

# On the addressability problem on CSS codes

Jérôme Guyot\* Samuel Jaques\*\*

\* ENS Paris-Saclay, Université Paris-Saclay, France

\*\* University of Waterloo, Canada

**Abstract.** Recent discoveries in asymptotically good quantum codes have intensified research on their application in quantum computation and fault-tolerant operations. This study focuses on the addressability problem within CSS codes: what circuits might implement logical gates on strict subsets of logical qubits? With some notion of fault-tolerance, we show some impossibility results: for CSS codes with non-zero rate, one cannot address a logical  $H$ ,  $HP$ ,  $PH$ , nor CNOT to any non-empty strict subset of logical qubits using a circuit made only from 1-local Clifford gates.

Furthermore, we show that one cannot permute the logical qubits in a code purely by permuting the physical qubits, if the rate of the code is (asymptotically) greater than  $\frac{1}{3}$  and the distance is at least 3. We can show a similar no-go result for CNOTs and CZs between two such high-rate codes, albeit with a less reasonable restriction to circuits that we call “global” (though recent addressable CCZ gates use global circuits).

This work pioneers the study of distance-preserving addressability in quantum codes, mainly by considering automorphisms of the code. This perspective offers new insights and potential directions for future research. We argue that studying this trade off between addressability and efficiency of the codes is essential to understand better how to do efficient quantum computation.

**Keywords:** Addressability, Quantum error correction, Quantum computing, CSS codes

## Introduction

### Motivation

Quantum computers are particularly vulnerable to noise, and so the most promising path to large-scale quantum computing is to use error-correcting codes. In these codes, many *physical* qubits are combined into one or more *logical* qubit(s), such that the logical qubits are long-lived and error-resistant.

A drawback of quantum error correction is that, by design, it becomes difficult to modify the encoded logical state. Unlike with classical error-correcting codes, we cannot decode the state to compute on it, as it is unlikely to remain coherent long enough for any operation. Thus, we need fault-tolerant quantum computation: not only should we have a method to encode the data, but we should also be able to operate on it *while* it is encoded.

A powerful tool in constructing fault-tolerant quantum computation is a *transversal* gate. Strictly speaking, this is any physical circuit that is guaranteed not to propagate errors between qubits of the code, and more commonly we require that it enacts some specific action on the logical state as well.

As an example, in a self-dual CSS code, applying an  $H$  (Hadamard) gate to all physical qubits in the code will not only preserve the codespace, it will effectively apply an  $H$  gate to all *logical* qubits in the code. However, in most quantum circuits we need more precision than this. We need to be able to apply specific gates to *only one* qubit in the code. We need our fault-tolerant operations to be *addressable*.

This distinction does not matter for surface codes, which (depending on the precise description) encode only one logical qubit. A large-scale surface code computation is best seen as a *product* of codes, each working independently. Any transversal gate can be targeted to a single logical qubit (or pair of qubits for a CNOT) by simply applying the gates only to those physical qubits corresponding to the desired logical qubit.

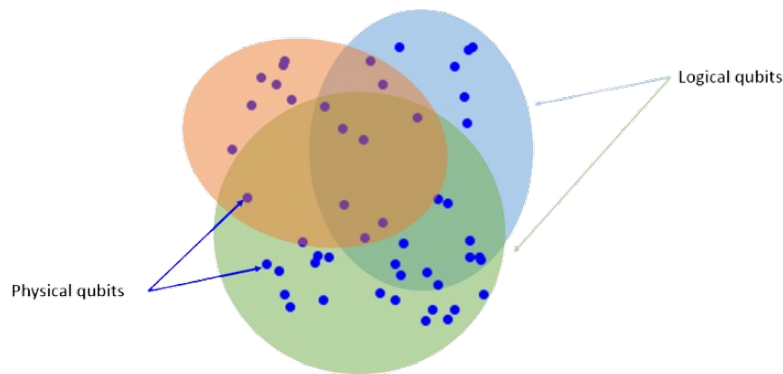
---

\* Email : [jerome.guyot@ens-paris-saclay.fr](mailto:jerome.guyot@ens-paris-saclay.fr)

\*\* Email : [sejaques@uwaterloo.ca](mailto:sejaques@uwaterloo.ca)

However, this strategy fails for more complicated codes that encode many qubits, where the notion of a correspondence between physical qubits and logical qubits is ill-defined (e.g., the overlaps in [Figure 1](#)). For good performance, the logical qubits are not spatially localized in this way. If we apply a gate to one physical qubit, it will impact many logical qubits.

Addressability is crucial for efficient quantum computation, as it removes the need for complex global circuits to extract it from transversality. While transversality was useful for single logical qubit codes like the surface code, its natural extension for larger codes is addressability. Unlike transversality, which treats all logical qubits collectively, addressability provides a more detailed view of a code's structure by considering each logical qubit individually. Studying addressability helps identify fundamental trade-offs in designing fault-tolerant operations for high-rate quantum codes, ensuring that logical operations remain precise and scalable in larger quantum systems.



**Fig. 1.** Visualization of a code

This addressability problem has become relevant recently, with the development of asymptotically good quantum codes [8,5]. As the size of the code increases, the number of logical qubits in these codes approaches exactly the number of physical qubits, while maintaining good code distance, which means logical qubits cannot be spatially localized. Thus, it is a challenging problem to find physical circuits which can address specific logical qubits for some desired logical gate, and that is what we address in this paper.

While considerable work has been done to find valid transversal implementations and study their actions on the code, very little has been done on the addressability problem until recently. Addressability is mentioned when a transversal gate allows it, such as in [12,3], but is rarely a goal itself. Previous works finding addressable gates like [10,9] do not solve fault-tolerance. Both [6] and [4] produce codes with addressable CCZ gates. While [6] is able to address disjoint triples of logical qubits, [4] is able to address any triple of logical qubits. In [4] they seek many of the same goals as we do, but with constructive results: their gates are fault tolerant, their codes can achieve constant rates, and they can address CCZ gates to arbitrary triples of logical qubits. Though, we will consider an even more stringent requirement: can one address arbitrary disjoint subsets of logical qubits *simultaneously*?

## Methods

We consider the problem of efficient physical circuits to enact logical gates addressably. There are two trivial ways to make addressable gates: the first is to decode, apply the gate, then re-encode, and the second is to use a product of smaller codes which admit transversal gates.

The first trivial method is problematic because it is not fault tolerant. The quantum state is unprotected after decoding. Thus, we consider gate sets that will not alter the distance of code. We take three approaches for this: first, 1-local circuits (i.e., circuits built from single-qubit gates); second, circuits made of SWAPs or other permutations; third, circuits made from a depth-1 CNOT or CZ circuit.

The second trivial method, products of codes, forbids us from having high-rate codes. One can readily see that if multiple codes are run in parallel, and we treat them as one larger code, the larger code’s distance is at most the minimum distance from one of the subcodes. Thus, asymptotically good codes cannot “split” into subcodes like this<sup>1</sup>.

We also notice that if we take any CSS code and apply any circuit of single-qubit gates, we will obtain another code with the same distance and rate. However, this new code may not be easy to work with and it may not have any of its own efficient fault-tolerant operations. Thus, we further require that our circuits preserve the original code space.

Ultimately, we are considering operators that preserve the code space, for CSS codes that do not split.

## Results

We show a series of impossibility results for addressable gates under the given restrictions.

We start with 1-local Clifford circuits: circuits made only from single-qubit Clifford gates. Since these have well-known commutation relations with Paulis, our main technique is to apply those relations to stabilizers and logical operators and ask when the output is consistent with the codespace and the desired logical action. We conclude that for any non-splitting code:

- Applying 1-local Clifford circuits which preserve the code cannot apply  $H$ ,  $PH$ , or  $HP$  to a strict subset of physical qubits (**Proposition 8**).
- No 1-local Clifford circuit can enact an addressable logical  $H$ ,  $PH$ ,  $HP$ , or CNOT gate (**Proposition 9**).
- If the code does not admit addressable  $P$  or  $PHP$  gates, it admits no addressable single-qubit gates from any level of the Clifford hierarchy (**Corollary 2**).

As introduced in [3], automorphisms of the code can be used to implement logical operations using permutations. Our second set of results uses this principle, just as in [3] or [7] which uses permutations to construct addressable Clifford gates. We show that the number of permutations which can preserve the codespace *and* produce distinct logical actions is, asymptotically, quite limited: for codes with rates above  $\frac{1}{3}$  and distance at least 3, it is less than  $k!$  when the code has  $k$  logical qubits.

With this idea, we can make several conclusions about CSS codes with distance at least 3:

- A circuit made from only SWAP gates (or any permutations of physical qubits) cannot implement any logical permutation on a code with rate asymptotically greater than  $\frac{1}{3}$ , cannot implement addressable CNOTs on codes with any constant rate, and for any 2-qubit gate  $G$ , such circuits cannot implement  $G$  addressably on codes with rates greater than  $\frac{3}{4}$ .
- A circuit between two codes, made by applying CNOT (resp. CZ) to all physical qubits, cannot implement *parallel* addressable CNOT (resp. CZ) on codes with rate asymptotically greater than  $\frac{1}{3}$  (**Propositions 12 and 13**). Here “parallel” means we can address CNOTs on disjoint sets of qubits simultaneously.

While the second result seems more restrictive, since the circuit must act on all physical qubits, the circuits for transversal CCZ gates from [4] satisfy this property, as would a CZ built from their methods. However, they do not aim for parallel addressability.

## Conclusions

Ideally, we would answer the question of addressability, by either giving a method to perform addressable gates on high-performance codes, or definitively proving that this is impossible. Instead, we have only *some* impossibility results. However, our results suggest what routes will be necessary if addressable gates are possible, highlight new proof techniques for considering these problems, and emphasize some of the restrictions we might need in considering the addressability problem.

For example, [9] and [10] seem to contradict our results by providing an addressable  $H$  gate. However, as these papers point out themselves, their techniques do not necessarily preserve distance. [9] involves enacting a linear transformation on the stabilizer vectors by applying a physical CNOT from each physical

<sup>1</sup> Or at least, they must contain an asymptotically good code which does not split.

qubit in the code to *an unprotected* auxiliary qubit. This means any phase error on this qubit will propagate up into the code. Hence, distance-preserving techniques remain an important consideration.

