y} + \mathbf{s}) = \frac{1}{\sqrt{p^n}} \sum_{\mathbf{x} \in \mathbb{F}_p^n} \omega^{-\mathbf{x} \cdot (\mathbf{y} + \mathbf{s})} \hat{g}(\mathbf{x}) \\ &= \frac{1}{\sqrt{p^n}} \sum_{\mathbf{x} \in V_0} \omega^{-\mathbf{x} \cdot (\mathbf{y} + \mathbf{s})} \hat{g}(\mathbf{x}) + \frac{1}{\sqrt{p^n}} \sum_{\mathbf{x} \in V_0^c} \omega^{-\mathbf{x} \cdot (\mathbf{y} + \mathbf{s})} \hat{g}(\mathbf{x}) \\ &= \frac{1}{\sqrt{p^n}} \sum_{\mathbf{x} \in V_0} \omega^{-\mathbf{x} \cdot \mathbf{s}} \omega^{-\mathbf{x} \cdot \mathbf{y}} \hat{g}(\mathbf{x}) \end{aligned}$$

$$\begin{aligned}
&= \frac{1}{\sqrt{p^n}} \sum_{\mathbf{x} \in V_0} \omega^{-\mathbf{x} \cdot \mathbf{y}} \hat{g}(\mathbf{x}) \\
&= \frac{1}{\sqrt{p^n}} \sum_{\mathbf{x} \in V_0} \omega^{-\mathbf{x} \cdot \mathbf{y}} \hat{g}(\mathbf{x}) + \frac{1}{\sqrt{p^n}} \sum_{\mathbf{x} \in V_0^c} \omega^{-\mathbf{x} \cdot \mathbf{y}} \hat{g}(\mathbf{x}) \\
&= \frac{1}{\sqrt{p^n}} \sum_{\mathbf{x} \in \mathbb{F}_p^n} \omega^{-\mathbf{x} \cdot \mathbf{y}} \hat{g}(\mathbf{x}) \\
&= (\mathcal{F}^{-1} \hat{g})(\mathbf{y}) = g(\mathbf{y}).
\end{aligned}$$

Here we have used the fact that  $\hat{g}(\mathbf{x})$  vanishes outside of  $V_0$  and that  $\mathbf{s}$  is orthogonal to all vectors in  $V_0$ .

From Lemma 3, it follows that the code  $\mathcal{C}$  can be written as a union of cosets of the code  $\mathcal{C}_0 = V_0^\perp$  generated by all vectors  $\mathbf{s}$  that are orthogonal to  $V_0$ . ◀

Now we are ready to prove Theorem 2. Let  $P_{\mathcal{Q}}$  denote the projection operator onto a CWS code  $\mathcal{Q} = ((n, K, d))_p$ , i. e.

$$\begin{aligned}
P_{\mathcal{Q}} &= \sum_{\mathbf{t} \in \mathcal{C}} \frac{1}{p^n} \sum_{\mathbf{x} \in \mathbb{F}_p^n} \omega^{\mathbf{t} \cdot \mathbf{x}} \mathbf{g}_1^{x_1} \dots \mathbf{g}_n^{x_n} = \frac{1}{p^n} \sum_{\mathbf{x} \in \mathbb{F}_p^n} \left( \sum_{\mathbf{t} \in \mathcal{C}} \omega^{\mathbf{t} \cdot \mathbf{x}} \right) \mathbf{g}_1^{x_1} \dots \mathbf{g}_n^{x_n} \\
&= \frac{1}{p^n} \sum_{\mathbf{x} \in \mathbb{F}_p^n} \alpha_{\mathbf{x}} \mathbf{g}_1^{x_1} \dots \mathbf{g}_n^{x_n} \tag{9}
\end{aligned}$$

where  $\mathbf{g}_1, \dots, \mathbf{g}_n$  are the generators of the stabilizer, and  $\mathcal{C} = (n, K)_p$  is a classical code.

First note that the coefficients  $\alpha_{\mathbf{x}}$  in (9) are uniquely determined since the  $p^n$  operators  $\{\mathbf{g}_1^{x_1} \dots \mathbf{g}_n^{x_n} : \mathbf{x} \in \mathbb{F}_p^n\}$  are a subset of the error-basis of linear operators on the space  $\mathbb{C}^{p^n}$ . The coefficient  $\alpha_{\mathbf{x}}$  is proportional to  $\text{tr}(\mathbf{g}_1^{x_1} \dots \mathbf{g}_n^{x_n} \cdot P_{\mathcal{Q}})$ . On the other hand,  $\alpha_{\mathbf{x}} = \sum_{\mathbf{t} \in \mathcal{C}} \omega^{\mathbf{t} \cdot \mathbf{x}} = f(\mathbf{x})$ , where  $f(\mathbf{x})$  is the function appearing in Lemma 4. So if the coefficients  $\alpha_{\mathbf{x}} = f(\mathbf{x})$  vanish outside of a proper subspace  $V_0 < \mathbb{F}_p^n$ , the classical code  $\mathcal{C}$  can be decomposed as union of cosets of  $\mathcal{C}_0 = V_0^\perp$ . Then (9) can be re-written as follows:

$$\begin{aligned}
P_{\mathcal{Q}} &= \frac{1}{p^n} \sum_{\mathbf{x} \in V_0} \left( \sum_{\mathbf{t}' \in \mathcal{C}'} \sum_{\mathbf{c} \in \mathcal{C}_0} \omega^{(\mathbf{t}' + \mathbf{c}) \cdot \mathbf{x}} \right) \mathbf{g}_1^{x_1} \dots \mathbf{g}_n^{x_n} \\
&= \frac{1}{p^n} \sum_{\mathbf{x} \in V_0} \left( \sum_{\mathbf{c} \in \mathcal{C}_0} \omega^{\mathbf{c} \cdot \mathbf{x}} \sum_{\mathbf{t}' \in \mathcal{C}'} \omega^{\mathbf{t}' \cdot \mathbf{x}} \right) \mathbf{g}_1^{x_1} \dots \mathbf{g}_n^{x_n} \\
&= \frac{|\mathcal{C}_0|}{p^n} \sum_{\mathbf{x} \in V_0} \left( \sum_{\mathbf{t}' \in \mathcal{C}'} \omega^{\mathbf{t}' \cdot \mathbf{x}} \right) \mathbf{g}_1^{x_1} \dots \mathbf{g}_n^{x_n} \tag{10}
\end{aligned}$$

In the last step we have used the fact that the spaces  $V_0$  and  $\mathcal{C}_0$  are orthogonal to each other, i. e., the inner product  $\mathbf{c} \cdot \mathbf{x}$  vanishes. Now assume that the space  $V_0$  has dimension  $m$  and that  $\{\mathbf{b}_1, \dots, \mathbf{b}_m\} \subset \mathbb{F}_p^n$  is a basis of  $V_0$ . Then every vector  $\mathbf{x} \in V_0$  can be expressed as  $\mathbf{x} = \sum_{j=1}^m y_j \mathbf{b}_j$ . For every  $\mathbf{t}' \in \mathcal{C}'$  we define the vectors  $\mathbf{s} \in \mathbb{F}_p^m$  with  $s_j = \sum_{i=1}^n t'_i b_{ji}$ , forming another classical code  $\mathcal{D} \subset \mathbb{F}_p^m$ . Further, we define the  $m$  operators  $\tilde{\mathbf{g}}_j = \prod_{i=1}^n \mathbf{g}_i^{b_{ji}}$ . This allows us to express (10) as

$$P_{\mathcal{Q}} = \frac{1}{p^m} \sum_{\mathbf{y} \in \mathbb{F}_p^m} \left( \sum_{\mathbf{s} \in \mathcal{D}} \omega^{\mathbf{s} \cdot \mathbf{y}} \right) \tilde{\mathbf{g}}_1^{y_1} \dots \tilde{\mathbf{g}}_m^{y_m}. \tag{11}$$

Hence, whenever the classical code associated to a CWS code has some non-trivial shift invariance, the projection onto a CWS code can be expressed as a projection onto a USt code (cf. (2)), thereby increasing the dimension of the underlying stabilizer code and reducing the size of the classical code. In order to obtain a unique representation, we may assume that the stabilizer code is of maximal dimension, and hence the classical code is “without any linear structure.”

In order to show uniqueness, consider the coefficients  $\text{tr}(\mathbf{M} \cdot P_{\mathcal{Q}})$  of the expansion of the projection  $P_{\mathcal{Q}}$  in terms of the operator basis formed by the  $n$ -qudit Pauli matrices  $\mathbf{M}$ . Clearly, we have  $\{\mathbf{M} : \text{tr}(\mathbf{M} \cdot P_{\mathcal{Q}}) \neq 0\} \subset \mathcal{S} = \langle \tilde{\mathbf{g}}_1, \dots, \tilde{\mathbf{g}}_m \rangle$ . If the group  $\mathcal{S}' = \langle \mathbf{M} : \text{tr}(\mathbf{M} \cdot P_{\mathcal{Q}}) \neq 0 \rangle$  was a proper subgroup of  $\mathcal{S}$ , the coefficients  $\sum_{\mathbf{s} \in \mathcal{D}} \omega^{\mathbf{s} \cdot \mathbf{y}}$  would vanish for  $\mathbf{y}$  outside a proper subspace  $V_0 < \mathbb{F}_p^m$ , contradicting the assumption the classical code  $\mathcal{D}$  has no linear structure.

Note that the stabilizer  $\mathcal{S}$  is only unique up to the choice of some phase factors of the error basis. For example, replacing  $\tilde{\mathbf{g}}_1$  by  $\omega \tilde{\mathbf{g}}_1$  will introduce some phase factor which has to be compensated by changing the first coordinate  $s_1$  of the codewords  $\mathbf{s}$  of the classical code  $\mathcal{D}$ . To finally fix these degrees of freedom, we can enforce  $\mathbf{g}_i = M_1 \otimes \dots \otimes M_n$ , with  $M_j = X_j^a Z_j^b$  for  $j = 1, 2, \dots, n$  and  $a, b \in \{0, 1, \dots, p-1\}$ . ◀

#### 4 Symmetries of the stabilizer state of a CWS code

We are now ready to discuss the relationship between the symmetries of the CWS code  $\mathcal{Q}$  and that of the corresponding stabilizer state  $\mathcal{S}$ .

► **Theorem 5.** *For any CWS code  $\mathcal{Q}$  with permutation symmetry  $\sigma$ , there exists a stabilizer state  $\mathcal{S}$  with the same permutation symmetry  $\sigma$  such that  $\mathcal{Q} = (\mathcal{S}, \mathcal{C})$ .*

**Proof.** To prove this theorem, we will need some lemmas.

► **Lemma 6.** *If the projection operator  $P_{\mathcal{C}}$  given in Eq. (9) is invariant under a permutation  $\sigma$  of the qudits, then the stabilizer code related to expressing  $P_{\mathcal{C}}$  in terms of a USt code as in Eq. (11) is invariant with respect to the permutation as well.*

**Proof.** The statement follows directly from the uniqueness of the stabilizer group  $\mathcal{S} = \langle \tilde{\mathbf{g}}_1, \dots, \tilde{\mathbf{g}}_m \rangle$  generated by the operators in Eq. (11). ◀

We now prove a lemma for a special case of Theorem 5, when the CWS code is a Calderbank–Shor–Steane (CSS) code [4, 22].