One easy fix might be to encode the auxiliary qubit in a different code (say, a surface code). However, it is not clear that there is such a targeted CNOT *between* such different codes. This is an open question that we hope can be resolved with techniques similar to those we employ in this work.

In concurrent work, [4] use a depth-1 physical CCZ circuit for both “intra-code” and “inter-code” addressable logical CCZ gates. They prove a constructive result for a constant code rate, whereas our CZ impossibility results apply to codes with higher rates than they construct. Despite the similarities between our impossibility results and their constructions, our results do not apply to their codes. The main difference is that our results forbid what we call “parallel addressability” (Definition 4), where if two logical gates act on disjoint sets of logical qubits, we can apply both simultaneously. Their construction has some ability to do this, but not completely.

In another concurrent work, [7] constructs codes with fault-tolerant circuits for addressable Clifford gates constructed from permutation automorphisms. Our results (Corollary 5) show that this method can only work for codes with asymptotically low rates (in  $o(1)$ ), and our upper bound is not far from the rate of their codes.

One method to escape our restrictions would be to allow the physical circuit to modify the code. For example, maybe there is a family of codes that can all be reached from each other by depth-1 CNOT circuits. This would be a special structure to have, so we assumed it did not exist, but finding such a structure would open up many possibilities for addressable gates.

Overall, we hope our results motivate more consideration of addressability and that our techniques can be taken further, either for constructive results or impossibility theorems. This work also shows that we should not take it for granted that, because one quantum error-correcting code is able to encode logical qubits more efficiently than another one, it will be overall more efficient for computation.

## 1 Background

### 1.1 Notation

Let  $\mathcal{P}_n$  be the set of  $n$ -qubit Pauli operators.

We define the Clifford hierarchy inductively as follows:  $\mathcal{C}_n^1 = \mathcal{P}_n$ , and for  $k > 1$ ,

$$\mathcal{C}_n^k = \{U \in \mathcal{U}_{2^n} \mid U\mathcal{P}_nU^\dagger \subseteq \mathcal{C}_{k-1}^n\}. \quad (1)$$

We call  $\mathcal{C}_n^k$  the  $k$ th level of the Clifford hierarchy, and we simply call  $\mathcal{C}_n^2$  the Clifford gates.

We let  $\llbracket n \rrbracket$  denote the set  $\{1, 2, \dots, n\}$ .

For a vector  $a \in \mathbb{F}_2^n$  and a single-qubit gate  $G$ , we let  $G^a$  denote the operator  $\otimes_{i:a_i=1} G_i$ , where  $G_i$  is  $G$  applied to qubit  $i$ .

For a vector  $a \in \mathbb{F}_2^n$ , and a set  $h \subseteq \llbracket n \rrbracket$ , we will sometimes use  $a \cap h$  to denote a vector in  $\mathbb{F}_2^n$  such that  $(a \cap h)_i = 1$  if and only if  $a_i = 1$  and  $i \in h$ .

A quantum code on  $n$  physical qubits, encoding  $k$  logical qubits, with distance  $d$ , is denoted as a  $\llbracket n, k, d \rrbracket$  code.

### 1.2 CSS Codes

We will work entirely with CSS codes [2]. A CSS code is constructed from two classical codes  $C_X, C_Z \subseteq \mathbb{F}_2^n$  such that  $C_Z \subseteq C_X^\perp$ . Let  $H_X$  and  $H_Z$  be the parity check matrices of  $C_X^\perp$  and  $C_Z^\perp$ .

We will let  $S_X = \{X^a \mid a \in C_X\}$  and  $S_Z = \{Z^b \mid b \in C_Z\}$ . We define the code  $\text{CSS}(C_X, C_Z)$  to be the set of quantum states in the +1 eigenspace of all operators in  $S_X$  and  $S_Z$ .

The orthogonality condition implies that all operators in  $S_X$  commute with all operators in  $S_Z$ .

Using generalized Paulis for the stabilizers, CSS codes can also be defined on qudits from codes on  $\mathbb{F}_q^n$  [11].

We define a logical operator to be any operator which preserves the codespace. If an operator acts as the identity on the codespace, we call it a logical identity.

**Proposition 1.**  *$L$  is a logical operator for a code  $C$  if and only if  $LI(C)L^\dagger \subseteq I(C)$  where  $I(C)$  is the set of logical identities for the code  $C$ .*

*Proof.* Let  $|\psi\rangle$  be a codeword and  $L$  a logical operator. Then  $L|\psi\rangle = |\phi\rangle$  for  $|\phi\rangle \in C$ . Let  $s \in I(C)$ . Then  $sL^\dagger|\phi\rangle = L^\dagger|\phi\rangle$ , so  $LsL^\dagger|\phi\rangle = |\phi\rangle$ . Thus,  $LsL^\dagger$  is a logical identity.

Conversely, if  $LI(C)L^\dagger \subseteq I(C)$  for an operator  $L$ , then for any  $s \in I(C)$ , there is  $s' \in I(C)$  such that  $sL = Ls'$ , so  $sL|\psi\rangle = Ls'|\psi\rangle = L|\psi\rangle$  for any  $|\psi\rangle \in C$ . Since the stabilizers for the code are included in  $I(C)$ , this implies  $L|\psi\rangle \in C$ , so  $L$  is a logical operator. □

The *normalizer* of a group  $G$  contained in a group  $E$  is the set of all  $h$  such that  $hGh^{-1} \subseteq G$ , and is denoted  $N_E(G)$  or just  $N(G)$  if  $E$  is clear from context.

For a stabilizer code,  $N_{P_n}(S)$  contains all logical Pauli operators on the code. More precisely for CSS codes,  $N_{P_n}(S_X)$  are all logical Pauli- $Z$  operators and  $N_{P_n}(S_Z)$  are all logical Pauli- $X$  operators. Quotienting by the stabilizer gives distinct logical Pauli operators as cosets of this space.

Since  $N(S_X)$  are Pauli- $Z$  strings, we can let each coset of  $N(S_X)/S_Z$  to be a logical  $Z$  operator, and similarly for  $N(S_Z)/S_X$ . This allows us to easily reason about the logical qubits and logical gates; for example, it tells us that the number of logical qubits is  $n - s_z - s_x$  where  $s_z = \dim(C_Z) = \text{rank}(H_Z)$  is the number of generators of  $S_Z$ , and similarly for  $s_x$ .

### 1.3 Code Rates

The *rate* of a code is the number of logical qubits  $k$  divided by the number of physical qubits  $n$ .

**Proposition 2.** *Let  $C = \text{CSS}(C_1, C_2)$ , and let  $\rho', \rho''$  be the maximum and minimum of the rates of the classical codes of  $C_1$  and  $C_2$ . Letting  $\rho$  be the rate of  $C$ , we have that  $\rho = \rho' + \rho'' - 1$  and  $2\rho'' - 1 \leq \rho \leq 2\rho' - 1$ .*

*Proof.* The rate is  $\rho = \frac{k}{n} = \frac{n-r}{n}$  where  $r = \dim(C_1^\perp) + \dim(C_2^\perp)$ . Thus,  $\rho_1 = \frac{n-\dim(C_1^\perp)}{n}$  and  $\rho_2 = \frac{n-\dim(C_2^\perp)}{n}$ , and hence  $\rho = \rho_1 + \rho_2 - 1$ . This directly gives  $2\rho'' - 1 \leq \rho \leq 2\rho' - 1$ . □

### 1.4 Transversality

Informally, a “transversal” gate is any gate which efficiently implements a logical qubit using physical gates, and typically refers to the case where we apply some physical gate  $U$  to all physical qubits and obtain the action of  $U$  on the logical qubits. However, transversality has a more general definition:

**Definition 1 (Transversality).** *Let  $\mathcal{Q} = (Q_i)_{i \in I}$  be a partition of the qubits in a code. We say that a gate  $U$  is transversal with respect to  $\mathcal{Q}$  if it can be decomposed as  $U = \otimes_{i \in I} U_i$  where  $U_i$  acts only on  $Q_i$ .*

*If  $\mathcal{Q}$  is not mentioned explicitly, it is taken to be  $Q_i = \{i\}$  for  $i = 1$  to  $n$ , or for multiply qubit gates with  $p$  blocks of a code, it is taken to be  $Q_i = \{i_1, i_2, \dots, i_p\}$  for  $i = 1$  to  $n$ .*

## 2 Addressability

We have previously defined a logical operator as an operator which preserves the codespace. We can now ask what action it has. First we recall that any operator  $U$  can be written as a linear combination of Paulis, i.e.,

$$U = \sum_{U_i \in \mathcal{P}_k} \alpha_i U_i \tag{2}$$

for coefficients  $\alpha$ . Thus, we say that a physical circuit  $G$  has the logical action of  $U$  on a code  $C$  if  $G$  is a logical operator on  $C$ , and for any  $|\psi\rangle$  in the code

$$G|\psi\rangle = \sum_{U_i \in \mathcal{P}_k} \alpha_i \bar{U}_i |\psi\rangle \tag{3}$$

where  $\bar{U}_i$  is a logical operator for the Pauli  $U_i$ .

Figure 2 visualizes such a circuit.

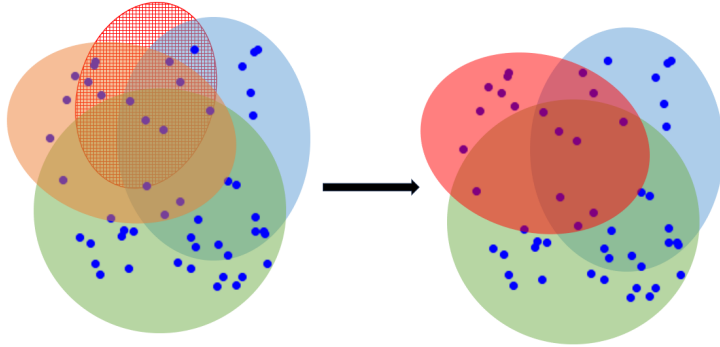


Fig. 2. As in Figure 1 we visualize a code with 3 logical qubits by the solid colored regions (with the coloring denoting the logical state of that qubit), and a physical circuit by the red hatched region. The physical circuit targeted the orange qubit: despite acting on some of the physical qubits in the blue logical qubit, the blue qubit does not change its logical state, while the state of the orange logical qubit changes from orange to red.