► **Lemma 7.** *For a CSS code  $\mathcal{Q}$  with permutation symmetry  $\sigma$ , there exists a stabilizer state  $|\psi\rangle \in \mathcal{Q}$  such that  $|\psi\rangle$  has the same permutation symmetry as  $\mathcal{Q}$ .*

**Proof.** For a CSS code  $\mathcal{Q}$ , the stabilizer generators can always be chosen such that every generator is either a tensor product of powers of  $X$  (denoted by  $\mathcal{S}_X$ ) or a tensor product of powers of  $Z$  (denoted by  $\mathcal{S}_Z$ ). We can use the following matrix form:

$$\left[ \begin{array}{c|c} \mathcal{S}_X & 0 \\ \hline 0 & \mathcal{S}_Z \end{array} \right]$$

As the permutation symmetry  $\sigma$  of  $\mathcal{Q}$  does not change the type of an operator, both  $\mathcal{S}_X$  and  $\mathcal{S}_Z$  have necessarily the same symmetry  $\sigma$ . Furthermore, the logical operators can also be chosen as either tensor products of powers of  $X$  or tensor products of powers of  $Z$ , which correspond to the dual of the classical codes associated to either the  $Z$  stabilizers or the  $X$  stabilizers, respectively. Without loss of generality let us choose a set  $\mathcal{L}_Z$  of commuting



logical operators which are all of  $Z$  type. Then the group generated by the set  $\mathcal{S}_X \cup \mathcal{S}_Z \cup \mathcal{L}_Z$  of mutually commuting operators is again invariant under the permutation  $\sigma$ . As the stabilizer group is maximal, it stabilizes a unique state  $|\psi\rangle$ . Hence  $|\psi\rangle$  is the stabilizer state with the desired symmetry, and the CSS code can be expressed as CWS code in terms of  $|\psi\rangle$  and some classical code  $\mathcal{C}$ . ◀

We now prove a lemma for the stabilizer code case of Theorem 5, which improves the result of Lemma 7.

► **Lemma 8.** *For a stabilizer code  $\mathcal{Q}$  with permutation symmetry  $\sigma$ , there exists a stabilizer state  $|\psi\rangle \in \mathcal{Q}$  such that  $|\psi\rangle$  has the same permutation symmetry as  $\mathcal{Q}$ .*

**Proof.** To prove this lemma, we shall use a standard form for stabilizers (see [20, Section 10.5.7]):

$$\left[ \begin{array}{ccc|ccc} I & A_1 & A_2 & B & 0 & C \\ 0 & 0 & 0 & D & I & E \end{array} \right] = \left[ \begin{array}{c|c} \mathcal{S}_X & \mathcal{S}_Z \\ 0 & \mathcal{S}'_Z \end{array} \right] = \left[ \begin{array}{c} \mathcal{S} \\ \mathcal{S}' \end{array} \right]$$

where  $A_1$  is an  $r \times (n - k - r)$  matrix,  $A_2$  is an  $r \times k$  matrix,  $B$  is an  $r \times r$  matrix,  $C$  is an  $r \times k$  matrix,  $D$  is an  $(n - k - r) \times r$  matrix, and  $E$  is an  $(n - k - r) \times k$  matrix. Similar as in the CSS case, we can choose a set  $\mathcal{L}_Z$  of commuting logical operators which are all of  $Z$  type. In matrix form, they are given by  $[0 \ 0 \ 0 | -A_2^t \ 0 \ I]$ . Then the group generated by the mutually commuting operators in  $\mathcal{S} \cup \mathcal{S}' \cup \mathcal{L}_X$  stabilizes a unique state  $|\psi\rangle$  which is invariant with respect to the permutation  $\sigma$ . Hence  $|\psi\rangle$  is the stabilizer state with the desired symmetry that can be used to express  $\mathcal{Q}$  as CWS code with some classical code  $\mathcal{C}$ . ◀

To prove Theorem 5, given a CWS code  $\mathcal{Q}$ , we first find its unique decomposition as a UST code  $\mathcal{Q} = (\mathcal{S}, \mathcal{C})$ , based on Theorem 2. Here  $\mathcal{S}$  is in general a stabilizer code with  $m = n - k$  generators. If  $\mathcal{Q}$  has a permutation symmetry  $\sigma$ , then according to Lemma 6, the stabilizer code  $\mathcal{S}$  must also have the symmetry  $\sigma$ . Now according to Lemma 8, there exists a quantum state  $|\psi\rangle$  in the stabilizer code  $\mathcal{S}$  which also has the symmetry  $\sigma$ . Hence  $|\psi\rangle$  is the stabilizer state with the desired symmetry. Note that the stabilizer  $\mathcal{S}'$  of the state  $|\psi\rangle$  contains the original stabilizer  $\mathcal{S}$ . Therefore, common eigenspaces of  $\mathcal{S}$  are further decomposed into one-dimensional joint eigenspaces of  $\mathcal{S}'$ , and we can rewrite the projection  $P_{\mathcal{Q}}$  onto the UST code in the form corresponding to a CWS code. ◀

## 5 Symmetries of the Classical Code

Theorem 5 does not make any statement about the symmetry of the classical code. In general, if we insist to use the canonical form of the CWS code as given by Theorem 2, we cannot expect that the (non-linear) classical code  $\mathcal{C}$  associated with the CWS code  $\mathcal{Q} = (\mathcal{S}, \mathcal{C})$  has the same symmetry as  $\mathcal{Q}$ . That is, in this case, even if the stabilizer  $\mathcal{S}$  has the same permutation symmetry  $\sigma$  as the quantum code  $\mathcal{Q}$ , one might not be able to find a classical code  $\mathcal{C}$  with the same symmetry  $\sigma$  in general. Let us look at an example.

► **Example 9.** Consider the stabilizer state  $1/\sqrt{2}(|00\dots 0\rangle - |11\dots 1\rangle)$  (hence a CWS code, denoted by  $\mathcal{Q}$ ), which is invariant under all permutations. Using the canonical form of  $\mathcal{Q} = (\mathcal{S}, \mathcal{C})$  as given by Theorem 2, the group  $\mathcal{S}$  is generated by  $XX\dots X$  and all pairs of  $Z$ , which is permutation invariant. However, the classical code  $\mathcal{C}$  consists of the vector which is one in the first coordinate and zero elsewhere, i. e.,  $\mathcal{C}$  is a code with a single codeword  $10\dots 0$ , which has a smaller symmetry group than that of  $\mathcal{Q}$ .

On the other hand, if we choose the group  $\mathcal{S}'$  generated by  $-XX \dots X$  and all pairs of  $Z$ , the corresponding classical code  $\mathcal{C}'$  consists just of the zero vector. So in the representation  $\mathcal{Q} = (\mathcal{S}', \mathcal{C}')$ , both  $\mathcal{S}'$  and  $\mathcal{C}'$  have the same permutation symmetries as  $\mathcal{Q}$ .

This example indicates that exploiting the phase factor freedom in the USt code decomposition of a CWS code, and thereby deviating slightly from the canonical form, there is some chance to find both a stabilizer and a classical code with the same permutation symmetry as the CWS code.

To study the properties of the classical code  $\mathcal{C}$  associated with a CWS code  $\mathcal{Q} = (\mathcal{S}, \mathcal{C})$ , consider the case where the stabilizer state  $\mathcal{S}$  has some permutation symmetry  $\sigma$ . Then for given generators  $\{\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_n\}$  of the stabilizer  $\mathcal{S}$ , the permuted operators  $\{\mathbf{g}_1^\sigma, \mathbf{g}_2^\sigma, \dots, \mathbf{g}_n^\sigma\}$  generate the same stabilizer  $\mathcal{S}$ . The transformation  $\mathbf{g}_i \mapsto \mathbf{g}_i^\sigma$  can be characterized by a  $\mathbb{Z}_p$ -valued, invertible  $n \times n$  matrix  $R$  given by

$$\mathbf{g}_i^\sigma = \prod_{j=1}^n \mathbf{g}_j^{R_{ji}}. \quad (12)$$

Let us write the  $K$  classical codewords in  $\mathcal{C}$  as an  $K \times n$  matrix with entries  $c_{ij}$ . We are now ready to present the following theorem, which gives a sufficient condition for  $\mathcal{C}$  to guarantee that  $\mathcal{Q}$  has the same permutation symmetry as  $\mathcal{S}$

► **Theorem 10.** *Let  $\mathcal{Q} = (\mathcal{S}, \mathcal{C})$  be a CWS code, and let  $\{\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_n\}$  be generators of  $\mathcal{S}$ . If  $\mathcal{S}$  has permutation symmetry  $\sigma$ , where  $\mathbf{g}_i^\sigma = \prod_{j=1}^n \mathbf{g}_j^{R_{ji}}$ , and  $\mathcal{C}R \cong \mathcal{C}$ , then  $\mathcal{Q}$  has the same permutation symmetry  $\sigma$  as  $\mathcal{S}$ . Here by  $\mathcal{C}R \cong \mathcal{C}$  we mean that the set of rows of  $\mathcal{C}R$ , corresponding to the transformed code, equals the code  $\mathcal{C}$  (not as a matrix).*

**Proof.** We start by applying the permutation  $\sigma$  to the projection  $P_{\mathcal{Q}}$  onto the code space given by Eq. (3):

$$\begin{aligned} P_{\mathcal{Q}}^\sigma &= \sum_{\mathbf{t} \in \mathcal{C}} \frac{1}{p^n} \sum_{\mathbf{x} \in \mathbb{F}_p^n} \omega^{\mathbf{t} \cdot \mathbf{x}} (\mathbf{g}_1^\sigma)^{x_1} \dots (\mathbf{g}_n^\sigma)^{x_n} = \sum_{\mathbf{t} \in \mathcal{C}} \frac{1}{p^n} \sum_{\mathbf{x} \in \mathbb{F}_p^n} \omega^{\mathbf{t} \cdot \mathbf{x}} \left( \prod_j \mathbf{g}_j^{R_{j1}} \right)^{x_1} \dots \left( \prod_j \mathbf{g}_j^{R_{jn}} \right)^{x_n} \\ &= \sum_{\mathbf{t} \in \mathcal{C}} \frac{1}{p^n} \sum_{\mathbf{x} \in \mathbb{F}_p^n} \omega^{\mathbf{t} \cdot \mathbf{x}} \mathbf{g}_1^{\sum_j R_{1j} x_j} \dots \mathbf{g}_n^{\sum_j R_{nj} x_j} \end{aligned} \quad (13)$$