**Definition 2 (Addressability).**

Let  $U$  be a unitary on  $p$  qubits, and  $P$  be a family of quantum circuits. We say that  $U$  is  $P$ -addressable if, for any ordered tuple of  $p$  logical qubits  $t$ , there is a circuit in  $P$  implementing  $\bar{U}_t$ : the logical action  $\bar{U}$  the tuple  $t$ .

Figure 3 shows what it would mean to be addressable.

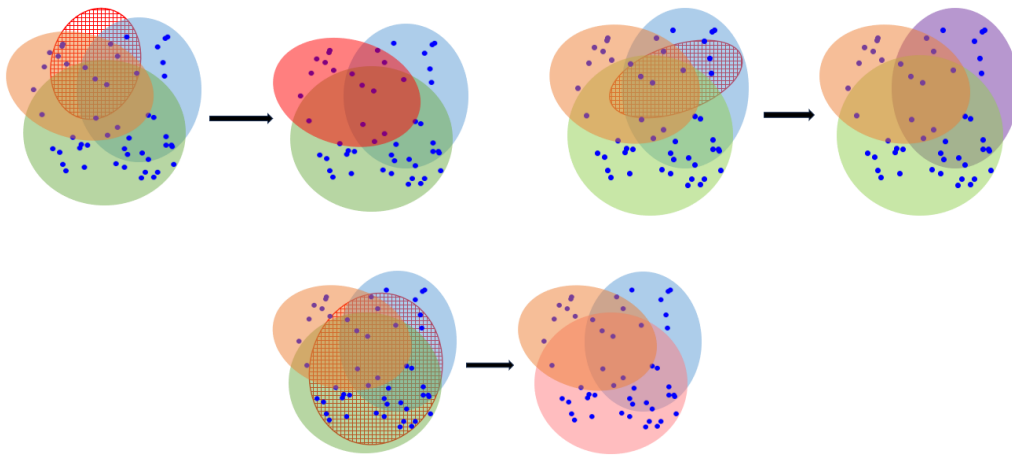


Fig. 3. As in Figure 2 we visualize a code with 3 logical qubits by the solid colored regions (with the coloring denoting the logical state of that qubit), and a physical circuit by the red hatched region. The physical circuits target only one logical qubit each time and act as some unitary that sends 'orange' to 'red', 'blue' to 'purple' and 'green' to 'pink'. In this case, this unitary is addressable on the code.

The restriction to a circuit family  $P$  ensures we do not capture the trivial circuits of decode-apply-encode. Some more useful families of circuits might be:

1. Circuits made from Clifford gates (Section 4)
2. Circuits with depth less than  $n$
3. Circuits with fewer than  $n$  gates
4. Circuits made from SWAPs (Section 5)
5. Circuits acting on all physical qubits (Section 5.3)

Some of these properties are not closed under composition (2,3), while others (1,4,5) are closed. To see why this matters, suppose we had an addressable  $T$  gate from depth-2 circuits, and we wanted to apply  $T$  gates to logical qubits 1 and 2. At the logical level, these gates *should* commute with each other and we should be able to apply them in parallel, but there is no guarantee that the physical circuit will still have depth 2. Thus, we give a stronger definition:

**Definition 3 (Parallel Addressability).** *Let  $U$  be a  $p$ -qubit unitary and  $P$  a family of circuits. We say that  $U$  is  $P$ -parallel addressable on  $C$  if, for any set  $I$  of disjoint ordered tuples of  $p$  logical qubits, there is a circuit in  $P$  which has the logical action  $\bar{U}$  applied to all tuples in  $I$ .*

It is easy to see that these definitions are equivalent if  $P$  is closed under composition:

**Lemma 1.** *Let  $U$  be a  $p$ -qubit unitary and  $P$  a family of circuits which is closed under composition. Then  $U$  is  $P$ -addressable if and only if  $U$  is  $P$ -parallel addressable.*

*Proof.* One direction is easy. Conversely, if  $U$  is  $P$ -addressable, then for any disjoint set of  $p$ -tuples of logical qubits  $\{I_k\}$ , we can find circuits in  $P$  for each tuple. Composing these together will have the required logical action, and the composed circuit will also be in  $P$ .  $\square$

We finally give a restricted definition of addressability to capture cases where we may be able to target *some* subsets of the logical qubits, but not all of them.

**Definition 4 (Partial Addressability).** *Let  $U$  be a  $p$ -qubit unitary and  $P$  a set of circuits. We say that  $U$  is  $P$ -partially addressable on  $C$  if there exists a set  $I$  of disjoint ordered tuples of  $p$  logical qubits ( $I \neq \emptyset, \llbracket k \rrbracket$ ) and a logical operator in  $P$  that has the logical action  $\bar{U}$  applied to all tuples in  $I$ .*

*Example 1.* Fig. 2 shows that  $U$  is partially addressable on this code since there is a targeting circuit implementing  $U$  on  $I = \{ \text{(Orange logical qubit)} \}$ .

Finally, we make a brief note about basis. The definition of a logical action requires a particular choice of “basis”, i.e., which logical operators in  $N(S)$  represent which logical Pauli operator. A different choice would change the logical action of an otherwise addressable gate; thus, our definitions are basis-dependent.

However, we do not see this as a limitation: firstly, some of our results forbid *any* logical action from certain circuit families, which is inherently a basis-independent result. Second, if we are allowed to modify the basis of a code, any gate becomes possible. For example, instead of performing a logical  $H$  gate, we could re-define the basis of the code to swap those  $X$  and  $Z$  stabilizers. This would require modifying all future gates, equivalent to commuting the  $H$  through all subsequent gates in the circuit. While such compilation can be extremely useful (such as  $X$  and  $Z$  gates in the surface code), we cannot efficiently compute this for *all* gates in a quantum circuit, or else quantum circuits would be efficiently classically simulatable! Hence why we restrict to a single basis.

### 3 Splitting Codes

We now consider the second main restriction. If a code  $C$  is simply two codes  $C_1$  and  $C_2$  run in parallel, then one of these two codes will have parameters at least as good as  $C$ . Hence, we want to discard such codes, as our motivation is performing computations on asymptotically good codes. If we are willing to sacrifice code performance for ease of addressable gates, the surface code is a great choice.

One of our main proof techniques is proving that the only way to have partial addressability for certain gates is if the code has this product structure. We say such a code “splits” (as shown in Figure 4).

**Definition 5 (Splitting).** Let  $C = \text{CSS}(A, B)$ . We say that  $A$  splits on some non-empty support  $h \subsetneq \{1, \dots, n\}$  if  $A$  can be written as  $A_1 \oplus A_2$ , where  $h$  is the support of  $A_1$ .

If  $A$  and  $B$  both split on the support  $h$ , we say that the stabilizer group  $S$  and the code  $C$  split on  $h$ .

We see that this definition is equivalent to saying that  $C = C_1 \otimes C_2$ , where  $C_1$  and  $C_2$  are both CSS codes.

*Example 2.* Let us consider the following CSS codes where we are given the parity check matrices for the  $X$  and  $Z$  stabilizers as  $A$  and  $B$ . We first show the splits in  $A$  and  $B$  using red boxes, and then show that they have common split (which splits the overarching CSS code) in green.

$$\begin{array}{c}
 A = \begin{pmatrix} \boxed{1 \ 1} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \boxed{1 \ 1} & 0 & 0 & 0 \\ 0 & 0 & \boxed{0 \ 1 \ 1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \boxed{1 \ 1} \end{pmatrix} \\
 \\
 A = \begin{pmatrix} \boxed{1 \ 1} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \boxed{1 \ 1} & 0 & 0 & 0 \\ 0 & 0 & \boxed{0 \ 1 \ 1} & 0 & 0 & 0 \\ 0 & 0 & \boxed{0 \ 0 \ 0} & 0 & 0 & \boxed{1 \ 1} \end{pmatrix} \\
 \\
 B = \begin{pmatrix} \boxed{1 \ 1} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \boxed{1 \ 1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \boxed{1 \ 1} & 0 \\ 0 & 0 & 0 & 0 & \boxed{0 \ 1 \ 1} \end{pmatrix} \\
 \\
 B = \begin{pmatrix} \boxed{1 \ 1} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \boxed{1 \ 1} & 0 & 0 & 0 \\ 0 & 0 & \boxed{0 \ 0} & \boxed{1 \ 1} & 0 & 0 \\ 0 & 0 & \boxed{0 \ 0} & \boxed{0 \ 1 \ 1} \end{pmatrix}
 \end{array}$$

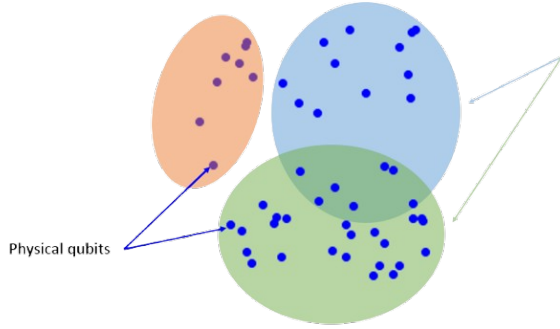


Fig. 4. Visualization of a splitting code

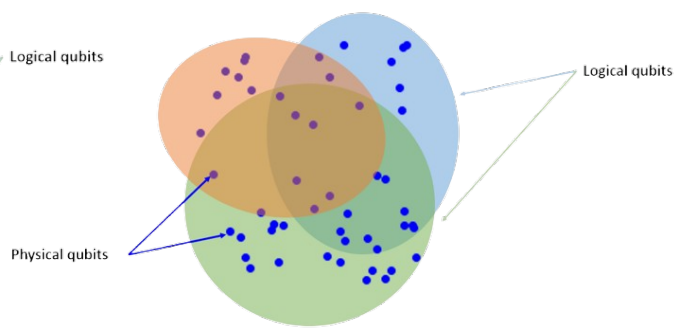


Fig. 5. Visualization of a non-splitting code

We provide the following proposition, whose proof is straightforward:

**Proposition 3.** Let  $C$  be a  $[[n, k, d]]$  CSS code splitting into an  $[[n_1, k_1, d_1]]$ -code  $C_1$  and an  $[[n_2, k_2, d_2]]$ -code  $C_2$ . Then:

- $\frac{k}{n} = \frac{k_1+k_2}{n_1+n_2} \leq \max_{i \in \{1,2\}} \frac{k_i}{n_i}$ .
- $d = \min_{i \in \{1,2\}} d_i$
- If  $U$  is addressable on  $C_1$  and  $C_2$  then  $U$  is addressable on  $C$ . If  $U$  is partially addressable on  $C_1$  or  $C_2$  then  $U$  is partially addressable on  $C$ .