Let  $x'_j = \sum_i R_{ji} x_i$  and  $t_i = \sum_j R_{ji} t'_j$ . Then for  $\mathbf{t} \in \mathcal{C}$ , we have  $\mathbf{t}' \in \mathcal{C}'$ , where the transformed code  $\mathcal{C}'$ , considered as a  $K \times n$  matrix, is given by

$$\mathcal{C} = \mathcal{C}'R. \quad (14)$$

Then Eq. (13) becomes

$$\begin{aligned} P_{\mathcal{Q}}^\sigma &= \sum_{\mathbf{t}' \in \mathcal{C}'} \frac{1}{p^n} \sum_{\mathbf{x} \in \mathbb{F}_p^n} \omega^{\sum_i \sum_j R_{ji} t'_j x_i} \mathbf{g}_1^{\sum_j R_{1j} x_j} \dots \mathbf{g}_n^{\sum_j R_{nj} x_j} \\ &= \sum_{\mathbf{t}' \in \mathcal{C}'} \frac{1}{p^n} \sum_{\mathbf{x} \in \mathbb{F}_p^n} \omega^{\sum_j t'_j (\sum_i R_{ji} x_i)} \mathbf{g}_1^{\sum_j R_{1j} x_j} \dots \mathbf{g}_n^{\sum_j R_{nj} x_j} \\ &= \sum_{\mathbf{t}' \in \mathcal{C}'} \frac{1}{p^n} \sum_{\mathbf{x}' \in \mathbb{F}_p^n} \omega^{\mathbf{t}' \cdot \mathbf{x}'} \mathbf{g}_1^{x'_1} \dots \mathbf{g}_n^{x'_n}. \end{aligned} \quad (15)$$

Now because of  $\mathcal{C}R \cong \mathcal{C}$ , the rows of  $\mathcal{C}R$  are a permutation of the rows of  $\mathcal{C}$ . Hence there exists a permutation matrix  $P$  such that  $PCR = \mathcal{C}$ , which gives

$$PC = \mathcal{C}R^{-1} = \mathcal{C}'. \tag{16}$$

The second equality follows from Eq. (14). Hence the rows of  $\mathcal{C}'$  are a permutation of the rows of  $\mathcal{C}$ , i. e.,  $\mathcal{C}$  and  $\mathcal{C}'$  are the same code. Therefore Eq. (15) becomes

$$P_{\mathcal{Q}}^{\sigma} = \sum_{\mathbf{t}' \in \mathcal{C}} \frac{1}{p^n} \sum_{\mathbf{x}' \in \mathbb{F}_p^n} \omega^{\mathbf{t}' \cdot \mathbf{x}'} \mathbf{g}_1^{x'_1} \dots \mathbf{g}_n^{x'_n} = P_{\mathcal{Q}}, \tag{17}$$

which proves the theorem. ◀

Note that although Theorem 10 is stated in terms of a set of generator  $\mathbf{g}_i$  of  $\mathcal{S}$ , it is actually independent of the choice of the generators. That is to say, if  $\mathbf{g}_i^{\sigma} = \prod_{j=1}^n \mathbf{g}_j^{R_{ji}}$ , and  $\mathcal{C}R \cong \mathcal{C}$

holds, then for some other generators  $\mathbf{g}'_i$  of  $\mathcal{S}$ , where  $\mathcal{Q} = (\mathcal{S}_{\mathbf{g}'}, \mathcal{C}')$  and  $(\mathbf{g}'_i)^{\sigma} = \prod_{j=1}^n (\mathbf{g}'_j)^{R'_{ji}}$ , one would then have  $\mathcal{C}'R' \cong \mathcal{C}'$ .

Theorem 10 gives a sufficient condition that the CWS code  $\mathcal{Q} = (\mathcal{S}, \mathcal{C})$  may have the same permutation symmetry as  $\mathcal{S}$ . Note that [8, Proposition 5.2] considers a special case of Proposition 10, where the permutation  $\sigma$  is the cyclic shift. However, it turns out that the argument in [8] is false; the cyclic symmetry of the stabilizer  $\mathcal{S}$  is not sufficient to guarantee the cyclic symmetry of the resulting quantum code  $\mathcal{Q}$ ; the classical code  $\mathcal{C}$  must also have a cyclic symmetry, as discussed in Corollary 12.

It remains unclear whether the condition given in Theorem 10 is also necessary, at least in the case when both the CWS code  $\mathcal{Q}$  and the stabilizer  $\mathcal{S}$  have a permutation symmetry  $\sigma$ . We expect that in this case the condition  $\mathcal{C}R \cong \mathcal{C}$  would be necessary. However, while the condition might be violated for a particular choice of  $\mathcal{S}$ , it might hold for a different representation  $\mathcal{Q} = (\mathcal{S}', \mathcal{C}')$ .

## 6 The Standard Form $\mathcal{Q} = (\mathcal{G}, \mathcal{C})$

Starting with the unique representation of a CWS code as a USt code, we can derive a standard form of a CWS code. We know that up to local Clifford (LC) operations, any CWS code  $\mathcal{Q}$  can be represented by a graph  $\mathcal{G}$  and a binary classical code  $\mathcal{C}$  [5, 6]. Starting with a given CWS code  $\mathcal{Q} = (\mathcal{S}, \mathcal{C})$ , one can transform the stabilizer  $\mathcal{S}$  into a graph state using LC operations, and then  $\mathcal{C}$  will be transformed accordingly [5]. Our concern is that if  $\mathcal{Q}$  has some permutation symmetry  $\sigma$ , whether it can be kept during this LC operations, in other words, whether one can always obtain a graph with the same permutation symmetry  $\sigma$  as  $\mathcal{Q}$  has.