These results tell us that if a code splits, the subcodes cannot have worse rates. Thus, for an asymptotically good code, it must have some non-splitting, “irreducible” core. We also know this core must encode more than 1 logical qubit, as the rates of single-logical qubit codes cannot be arbitrarily high.



## 4 Clifford Addressability

In this section we study 1-local Clifford circuits: circuits made only from single-qubit Clifford gates. We will show that for circuits with  $H$  gates, even being a logical operator at all (let alone what action it might have) implies the code splits. Hence, for good (non-splitting) CSS codes they cannot have such logical operators.

### 4.1 Tools

**Proposition 4.** *Let  $U$  be a Clifford circuit and let  $S$  be the stabilizer group of  $C$ . If  $U$  is a logical operator, then  $USU^\dagger \subseteq S$ .*

*Proof.* Using [Proposition 1](#) we get that  $U$  must send logical identities to logical identities. Since  $U$  is Clifford, it sends Paulis to Paulis. Since  $S$  corresponds to all Pauli logical identities, we get  $USU^\dagger \subseteq S$ .  $\square$

More precisely, for a CSS code  $\text{CSS}(A, B)$ , we can take any  $a \in A$  and any  $b \in B$  (including 0 for either) and we have that

$$UX^aU^\dagger = i^m X^{a'} Z^{b'} \quad (4)$$

where  $a' \in A$ ,  $b' \in B$ , and  $m$  is even.

**Proposition 5.** *Let  $U$  be a 1-local Clifford circuit. Then there is a depth 1 circuit  $V$ , with gates from the set  $C_{P,H} := \{I, P, HP, PHP, PH, H\}$ , such that  $U$  is a logical operator with logical action  $\bar{U}$  if and only if  $V$  is (up to phase) a logical operator with action  $\bar{U}$  (up to phase).*

*Proof.* By definition, on each qubit  $U$  is a product of gates in  $C_{P,H}$  with Paulis. Since the gates in  $C_{P,H}$  preserve Paulis by conjugation, we can commute all the Paulis to the right. Thus,  $U = VP$  where  $P$  is a Pauli circuit and  $V$  only contains gates from  $C_{P,H}$ .

Then since Paulis either commute or anti-commute, for any  $X^a Z^b$ , we have that

$$UX^a Z^b U^\dagger = V P X^a Z^b P^\dagger V^\dagger \quad (5)$$

$$= (-1)^m V X^a Z^b V^\dagger \quad (6)$$

for some  $m$ . This immediately gives the result: if  $a \in A$  and  $b \in B$ , then for  $U$  to be a logical operator, the left-hand-side must be  $X^{a'} Z^{b'}$  for some  $a' \in A$  and  $b' \in B$ , which tells us that  $V$  is also a logical operator (ignoring the phase).

If  $a \in N(B)$  and  $b \in N(B)$ , then the logical action of  $U$  is determined by its action on these states, but  $V$  will have the same action (up to phase).  $\square$

Thanks to [Proposition 5](#), we will assume every 1-local Clifford circuit has been compiled down to contain only  $\{I, P, HP, PH, PHP, H\}$ , followed by Paulis. Up to phase, those gates act on single-qubit Paulis as:

$$I : X \mapsto X, \quad Z \mapsto Z \quad (7)$$

$$P : X \mapsto XZ, \quad Z \mapsto Z \quad (8)$$

$$HP : X \mapsto XZ, \quad Z \mapsto X \quad (9)$$

$$PH : X \mapsto Z, \quad Z \mapsto XZ \quad (10)$$

$$PHP : X \mapsto X, \quad Z \mapsto XZ \quad (11)$$

$$H : X \mapsto Z, \quad Z \mapsto X \quad (12)$$

**Definition 6.** *Let  $U$  be a 1-local Clifford circuit. For a set  $K$  of specific single-qubit Cliffords, we define  $U_K = \{i : U_i \in K\}$ .*

*Example 3.* Let  $U = P \otimes X Z H \otimes P H \otimes H$ . Then this is equivalent by [Proposition 5](#) to  $P \otimes H \otimes P H \otimes H$ , and  $U_H = \{2, 4\}$  and  $U_{P,H} = \{1, 2, 4\}$ .

This means that for any 1-local Clifford circuit  $U$ , the equivalent  $V$  can be written as  $V = \bigotimes_{R \in C_{P,H}} R^{V_R}$ .

All of this leads to our main technical tool:

**Proposition 6.** *Let  $C = \text{CSS}(A, B)$  and  $U$  a Clifford circuit. If  $U$  is a logical operator on  $C$ , then it is equivalent to some  $V$  such that for all  $a \in A$  and all  $b \in B$ :*

$$a \cap V_{P,HP,PH,H} \in B \quad (13)$$

$$a \cap V_{PH,H} \in A \quad (14)$$

$$b \cap V_{HP,PHP,PH,H} \in A \quad (15)$$

$$b \cap V_{HP,H} \in B \quad (16)$$

*Proof.* Using  $\sim$  as equality up to phase and  $\equiv$  as equivalence up to stabilizer, we know that  $U X^a U^\dagger$  must be a stabilizer for any  $a \in A$ . Thus:

$$U X^a U^\dagger \sim V X^a V^\dagger \sim X^{a \cap V_{I,PHP,P,HP}} Z^{a \cap V_{PH,H,P,HP}} \equiv X^{a \cap V_{PH,H}} Z^{a \cap V_{P,HP,PH,H}} \quad (17)$$

where the last equivalence holds since  $x$  is a stabilizer and (since all gates in  $V$  are in  $C_{P,H}$ ) we have that  $a \cap U_{PH,H} + a \cap U_{I,PHP,P,HP} = a$ .

In a CSS code, if product  $X^{a'} Z^{b'}$  is a stabilizer, then both  $X^{a'}$  and  $Z^{b'}$  are stabilizers, so  $a' \in A$  and  $b' \in B$ . Applying this to the above gives the first two lines of the result; repeating the logic with a  $Z$  stabilizer  $Z^b$  completes the proof.  $\square$

## 4.2 Impossibility Results for Hadamard-Type Circuits

Our first result follows almost immediately from [Proposition 6](#).

**Proposition 7.** *Let  $C = \text{CSS}(A, B)$  and  $U$  a 1-local Clifford circuit. If  $U$  is a logical operator, then the code splits in  $U_{HP}$ ,  $U_{PH}$ , and  $U_H$ .*

*Proof.* If  $a \in A$ , then [Equation \(14\)](#) tells us  $a \cap U_{PH,H} \in A$ . Applying [Equation \(13\)](#) to  $a \cap U_{PH,H}$  tells us  $a \cap U_{PH,H} \in B$  as well, since  $U_{PH,H} \subseteq U_{P,HP,PH,H}$ . Then [Equation \(16\)](#) applied to  $a \cap U_{PH,H}$  tells us  $(a \cap U_{PH,H}) \cap U_{HP,H} = a \cap U_H \in B$ . Then applying [Equation \(15\)](#) to  $a \cap U_H$ , we see that  $a \cap U_H \in A$  as well. Thus,  $A$  splits on  $U_H$ .

Doing the same procedure for an arbitrary  $b \in B$  shows that  $b \cap U_H \in B$ , so  $B$  splits on  $U_H$  as well, and hence the full CSS code splits.

Similarly pushing these intersections through the statement of [Proposition 6](#) gives the other two results.  $\square$

Our results so far restrict the set of circuits that are logical operators, *regardless of their action*. We now show that no addressable logical action is possible:

**Proposition 8.** *Let  $C$  be a non-splitting CSS code, and  $U$  a 1-local Clifford partially addressable unitary. Then the physical implementation of  $U$  contains no  $H$ ,  $PH$ , or  $HP$  gates.*

*Proof.* [Proposition 7](#) tells us that we either apply  $H$  to all or none of the qubits (similarly with  $PH$  and  $HP$ ). If our circuit  $C$  for  $U$  applies  $H$  to every gate, then for any logical operator  $X^{x_i}$ ,  $C X^{x_i} C^\dagger = Z^{x_i}$ . In particular, if  $U$  is partially addressable, there must be some logical operator  $X^{x_i}$  which should be unchanged by the action of  $U$ . But  $Z^{x_i}$  cannot be equivalent by stabilizers to  $X^{x_i}$ , as  $x_i$  is not in the span of  $A$  (where the code is  $\text{CSS}(A, B)$ ).

The same reasoning holds if the circuit contains only  $PH$  or  $HP$  gates, by taking their action on either a logical  $X$  or logical  $Z$  operator.  $\square$

Thanks to [Proposition 8](#), we know that 1-local Clifford addressable gate must only use  $P$  or  $PHP$  gates. We now show that this set is too restrictive to enact any  $H$ ,  $PH$ ,  $HP$ , or CNOT gates.