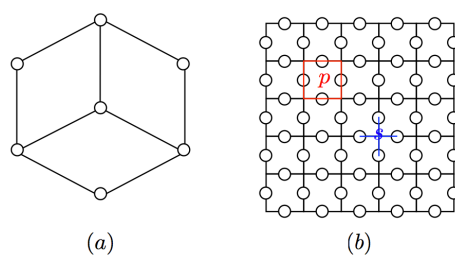
Indeed, even if one can always find a stabilizer state  $\mathcal{S}$  with the same symmetry as  $\mathcal{Q}$  has, we are asking too much here for the graph  $\mathcal{G}$ . In general, one cannot find a graph with the same permutation symmetry as  $\mathcal{Q}$  has. Let us look at an example.

► **Example 11.** The stabilizer  $\mathcal{S}$  for the 7-qubit Steane code is generated by

$$\mathbf{g}_1 = X1XXX11, \quad \mathbf{g}_2 = 1X1XXX1, \quad \mathbf{g}_3 = 11X1XXX, \tag{18}$$

which are the three  $X$ -type generators, and the three  $Z$ -type generators

$$\mathbf{g}_4 = Z1ZZZZ11, \quad \mathbf{g}_5 = 1Z1ZZZZ1, \quad \mathbf{g}_6 = 11Z1ZZZZ. \tag{19}$$



■ **Figure 1** (a) The graph for the Steane code with three-fold cyclic symmetry. (b) The toric code on a square lattice. Qubits are sitting on edges of the lattice.  $p$  denotes a plaquette, which contains 4 qubits as shown across the red lines.  $s$  denotes a star, which contains 4 qubits as shown across the blue lines.

This code is cyclic, and for its CWS representation, one can choose, e.g., the stabilizer state  $|\psi\rangle$  with stabilizer  $\mathcal{S}'$  generated by  $\mathcal{S}' = \langle \mathbf{g}_1, \mathbf{g}_2, \mathbf{g}_3, \mathbf{g}_4, \mathbf{g}_5, \mathbf{g}_6, Z^{\otimes 7} \rangle$ . Then  $|\psi\rangle$  is cyclic as well. However, when transforming the Steane code into the standard form of its CWS representation, one cannot find it a cyclic graph [10]. In fact, the best symmetric graph one can find is with a three-fold cyclic symmetry instead of a 7-fold cyclic symmetry, as shown in Fig. 1(a). The three-fold symmetry is in fact the symmetry of the generators of  $\mathcal{S}'$  instead of the symmetry of the entire stabilizer group  $\mathcal{S}'$ . This is related to the fact that the graph  $\mathcal{G}$  in some sense represents only the stabilizer generators of its corresponding graph state.

The toric code turns out to provide another example, as shown in Fig. 1(b), which is in some sense even worse than the Steane code example. Despite the fact that the generators of the stabilizer group for the toric code have a translational symmetry, we will show in Theorem 13 that one cannot find a graph with translational symmetry. However, both the Steane code and the toric code do not provide counterexamples to Theorem 5, as the logical zero has the desired symmetry in both cases.

Nevertheless, there might still be some interesting relationship between the permutation symmetries of  $\mathcal{Q}$  and the symmetries of  $\mathcal{G}$  and  $\mathcal{C}$ . Let us start with a simple case:

► **Corollary 12.** *For a CWS code  $\mathcal{Q} = (\mathcal{G}, \mathcal{C})$ , if both  $\mathcal{G}$  and  $\mathcal{C}$  have a permutation symmetry  $\sigma$ , then the code  $\mathcal{Q}$  has the permutation symmetry  $\sigma$  as well.*

**Proof.** This is actually a direct implication of Theorem 10; in this case the matrix  $R$  is nothing but a permutation matrix corresponding to the permutation  $\sigma$ . ◀

This turns out to be good luck, as due to the structure of the stabilizer generators of graph states, a permutation of the qubits corresponds to the same permutation of the generators  $\mathbf{g}_i$ , and hence also corresponds to a permutation of the coordinates in the classical code  $\mathcal{C}$ . Prominent examples are the  $((5, 2, 3))$  code and the  $((5, 6, 2))$  code, whose corresponding graph is a pentagon in both cases, and the corresponding classical codes are cyclic (see [6, Sec. IIIA,B]).

Finally, let us examine the graph symmetry for the toric code. The toric code was first proposed by Kitaev in 1997 as an example demonstrating topologically ordered quantum systems [13, 14]. The setting is a two-dimensional square lattice with periodic boundary conditions and with a qubit sitting on each edge of the lattice. There are two types of stabilizer generators:

1. + (star) type, indicated in Fig. 1(b) as  $s$ :

$$A_s^X = \prod_{j \in \text{star}(s)} X_j \quad (20)$$

2.  $\square$  (plaquette) type, indicated in Fig. 1(b) as  $p$ :

$$A_p^Z = \prod_{j \in \text{plaquette}(p)} Z_j \quad (21)$$

It is straightforward to check that  $A_s^X$  and  $A_p^Z$  commute for any pair  $s$  and  $p$ .

These stabilizer generators are by definition translational invariant, for the translation along each direction of the two-dimensional square lattice. What is more, one can even find an encoding graph which is also translational invariant [2]. We will show that unfortunately one cannot find a translational invariant graph to represent the toric code as a CWS code.

► **Theorem 13.** *A graph corresponding to the toric code cannot have the same translational symmetry as the code.*

**Proof.** Let  $\mathcal{T}$  be the toric code stabilizer generated by the star and plaquette operators as given by Eq. (20) and Eq. (21). Suppose that  $\mathcal{Q} = (\mathcal{G}, \mathcal{C})$  is a code where  $\mathcal{G}$  is as symmetric as the toric code stabilizer (i.e., translational invariant) and is local Clifford equivalent to  $\mathcal{T}$ . This means that if we let  $\mathcal{S}$  be the stabilizer of  $\mathcal{Q}$ , then there are local Clifford elements  $C_1, C_2, \dots$  such that  $\mathcal{S} = \widehat{C}\mathcal{T}\widehat{C}^\dagger$ , where  $\widehat{C} = C_1 \otimes C_2 \otimes \dots$  (here we choose an arbitrary indexing of qubits).