**Proposition 9.** *The  $H$ ,  $PH$ ,  $HP$  and CNOT gates are not 1-local Clifford partially addressable for any non-splitting CSS code.*

*Proof.* Using [Proposition 8](#), no matter how we construct our circuit  $U$ , if it enacts some addressable logical action it must be equivalent to  $U$  made from only  $I$ ,  $P$ , and  $PHP$  gates. For any logical  $X$  operator  $X^x$ , or logical  $Z$  operator  $Z^z$ , we can see that the action of  $U$  on these will be

$$UX^xU^\dagger = X^x Z^{x \cap U_P} \quad (18)$$

$$\text{and } UZ^zU^\dagger = X^{z \cap U_{PHP}} Z^z \quad (19)$$

by the commutation rules in [Equation \(8\)](#) and [11](#).

Throughout, we will use  $X^{x_i}$  to denote a logical  $X$  operator on the  $i$ th logical qubit, and the same for  $Z^{z_i}$ .

If we want  $U$  to enact an addressable  $\overline{H}$  or  $\overline{PH}$  gate, there must be some qubit  $i$  such that  $U$  sends  $X^{x_i}$  to an operator equivalent to  $Z^{z_i}$ . Thus,  $X^x Z^{x \cap U_P}$  must be equivalent up to stabilizers to  $Z^{z_i}$ . This would imply  $X^x$  is a stabilizer, contradicting that it was a logical  $X$  operator. The same logic applied  $Z^{z_i}$  works to show that  $\overline{HP}$  cannot address a qubit  $i$ .

For  $U$  to enact an addressable  $\overline{\text{CNOT}}$  gate, it must act on some target  $i$  and control  $j$ , so that  $UX^{x_i}U^\dagger \equiv X^{x_i+x_j}$ . This would imply  $X^{x_i} Z^{x_i \cap U_P} \equiv X^{x_i+x_j}$ , but this would mean  $X^{x_j}$  is a stabilizer, not a logical operator (a contradiction). □

As a final note, we show how our non-splitting requirement implies a distance bound:

**Corollary 1.** *If an  $[[n, k, d]]$  CSS code  $C$  admits a 1-local Clifford addressable  $H$ ,  $PH$ ,  $HP$ , or CNOT gate, then its rate is at most  $\frac{1}{2d+1}$ .*

*Proof.* By [Proposition 9](#), such a code must split, and the subcodes must further split until they encode only 1 logical qubit. Let the parameters of each code be  $[[n_i, 1, d_i]]$ . The quantum singleton bound tells us that  $n_i - 1 \geq 2(d_i - 1)$ . We know  $\sum_{i=1}^k n_i = n$ , meaning  $n - k \geq 2(\sum_{i=1}^k d_i - 1) \geq 2(k \min_i \{d_i\} - 1)$ . However,  $\min_i \{d_i\} = d$  by [Proposition 3](#), so  $n - k \geq 2kd - 2$ . Rearranging gives  $\frac{k}{n} \leq \frac{1}{2d+1} - \frac{2}{k}$ . □

### 4.3 The Clifford Hierarchy

Recall the Clifford hierarchy from [Equation \(1\)](#). We say that a physical circuit is *global* if it has a non-identity action on all physical qubits, and non-global otherwise.

**Theorem 1.** *Let  $C$  be a non-splitting CSS code of distance greater than 2. Suppose there is some  $m$  such that no 1-local circuit in  $C_n^k \setminus C_n^{k-1}$  is a logical identity. Then for all  $m \geq k$ , no 1-local circuit in  $C^m \setminus C^{k-1}$  is a logical identity.*

*Proof.* We show this inductively. The base case is given by the assumptions of the theorem, so we suppose that there are no 1-local stabilizers with gates from the  $k - 1$  level of the Clifford hierarchy, for some  $k$ .

Suppose  $C$  is a non-global circuit composed of 1-local gates in the  $k$ th level of the Clifford hierarchy, such that at least one physical qubit  $i$  has a gate which is in the  $k$ th level but not the  $k - 1$  level, and such that  $C$  preserves the codespace. That is,

$$C = C_1 \otimes C_2 \otimes \cdots \otimes C_n$$

where each  $C_n$  is a single-qubit gate in  $C_1^k$ , and  $C_i \notin C_1^{k-1}$ .

Because  $C_i \notin C_1^{k-1}$ , there is a Pauli matrix  $V$  (either  $X$ ,  $Z$ , or  $XZ$ ) such that  $C_i V = A_i C_i$  for  $A_i \in C_1^{k-1} \setminus C_1^{k-2}$ . Because the code has distance greater than 1 and does not split, for every physical qubit there is both an  $X$  and  $Z$  stabilizer with support on that qubit, and thus there is some Pauli stabilizer  $S$  whose support on  $i$  is the Pauli matrix  $V$  defined above.

Since  $C$  is in the  $k$ th level, there is a operator  $A$  such that  $CX^a = AC$ , where  $A$ . By choice of  $C$ , we know that the action of  $A$  on the  $i$ th qubit,  $A_i$ , is not in the  $k-2$  level of the Clifford hierarchy, so  $A \in C_n^{k-1} \setminus C_n^{k-2}$  as well.

Then we have that for any state  $|\psi\rangle$  in the code,  $CX^a |\psi\rangle = |\psi'\rangle$  is still in the code, so:

$$\begin{aligned} |\psi'\rangle &= CS |\psi\rangle \\ &= AC |\psi\rangle \\ &= A |\psi'\rangle \end{aligned}$$

Thus,  $A$  is a logical identity of the code. This contradicts the inductive hypothesis since  $A$  is a 1-local circuit in the  $k-1$  level of the Clifford hierarchy.

Thus, the assumption that  $C$  exists must be false. □

**Corollary 2.** *If a CSS code  $C = \text{CSS}(A, B)$ :*

- *is non-splitting;*
- *has distance at least 2;*
- *is not self-dual (i.e.,  $A \neq B$ );*
- *admits no logical operator from  $P$  or  $PHP$  gates;*

*then  $C$  does not admit any circuit from single-qubit gates in any higher level of the Clifford hierarchy.*

*Proof.* From [Proposition 8](#), we know that there are no non-global circuits with  $H$ ,  $HP$ , or  $PH$  gates that preserve the code. If such a circuit is global, it can only preserve the code if  $A = B$ , using the rules in [Proposition 6](#). Thus  $H$ ,  $HP$ , and  $PH$  cannot form logical identities on  $C$ .

If the code does not admit any logical operators from  $P$  or  $PHP$  gates, it admits no gates in  $C_n^2$  except those already in  $C_n^1$  (the Paulis). Using [Theorem 1](#), this means it can admit no physical gate from any higher level of the Clifford hierarchy, as such a gate would need to preserve the codespace. □

In short, either the code admits logical operators from phase (or  $PHP$ ) gates, or it admits nothing else from the (1-local) Clifford hierarchy.

In turn, we might wonder whether similar techniques from our  $H$  impossibility results could apply to just  $P$ . However, this is not true: the same commutation rules from [Equation \(8\)](#) tell us that if a code  $\text{CSS}(A, B)$  admits a logical operator formed by single-qubit  $P$  circuit on a set of physical qubits  $p$ , then we can conclude that  $a \cap p \in B$  for all  $a \in A$ . This is significantly less restrictive than the requirements for  $H$ , and indeed codes with transversal  $T$  gates admit partially addressable  $P$  gates.

## 5 Permutation Isomorphisms and Addressability

Because of our restrictions that addressable gates should be logical operators, i.e., preserve the codespace, we are effectively studying automorphisms of the code. Here we consider this more directly, but consider isomorphisms between codes, and consider only isomorphisms formed by permutations of qubits. Such isomorphisms (in particular automorphisms) were proposed as a method to perform logical operations as early as 2013 [\[3\]](#), and recently detailed for certain quantum LDPC codes [\[7\]](#). We show that there are actually not that many isomorphisms like this, which rules out certain kinds of circuits for high-rate codes.

Throughout this section we will implicitly work with *qudit* CSS codes except where otherwise mentioned.

## 5.1 Counting Permutations

**Definition 7.** Let  $C_1, C_2$  be classical codes with parity checks  $H_1$  and  $H_2$  respectively, we say that  $\tau_n \in S_n$  is a permutation isomorphism from  $C_1$  to  $C_2$  iff there exists  $U \in GL_r(\mathbb{F}_q)$  such that  $UH_1 = H_2P$  where  $P$  is the permutation matrix of  $\tau_n$ .

If  $C_1 = C_2$ , we say  $\tau_n$  is a permutation automorphism.

*Remark 1.* We can define it equivalently with the generator matrix, since if  $P$  preserve the codespace, it equivalently preserves its orthogonality.

*Proof.* Suppose  $UG_1 = G_2P$ . For any  $x \in C_2^\perp$  and  $y \in C_1$ ,  $\langle y, xP \rangle = \langle Uy', xP \rangle$  for some  $y' \in C_1$ , since  $U$  is invertible. But this means  $Uy' = y''P$  for some  $y'' \in C_2$ , so the inner product is equal to  $\langle y''P, xP \rangle = \langle y'', x \rangle = 0$ . Thus,  $xP \in C_1^\perp$  for any  $x \in C_2^\perp$ ; by dimensionality arguments, this tells us  $UH_1 = H_2P$ .  $\square$

**Definition 8.**  $\tau_n \in S_n$  is a permutation isomorphism from  $\text{CSS}(C_{11}, C_{12})$  to  $\text{CSS}(C_{21}, C_{22})$  iff it is a permutation isomorphism from  $C_{11}$  to  $C_{21}$  and from  $C_{12}$  to  $C_{22}$ .

In this case, for  $i \in \{1, 2\}$  we can form a matrix  $H_i = \begin{pmatrix} H_{i1}^T & H_{i2}^T \end{pmatrix}^T$  where  $H_{i1}, H_{i2}$  are the respective parity checks of  $C_{i1}, C_{i2}$ . Then we get that

$$UH_1 = H_2P \text{ with } U = \begin{pmatrix} U_1 & 0 \\ 0 & U_2 \end{pmatrix}. \quad (20)$$

*Example 4.* For an automorphism, take  $H_1 = \begin{pmatrix} 1 & 1 & 0 \end{pmatrix}$  and  $H_2 = \begin{pmatrix} 0 & 1 & 1 \end{pmatrix}$ , we get  $H = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$ .

$$\text{We can see that } \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

This means that the permutation of qubits represented by the permutation matrix on the right preserves the stabilizer group, meaning that it is a valid permutation automorphism for the classical code represented by  $H$  but it is not a valid permutation automorphism for  $\text{CSS}(C_1, C_2)$  as it is not an automorphism on  $C_1, C_2$ .

*Remark 2.* The matrix  $H = \begin{pmatrix} H_1^T & H_2^T \end{pmatrix}^T$ , corresponds to the parity check matrix of the CSS code where we forget if a check is of type  $X$  or  $Z$ .

Intuitively, this means that a permutation isomorphism can permute the columns of  $G$  from the first code in such a way that it maps to the second codespace. However this puts strong conditions on the form of the invertible matrix  $U$ . From those conditions we can extract an upper bound on the number of different such matrices  $U$ , and thus an upper bound of the number of permutation automorphisms.

**Proposition 10.** The number of pairs  $U, P$  of invertible matrix and permutation such that  $UH_2 = H_1P$  only depends on the vector spaces  $\text{span}(H_1)$  and  $\text{span}(H_2)$ . Moreover, the number of such pairs is constant under permutations of the columns of  $H_2$  or  $H_1$ .

*Proof.* Let  $\bar{H}_1$  be another basis of the first vector space and  $\bar{H}_2$  another basis of the second. This means that there exists  $W_1$  and  $W_2$  such that  $\bar{H}_1 = W_1 H_1$  and  $\bar{H}_2 = W_2 H_2$ . Let  $P'_1$  and  $P'_2$  be arbitrary permutations.

Let  $U, P$  be an invertible matrix and a permutation such that  $U H_2 = H_1 P$ , or  $U H_2 P^{-1} = H_1$ . Then  $(W_1 U W_2^{-1}) \bar{H}_2 P'_2 (P_2'^{-1} P^{-1} P'_1) = W_1 H_1 P'_1 = \bar{H}_1 P'_1$ . Since  $W U W^{-1}$  is invertible and  $P_2'^{-1} P^{-1} P'_1$  is a permutation, this is a valid pair for  $\bar{H}_2 P'_2$  and  $\bar{H}_1 P'_1$ . Thus, there are as many pairs for  $(H_1, H_2)$  as for  $(\bar{H}_1 P'_1, \bar{H}_2 P'_2)$ .  $\square$

Here we make a distinction between counting distinct pairs  $(U, P)$ , counting distinct permutations  $P$  that belong to such a pair, and counting distinct  $U$  that belong to such a pair.

**Lemma 2.** *Let  $m$  be the number of distinct pairs  $(U, P)$  of an invertible matrix  $U$  and a permutation  $P$  such that  $U H_2 = H_1 P$ , and let  $m_u$  be the number of distinct  $U$  from such a pair and  $m_p$  the number of distinct  $P$ . Then for a fixed  $U$ , if it is part of pair  $(U, P_1)$  then  $(U, P_2)$  is also a valid pair if and only if  $P_2$  is in the same right coset as  $P_1$  of the subgroup of permutations  $\text{Sym}(H_1) := \{P \in \text{Sym}(n) : H_1 P = H_1\}$ . Consequently,  $m_p = m = m_u |\text{Sym}(H_1)|$ .*

*Proof.* To prove  $m_p = m$ , we prove that each  $P$  has exactly one  $U$  that forms such a pair. If there were more than one, then  $U_1 H_2 = H_1 P = U_2 H_2$ , meaning  $U_2 U_1^{-1} H_2 = H_2$ . Since  $H_2$  is full-rank, this implies  $U_2 U_1^{-1} = I$ .

For the second, if  $(U, P_1)$  and  $(U, P_2)$  are valid pairs, then  $U H_2 = H_1 P_1 = H_1 P_2$ . This implies  $H_1 P_1 P_2^{-1} = H_1$ . Immediately this implies  $P_1 P_2^{-1} \in \text{Sym}(H_1)$ . Conversely, if any  $P$  is in  $\text{Sym}(H_1) P_1$ , then  $P = P' P_1$  where  $P' \in \text{Sym}(H_1)$ . Then  $H_1 P = H_1 P' P_1 = H_1 P_1$ , so  $U H_2 = H_1 P$  as well.  $\square$

The size of this group of permutations that fix  $H_1$  can be easily found, since they are simply products of permutations of columns of  $H_1$  which are exactly the same.

Clearly the number of valid permutations  $P$  tells us the number of qudit permutations which preserve the code. However, we will actually care more about the number of invertible matrices  $U$ , which is smaller. We need a small lemma to prove that we can quotient out by  $\text{Sym}(H_1)$  in this way:

**Lemma 3.** *Let  $C = \text{CSS}(A, B)$ , with  $H_A$  a parity check matrix for  $A$ . Then if two columns of  $H_A$  are identical, either  $C$  has distance at most 2 or swapping these two qubits acts as a logical identity.*

*Proof.* Suppose WLOG the first two columns are the same. Then the vector  $v := (1, -1, 0, \dots, 0) \in A^\perp$ , so  $Z^v$  is either a logical  $Z$  operator or a  $Z$  stabilizer. If  $Z^v$  is a logical operator, the code has distance at most 2.

If  $Z^v$  is a stabilizer, then every  $x \in B^\perp \subseteq \mathbb{F}_q^n$  must have  $x_1 = x_2$  to be orthogonal to  $v$ . However, all logical  $X$  operators must be of the form  $X^x$  for some  $x \in B^\perp$ , so  $x_1 = x_2$  for all  $X$  stabilizers and logical operators. Thus, swapping these two qubits acts as the identity on  $X$  operators.

For  $Z$  operators, take any  $b = (b_1, b_2, \dots, b_n) \in A^\perp$  (either a  $Z$  stabilizer or logical operator). If  $b_1 = b_2$  it is also invariant under swapping qubits 1 and 2, and if  $b_1 \neq b_2$ , then swapping the first two qubits will produce the operator:

$$(b_2, b_1, b_3, \dots, b_n) = b + (b_2 - b_1, b_1 - b_2, 0, \dots, 0) \quad (21)$$

However, the second vector is clearly a multiple of  $v = (1, -1, 0, \dots, 0)$ , and we know that  $Z^v$  is a  $Z$ -stabilizer. Thus, the operator  $Z^b$  is equivalent up to multiplication by a stabilizer to itself after the swap, so it must be the same logical operator.

Both arguments also show that the  $X$  and  $Z$  stabilizers are also invariant when  $Z^v$  is a  $Z$ -stabilizer.  $\square$

**Corollary 3.** *Let  $C = \text{CSS}(A, B)$  have distance at least 3. Then any permutation automorphism  $\tau$  such that  $H_A P_\tau = H_A$  acts as a logical identity.*

*Proof.* We can see that  $H_A P_\tau = H_A$  only if it permutes only columns of  $H_A$  which are identical. Thus, it can be constructed as a product of transpositions on such columns. From **Lemma 3**, each transposition is a logical identity, so their product is as well.  $\square$

Thus, to count logical operations, we care only about the number of invertible matrices  $U$  such that  $UH_2 = H_1P$ , not the number of pairs or permutations.

**Proposition 11.** *Calling  $m_u$  the number of invertible matrices  $U$  such that there exists a permutation  $P$  such that  $UH_2 = H_1P$ , and  $p$  the number of pairs of permutations such that  $P'H'_2 = H'_1P''$  we have  $p \leq m \leq \frac{n!}{(n-r)!}$ , where  $H'_1$  and  $H'_2$  are the right block in the row reduced forms of  $H_1$  and  $H_2$ .*

*Proof.* Since  $H_2$  has  $r$  independent rows, we can reduce it such that it has the form  $\bar{H}_2 = \left( I_r \middle| H'_2 \right) = WH_2P'$  where  $W \in GL_r(\mathbb{F}_q)$  and  $P'$  a permutation matrix of dimension  $n$ .

Using [Proposition 10](#) we get that there are as many pairs for  $H_2$  and for  $\bar{H}_2$ .

Let  $U$  be an invertible matrix of rank  $r$ , we get that  $U\bar{H}_2 = \left( U \middle| UH'_2 \right) = H_1P$ . Thus, for  $U$  to be part of a valid pair, it has to be made of  $r$  independent columns of  $H_1$ . And there are less than  $\frac{n!}{(n-r)!}$  ways to pick such set of columns.

For the lower bound, we can check that we can extend any valid permutation on  $H'_1, H'_2$  into a valid permutation on  $\bar{H}_1$ . Let  $P', P''$  be permutation matrix of dimension respectively  $r, n-r$ .

$$P'\bar{H}_2 = \left( P' \middle| P'H'_2 \right) = \left( P' \middle| H'_1P'' \right) = \left( I_r \middle| H'_1 \right) \begin{pmatrix} P' & 0 \\ 0 & P'' \end{pmatrix} = \bar{H}_1 \begin{pmatrix} P' & 0 \\ 0 & P'' \end{pmatrix}$$

Hence, any pair of permutations on  $H'_1, H'_2$  can be extended into a valid one on  $\bar{H}_1, \bar{H}_2$ .  $\square$

*Remark 3.* Furthermore, since we want  $U\bar{H}_2 = \bar{H}_1P$  with  $P$  a permutation of the columns, then we also need  $U\bar{H}_2$  to generate  $I_r$ , meaning that the columns of  $U^{-1}$  should also be in  $\bar{H}_2$ . This is a stricter restriction and could reduce the upper bound significantly depending on the code. We can use this observation to create an algorithm to find all matrices  $U$  having  $UB = BP$  without going over all permutations. This will be slightly better but still very inefficient.

Finally, we summarize as a theorem:

**Theorem 2.** *Let  $C = \text{CSS}(A, B)$  be an  $[[n, k, d]]$  code with  $d \geq 3$ . The number of distinct logical operations that can be implemented by permuted qubits in the code is upper-bounded by  $\frac{n!}{k_{\max}!}$ , where  $k_{\max} = \max\{\dim(A), \dim(B)\}$ .*

*Proof.* From [Corollary 3](#), if two permutations  $P_1$  and  $P_2$  are such that  $H_AP_1 = H_AP_2$ , they must produce the same logical action: this identity tells us  $P_1 = PP_2$  where  $H_A = H_AP$ , and  $P$  acts as a logical identity.