Let  $\sigma$  be a permutation symmetry of the toric code and define  $\widehat{C}_\sigma = C_{\sigma(1)} \otimes C_{\sigma(2)} \otimes \dots$ . Since  $\sigma$  is assumed to be a symmetry of  $\mathcal{S}$  as well, we have

$$\mathcal{S} = \widehat{C}\mathcal{T}\widehat{C}^\dagger = \widehat{C}_\sigma\mathcal{T}\widehat{C}_\sigma^\dagger.$$

Then for  $D_i = C_i^\dagger C_{\sigma(i)}$ , we have  $\widehat{D}\mathcal{T}\widehat{D}^\dagger = \mathcal{T}$ , where  $\widehat{D} = D_1 \otimes D_2 \otimes \dots$ .

Let  $XXXX$  be the element of this stabilizer group  $\mathcal{T}$  corresponding to some star  $\dagger$ . Since  $\widehat{D}$  is local, and  $XXXX$  is the only element of  $\mathcal{T}$  that acts on edges corresponding to  $\dagger$ , we must have  $\mathcal{D}XXXX\mathcal{D}^\dagger = XXXX$ . The same argument applies to the  $Z$ -terms corresponding to a plaquette  $\square$ . As a result, conjugation by  $D_i$  maps  $X$  to  $\pm X$  and  $Z$  to  $\pm Z$ . Hence  $D_i$  is an element of the Pauli group.

Now we know that  $\widehat{D}$  is in the Pauli group, and it holds for every permutation  $\sigma$ . On the other hand, the symmetry group of the toric code is transitive. Therefore, for every  $i, j$ , the product  $C_i^\dagger C_j$  is in the Pauli group, and furthermore

$$C_1 \otimes C_2 \otimes \dots = (H \otimes H \otimes \dots)(P_1 \otimes P_2 \otimes \dots),$$

where the factors  $P_i$  are in the Pauli group and  $H$  is some Clifford element acting on a single qubit.

$\widehat{C}\mathcal{T}\widehat{C}^\dagger$  is supposed to correspond to a graph state, but  $(P_1 \otimes P_2 \otimes \dots)$  just changes some signs in the stabilizer group, and  $(H \otimes H \otimes \dots)$  cannot turn the stabilizer group of the toric code into a graph-type stabilizer group. ◀

## 7 Summary and Discussion

In this work we have investigated the symmetry properties of CWS codes. Our main result shows that for a given CWS code  $\mathcal{Q}$  with some permutation symmetry  $\sigma$ , there always exists a stabilizer state  $\mathcal{S}$  with the same symmetry  $\sigma$  such that  $\mathcal{Q} = (\mathcal{S}, \mathcal{C})$  for some classical code  $\mathcal{C}$ . As many good CWS codes are found by starting from a chosen  $\mathcal{S}$ , this ensures that when trying to find CWS codes with certain permutation symmetry, the choice of  $\mathcal{S}$  with the same symmetry will suffice. A key point to reach our main result is to obtain a canonical representation for CWS codes, i.e., a unique decomposition as USt codes.

One natural question is whether there is any chance to find a classical code  $\mathcal{C}$  with the same symmetry  $\sigma$  as that of  $\mathcal{Q}$ , which, together with some  $\mathcal{S}$  with symmetry  $\sigma$ , gives  $\mathcal{Q} = (\mathcal{S}, \mathcal{C})$ . We do not know the answer in general, but we know that one can no longer restrict  $\mathcal{S}$  to the stabilizer used in the canonical form, but might have to introduce some phase factors. We have developed a sufficient condition that  $\mathcal{C}$  has to satisfy in order to ensure that in combination with some  $\mathcal{S}$  with symmetry  $\sigma$ , one will have  $\mathcal{Q} = (\mathcal{S}, \mathcal{C})$  with the same symmetry  $\sigma$ . Observing the fact that the permutation on the code  $\mathcal{Q}$  does not directly translate into a permutation of the classical  $\mathcal{C}$  (but a linear transformation given by the matrix  $R$ ), in general one cannot expect to find a classical code  $\mathcal{C}$  with the same symmetry as that of  $\mathcal{Q}$ .

One interesting case are cyclic codes. If there exists a graph  $\mathcal{G}$  which has the same symmetry  $\sigma$  as the CWS code  $\mathcal{Q} = (\mathcal{G}, \mathcal{C})$ , then the permutation of the code  $\mathcal{Q}$  translates directly into a permutation of the classical code  $\mathcal{C}$ . Hence, combining a graph  $\mathcal{G}$  whose symmetry group contains the cyclic group of order  $n$ , with a cyclic classical code  $\mathcal{C}$  of length  $n$ , gives a cyclic CWS code  $\mathcal{Q} = (\mathcal{G}, \mathcal{C})$ . It would be nice to see whether the converse is true as well, i. e., given a cyclic CWS code  $\mathcal{Q}$  which corresponds to a graph  $\mathcal{G}$  whose symmetry group contains the cyclic group of order  $n$ , can we always find a cyclic classical code  $\mathcal{C}$  of length  $n$ , such that  $\mathcal{Q} = (\mathcal{G}, \mathcal{C})$ . We leave this for future investigation.