Then [Lemma 2](#) tells us that the number of permutation automorphisms on the code, quotiented out by this subgroup, is precisely the number of invertible matrices  $U$  where there is some permutation such that  $UH_A = H_AP$ .

Then from [Proposition 11](#), the number of such invertible matrices is at most  $\frac{n!}{(n-\dim(H_A))!}$ . Since  $H_A$  is the parity check matrix, the dimension of the code  $A$  is  $k_A = n - \dim(H_A)$ . Thus, there are at most  $\frac{n!}{k_A!}$  distinct logical operations.

The same logic must apply to  $B$ , so our upper bound is

$$\min \left\{ \frac{n!}{k_A!}, \frac{n!}{k_B!} \right\} = \frac{n!}{k_{\max}!} \quad (22)$$

$\square$

[Theorem 2](#) gives a bound in terms of the rates of the underlying *classical* codes. Transforming this into a bound with a rate on the quantum code takes some care, using [Proposition 2](#).

## 5.2 Operators Constructed From SWAPs

We are now going to use the upper bound on the number of automorphisms on classical codes, to describe families of CSS codes on which certain gates are not SWAP addressable. The idea is that if we have more possible logical gates (e.g. SWAPs) than automorphisms, then SWAP cannot be SWAP addressable.

To prove this, we first need some lemmas on the asymptotic behavior of the bounds we will use:

**Lemma 4.** For all sequences  $(\rho_n)$  and  $(\rho'_n)$  such that  $\rho_n + \rho'_n > 1$ ,

$$\exists n_0 \in \mathbb{N} \text{ such that } \forall n \geq n_0, \frac{n!}{(\rho'_n n)!} < (\rho_n n)!$$

*Proof.* Since we are in the positive part of the logarithm, and it is an increasing function, it will be equivalent to prove that  $\sum_{\rho'_n n \leq i \leq n} \log(i) < \sum_{2 \leq j \leq \rho_n n} \log(j)$ .

Again because the logarithm is increasing, we can make integral inequalities:

$$\begin{aligned} \sum_{\rho'_n n \leq i \leq n} \log(i) &\leq \int_{\rho'_n n}^{n+1} \log(x) dx \\ \sum_{2 \leq i \leq \rho_n n} \log(i) &\geq \int_1^{\rho_n n-1} \log(x) dx \end{aligned}$$

Now we use  $\int_{\rho'_n n}^{n+1} \log(x) dx = g(n+1) - g(\rho'_n n)$  and  $\int_1^{\rho_n n-1} \log(x) dx = g(\rho_n n-1) - g(1)$ , where  $g(x) = x \log(x) - x$ . Hence, if  $g(n+1) - g(\rho'_n n) < g(\rho_n n-1) - g(1)$  then the inequality holds. We can do some algebra to see that this holds when the following expression is negative:

$$g(n+1) - g(\rho'_n n) - g(\rho_n n-1) + g(1) = (1 - \rho'_n - \rho_n)n \log(n) + \mathcal{O}(n)$$

Since we assumed  $\rho'_n + \rho_n > 1$ , it gives that there exists an  $n_0$  for which  $\forall n \geq n_0, \frac{n!}{(\rho'_n n)!} < (\rho_n n)!$  □

**Corollary 4.** For all sequence  $(\rho_n)$  and  $(\rho'_n)$  such that  $\frac{1}{2}\rho_n + \rho'_n > 1$ ,

$$\exists n_0 \in \mathbb{N} \text{ such that } \forall n \geq n_0, \frac{n!}{(\rho'_n n)!} < (\rho_n n)!!$$

*Proof.* The double factorial can instead be written as  $\sum_{2 < j < \frac{1}{2}\rho_n n} \log(2j+1)$ , and thus lower-bounded by

$$\int_1^{\frac{1}{2}\rho_n n-1} \log(2x+1) dx = \frac{1}{2} (g(\rho_n n-1) - g(3)).$$

and the final asymptotic expression is  $(1 - \rho'_n - \frac{1}{2}\rho_n)n \log(n) + \mathcal{O}(n)$ , giving the result. □

**Lemma 5.** For any integer  $q > 1$  and all sequences  $(\rho_n), (\rho'_n)$  such that  $\rho_n, \rho'_n > 0$  and  $\rho_n > \sqrt{\frac{\log n}{n \log q}} + \Omega\left(\frac{1}{\sqrt{n}}\right)$ ,

$$\exists n_0 \in \mathbb{N} \text{ such that } \forall n \geq n_0, \frac{n!}{(\rho'_n n)!} < q^{(\rho_n n)^2-1}$$

In particular,  $\frac{n!}{(\rho'_n n)!} < |GL_{\rho_n n}(q)|$ .



*Proof.* We apply precisely the same reasoning, and obtain that the result holds when the following expression is negative:

$$g(n+1) - g(\rho'_n n) - \log(q)(\rho_n n)^2 + 1 \quad (23)$$

which works out to

$$(n+1)\log(n+1) - n - 1 - (\rho'_n n)\log(\rho'_n n) - \log(q)\rho_n^2 n^2 + 1 \quad (24)$$

$$= (1 - \rho'_n)\frac{\log n}{n} - \log(q)\rho_n^2 n^2 O\left(\frac{\log n}{n^2}\right). \quad (25)$$

The lower bound on  $\rho_n$  shows that this will be negative.

To show that this relates to  $\text{GL}_{\rho_n n}(q)$ , we note that

$$|\text{GL}_k(q)| = \prod_{i=0}^{k-1} (2^k - 2^i) \quad (26)$$

which can be lower-bounded by  $q^{k^2-1}$ . □

**Theorem 3.** Let  $C_n = \text{CSS}(C_n^1, C_n^2)$  such that calling  $\rho_n$  the rate of  $C_n$  and  $\rho'_n$  the maximum dimension of the classical codes  $C_n^1, C_n^2$  we have  $\rho_n + \rho'_n > 1$  for all  $n > n_1$ . Then SWAP is not SWAP addressable on this family of codes.

*Proof.* By **Theorem 2**, the maximum number of distinct logical operations formed by permutations is at most  $\frac{n!}{(\rho'_n n)!}$ .

Since by assumption  $\rho_n + \rho'_n > 1$ , we can use **Lemma 4** and conclude there exists some  $n_0$  such that for all  $n \geq n_0$ ,  $\frac{n!}{(\rho'_n n)!} < (\rho_n n)! = k!$ .

If the addressable SWAPs existed, we could compose them to obtain all  $k!$  logical permutation gates from physical permutations; however, the inequality shows that there are not enough allowed physical permutation circuits to produce this many logical operators. □

*Remark 4.* We can swap two qubits by using 3 CNOTs between them:

$$\text{SWAP}_{i,j} = \text{CNOT}_{i,j} \text{CNOT}_{j,i} \text{CNOT}_{i,j}. \quad (27)$$

This means that if we had all logical CNOTs then we could generate all logical SWAPs. Thus CNOT is not SWAP-addressable on those codes either.

**Corollary 5.** The following gates are not permutation addressable on CSS codes with the following rates:

- SWAP gates for codes with an asymptotical rate greater than  $\frac{1}{3}$ ;
- Any 2-qubit gate for codes with with an asymptotical rate greater than  $\frac{3}{4}$ ;
- CNOTs gates for codes with an asymptotical rate in  $\Omega\left(\sqrt{\frac{\log n}{n}}\right)$ .

*Proof.* Let  $(C_n)_{n \in \mathbb{N}}$  be a family of CSS codes and  $n_0 \in \mathbb{N}$  such that  $\forall n > n_0, \rho_n > \frac{1}{3}$ . Let us now fix  $n > n_0$ , and call  $C_n^1, C_n^2$  the classical codes making  $C_n$ , and  $\rho'_n, \rho''_n$  the maximum and minimum of their rates. We get that  $\rho_n = \rho'_n + \rho''_n - 1$  by **Proposition 2**. Thus  $\rho_n \leq 2\rho'_n - 1$  which means that  $\rho'_n \geq \frac{\rho_n + 1}{2}$ . Hence  $\rho_n + \rho'_n \geq \frac{\rho_n + 1}{2} + \rho_n > \frac{4}{6} + \frac{1}{3} > 1$ . Thus, for all  $n > n_0$ ,  $\rho_n + \rho'_n > 1$ , and we can now use **Theorem 3**.

For arbitrary 2-qubit gates, if a 2-qubit gate is permutation addressable it is parallel addressable since permutations are closed under composition. Thus, the number of such logical gates is at least the number of choices of disjoint pairs of qubits, and there are at least  $\min\{k!!, k(k-1)!!\}$  such pairs<sup>2</sup>. Applying the

<sup>2</sup> This is the double factorial:  $k!! = k(k-2)(k-4) \dots$

logic above with  $\rho_n > \frac{3}{4}$ , we see that  $\frac{1}{2}\rho_n + \rho'_n > 1$ , and by [Corollary 4](#) this is greater than the number of permutation automorphisms on the code.

For CNOT gates, CNOTs generate all invertible linear matrices on the computational basis. By [Lemma 5](#), the size of invertible linear matrices on  $k = \rho n$  logical qubits is asymptotically greater than  $\frac{n!}{(\rho'n)!}$  when  $\rho_n > \sqrt{\frac{\log n}{n}} + \Omega\left(\frac{1}{\sqrt{n}}\right)$ . □

These results illustrate an example of a trade-off between the performance of a code (its parameters) and how easy it might be to implement some logical operations on it. In [\[8\]\[5\]](#) they prove methods to construct families of good quantum codes for any rate  $0 < \rho < 1$ ; however, using [Theorem 3](#) we know that using only physical swaps, none of these families can implement addressable CNOTs, and starting from  $\rho > \frac{1}{3}$  they cannot implement addressable logical swaps.