In general, although every CWS code  $\mathcal{Q}$  is local Clifford equivalent to a standard form  $(\mathcal{G}, \mathcal{C})$ , the local Clifford operation may destroy the permutation symmetry of the original code. In other words, one cannot expect to always find a graph  $\mathcal{G}$  which has the same symmetry as that of  $\mathcal{Q}$ . The seven-qubit Steane code is such an example where the graph can only possess a three-fold cyclic symmetry which is the symmetry of the stabilizer generators, instead of the seven-fold cyclic symmetry of the code. For the toric code, despite the stabilizer generators being translational invariant, we show that there does not exist any associated translational invariant graph. A general understanding of the conditions that graphs can possess the same symmetry as the CWS code is worth further investigation.

**Acknowledgements.** SB was in part supported by National Elites Foundation and by a grant from IPM (No. 91810409). JC is supported by NSERC and NSF of China (Grant No. 61179030). The CQT is funded by the Singapore MoE and the NRF as part of the Research Centres of Excellence programme. ZJ acknowledges support from NSERC, ARO and NSF of China (Grant Nos. 60736011 and 60721061). QW is supported by NSERC. BZ is supported by NSERC and CIFAR. MG acknowledges support by the Intelligence Advanced Research Projects Activity (IARPA) via Department of Interior National Business Center contract No. D11PC20166. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright annotation thereon. Disclaimer: The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of IARPA, DoI/NBC, or the U.S. Government.

The authors would like to thank Martin Roetteler for his suggestion to use the Fourier transformation to prove Lemma 4.

---

## References

- 1 S. Beigi, I. Chuang, M. Grassl, P. Shor, and B. Zeng. Graph concatenation for quantum codes. *Journal of Mathematical Physics*, 52(2):022201, February 2011.
- 2 S. Bravyi and R. Raussendorf. Measurement-based quantum computation with the toric code states. *Physical Review A*, 76(2):022304, August 2007.

- 3 A. R. Calderbank, E. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction via codes over  $GF(4)$ . *IEEE Transactions on Information Theory*, 44(4):1369–1387, 1998.
- 4 A. R. Calderbank and P. W. Shor. Good quantum error-correcting codes exist. *Physical Review A*, 54:1098–1105, August 1996.
- 5 I. Chuang, A. Cross, G. Smith, J. Smolin, and B. Zeng. Codeword stabilized quantum codes: Algorithm and structure. *Journal of Mathematical Physics*, 50(4):042109, April 2009.
- 6 A. Cross, G. Smith, J. A. Smolin, and B. Zeng. Codeword stabilized quantum codes. *IEEE Transactions on Information Theory*, 55(1):433–438, 2009.
- 7 L. E. Danielsen. On self-dual quantum codes, graphs, and Boolean functions. Master’s thesis, University of Bergen, 2005. <http://arxiv.org/abs/quant-ph/0503236>.
- 8 S. Dutta and P. P. Kurur. Quantum Cyclic Code. Preprint arXiv:1007.1697 [cs.IT], June 2010.
- 9 D. Gottesman. *Stabilizer Codes and Quantum Error Correction*. PhD thesis, California Institute of Technology, Pasadena, CA, 1997.
- 10 M. Grassl, A. Klappenecker, and M. Rötteler. Graphs, quadratic forms, and quantum codes. In *Proceedings 2002 IEEE International Symposium on Information Theory (ISIT 2002)*, page 45, Lausanne, Switzerland, June/July 2002. <http://arxiv.org/abs/quant-ph/0703112>.
- 11 M. Grassl and M. Rötteler. Non-additive quantum codes from Goethals and Preparata codes. *Proceedings of 2008 IEEE Information Theory Workshop*, pages 396–400, 2008.
- 12 M. Grassl and M. Rötteler. Quantum Goethals-Preparata codes. *Proceedings of 2008 IEEE International Symposium on Information Theory*, pages 300–304, 2008.
- 13 A. Yu. Kitaev. Quantum computations: algorithms and error correction. *Russian Math. Surveys*, 52:1191–1249, 1997.
- 14 A. Yu. Kitaev, A. H. Shen, and M. N. Vyalı. *Classical and Quantum Computation*, volume 47 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2002.
- 15 E. Knill. Group Representations, Error Bases and Quantum Codes. Technical Report LAUR-96-2807, LANL, 1996. Preprint <http://arxiv.org/quant-ph/9608049>.
- 16 E. Knill. Non-binary Unitary Error Bases and Quantum Codes. Technical Report LAUR-96-2717, LANL, 1996. Preprint <http://arxiv.org/quant-ph/9608048>.
- 17 Y. Li, I. Dumer, and L. P. Pryadko. Clustered Error Correction of Codeword-Stabilized Quantum Codes. *Physical Review Letters*, 104(19):190501, May 2010.
- 18 S. Y. Looi, L. Yu, V. Gheorghiu, and R. B. Griffiths. Quantum error correcting codes using qudit graph states. *Physical Review A*, 78(4):042303, 2008.
- 19 F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland Publishing Company, Amsterdam, 1977.
- 20 M. Nielsen and I. Chuang. *Quantum computation and quantum information*. Cambridge University Press, Cambridge, England, 2000.
- 21 C. E. Shannon. A mathematical theory of communication. *Bell Labs Technical Journal*, 27:379–423, 1948.
- 22 A. Steane. Multiple particle interference and quantum error correction. *Proceedings of the Royal Society of London, Series A*, 452:2551–2577, 1996.
- 23 S. Yu, Q. Chen, and C. H. Oh. Graphical quantum error-correcting codes. Preprint arXiv:0709.1780 [quant-ph], September 2007.