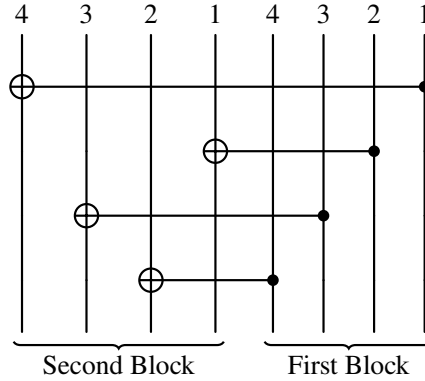
In [\[7\]](#) they construct various addressable Clifford gates, including CNOTs, from permutation automorphisms. The rate of their code family is  $\Theta\left(\frac{\log^2 n}{n}\right)$ , and [Corollary 5](#) shows that they are only a quadratic factor away from our upper bound on the best possible rate with this technique.

### 5.3 CNOT and CZ Results

Our techniques in the last section relied on counting automorphisms. We proved a more general statement about isomorphisms between codes so that we can consider addressable gates between two codes. We will consider two codes where we use physical CNOT or CZ gates, with the controls in one code and the targets in the second. We call a circuit *global* if precisely one gate acts on every physical qubit. This condition captures the addressable CCZ gates in [\[4\]](#).

Thanks to this condition, the physical gates define a permutation  $\pi \in S_n$ , where if  $i$  is the control of a CNOT in the first code,  $\pi(i)$  is the target of that CNOT in the second code (defined similarly for CZ). This representation using permutations makes it possible to link the results on isomorphisms to CNOTs and CZs. We will write such a circuit as CNOT( $\pi$ ) or CZ( $\pi$ ).

*Example 5.* Consider the following unitary :



where control and targets are from two different blocks of the same type of code made of 4 physical qubits. The permutation  $\pi$  would here be  $\pi = (142)(3)$ .

A critical component of the previous section was counting automorphisms *up to distinct logical actions*. We prove an analogous result here. For a general gate  $U$ , we use  $CU(\pi)$  to denote a global controlled- $U$  circuit, where every qubit  $i$  in one code is a control, whose target qubit is  $\pi(i)$  in a second code.

**Lemma 6.** *Let  $U$  be a single-qubit gate, and consider a global controlled- $U$  circuit with all controls in  $C_1 = \text{CSS}(A_1, B_1)$  and all targets in  $C_2 = \text{CSS}(A_2, B_2)$ , and let  $\pi$  be the permutation induced by mapping control to target. If  $\pi_1 \in \text{Sym}(H_{A_1}) \cup \text{Sym}(H_{B_1})$  and  $\pi_2 \in \text{Sym}(H_{A_2}) \cup \text{Sym}(H_{B_2})$ , then  $CU(\pi_2 \circ \pi \circ \pi_1)$  has the same logical action as  $CU(\pi)$  if both  $C_1$  and  $C_2$  have distance at least 3.*

*Proof.* We can see that  $CU(\pi_2 \circ \pi \circ \pi_1)$  is equivalent to the physical circuit obtained by permuting  $C_1$  by  $\pi_1^{-1}$ , permuting  $C_2$  by  $\pi_2^{-1}$ , applying  $CU(\pi)$ , then permuting  $C_1$  and  $C_2$  back by  $\pi_1$  and  $\pi_2$  respectively.

Using [Corollary 3](#), these physical permutations are logical identities, thus the logical action is the same as  $CU(\pi)$  itself.  $\square$

**Proposition 12.** *CNOT is not depth-one global CNOT parallel addressable on any two CSS codes with the same parameters, and asymptotical rates greater than  $\frac{1}{3}$ .*

*Proof.* Let the two codes be  $CSS(A_1, B_1)$  and  $CSS(A_2, B_2)$ .

By studying the actions on stabilizers, we have that  $CNOT_{I,J}$  between two blocks of the code being valid implies that

$$\begin{aligned} \forall a \in A_1, \pi(a \cap I) &\in A_2 \\ \forall b \in B_2, \pi^{-1}(b \cap J) &\in B_1 \end{aligned}$$

where  $I$  is the set of control on the first block of the code, and  $J$  the set of target on the second.  $\pi$  is the bijective function going from control to target, and these equations show that it acts as an isomorphism from  $A_1$  to  $A_2$ . Also  $\pi^{-1}$  as an isomorphism from  $B_2$  to  $B_1$ , so  $\pi$  is an isomorphism from  $B_1$  to  $B_2$ . Thus, each valid depth-one, global CNOT circuit corresponds to a valid isomorphism from the first code to the second, so our isomorphism upper bounds also apply to the number of such CNOT circuits.

Moreover, [Lemma 6](#) tells us that these circuits have distinct actions only if the permutations are in distinct cosets of  $\text{Sym}(H_{A_2})$ , and the number of such distinct actions is bounded by  $\frac{n!}{k_{max}!}$  by [Theorem 2](#).

If we want these circuits to implement all parallel addressable logical CNOTs between the two codes, there must be  $k!$  such gates.

The same counting arguments for the SWAP thus tell us that, asymptotically, there are not enough automorphisms to construct all such gates.  $\square$

**Proposition 13.** *CZ is not depth-one global CZ parallel addressable on any two CSS codes with the same parameters, and asymptotical rates greater than  $\frac{1}{3}$ .*

*Proof.* The proof will proceed almost identically to [Proposition 12](#). We first note that the required stabilizer relations are

$$\forall a \in A_1, \pi(a) \in B_2 \tag{28}$$

$$\forall a \in A_2, \pi^{-1}(a) \in B_1 \tag{29}$$

(with the intersection with  $I$  and  $J$  not shown because the circuit is global).

This tells us that  $\pi(A_1) \subseteq B_2$  and  $\pi(B_1) \subseteq A_2$ . Since the codes have the same parameters, we know that  $n - k = \dim(A_1) + \dim(B_1) = \dim(A_2) + \dim(B_2)$  (where  $k$  is the number of logical qubits). Thus,  $\pi(A_1) = B_2$  and  $\pi(B_1) = A_2$ , giving us an isomorphism  $\pi$  from  $A_1$  to  $B_2$  and  $B_1$  to  $A_2$ . Since [Proposition 11](#) does not care about the role of the codes, the counting arguments still apply, and still give the required upper bound.  $\square$

*Remark 5.* The stabilizers relations stays valid in the context of qudits, which makes us able to apply this result to the case of [\[4\]](#). To see this, in the context of qudits, the commutation rule of  $CZ_d$  gives :

$$CZ_d(X_d \otimes I) = (X_d \otimes Z_d)CZ_d$$

$$CZ_d(I \otimes X_d) = (Z_d \otimes X_d)CZ_d$$

$$CZ_d(Z_d \otimes I) = (Z_d \otimes I)CZ_d.$$

$$CZ_d(I \otimes Z_d) = (I \otimes Z_d)CZ_d.$$

Thus let  $a \in A$  be a vector with coefficient in  $\mathbb{F}_q$  representing a  $X$  stabilizer for a CSS qudit code. Then a global depth-1 circuit of  $CZ$  sends it to a stabilizer iff  $\pi(a) \in B$ . The only difference here being that we use coefficient in  $\mathbb{F}_q$ , but the relation stays the same.

**Proposition 13** relates to Open Question 1 from [4]: are there asymptotically good codes admitting transversal, addressable CCZ gates? The constructions they give for addressable CCZ gates are global, depth-one, and readily “downgrade” to addressable CZ gates. Thus, our results imply their techniques will not produce parallel addressable CCZ gates on an asymptotically good code with rates greater than  $\frac{1}{3}$ , unless one can (a) produce parallel addressable CCZ without simultaneously allowing parallel addressable CZ; or (b) produce non-global parallel addressable CCZ; or (c) use gates other than physical CZ or CCZ. Furthermore, using growing fields, [4] provides codes with non-zero relative distance and rate that allow addressable CCZ using global circuits. In this case, they show that they can make both rate and relative distance at least  $\frac{1}{6}$ , but by reducing the relative distance, they can boost the rate make it arbitrarily close to  $\frac{1}{3}$ . While their maximal rate matches our bound, it is important to note that we prove impossibility of parallel addressability, while they show the existence of addressability. Hence, it could be that they can achieve a better rate than  $\frac{1}{3}$ , but they would not be able to convert this method to parallel addressability.

Together, the results from **Sections 5.2** and **5.3** suggests a concerning inability to create entanglement between the qubits in high-rate quantum code. We cannot apply CNOTs between arbitrary pairs of qubits in the high-rate code with permutations, and many families of CNOTs (say, all CNOTs from qubit  $i$  to  $i + 1$ ) will generate all CNOTs, and thus are also impossible.

We might instead hope to use CNOTs to copy some data to another good quantum code, entangle the results there, and copy them back. However, **Proposition 12** tells us that an addressable CNOT between two good codes would only be able to send a given logical qubit in the first code to a small subset of logical qubits in the second code, and since the same no-go result would apply to the second, we would not be able to permute or entangle them before trying to copy them back.

To escape these results, we note two critical assumptions: first, that *both* codes has asymptotic rate at least  $\frac{1}{3}$ , and second, that the CNOTs are implemented by a permutation of the physical qubits. To escape the first, we might imagine copying to a less efficient code like the surface code. Such an architecture resembles caching, where quantum data is stored in the asymptotically good code, where computations are difficult, then copied into the surface code for computation.

For the second restriction, one might imagine implementing logical CNOTs with physical CNOTs. However, notice that if the physical CNOTs also compose to physical swaps, then we run afoul of the same permutation counting arguments. This does not mean a CNOT cannot be implemented: our results do not forbid some CNOTs together with single-qubit Clifford gates to enact a logical CNOT.

## 6 Algorithms for finding splits in CSS codes

We mentioned before that if a code splits then its distance is the minimum of the codes making it. Hence when we are trying to build the best code possible, we do not want them to split. In particular, the quantum Tanner code construction takes some code  $C_A, C_B$  at random and shows that with some probability, it will give an asymptotically good code.

Given a code, it is hard to compute its distance: it is equivalent to the problem of finding the smallest non-empty subset of dependent columns in the parity check matrix, and this is NP-hard. We thus expect that the splitting of the code gives a nice heuristic: if a code splits then most likely it will not have a good distance. Conversely, we hope that codes built this way with bad distance will split with good probability. This would give a better way to sample good quantum Tanner codes.

In the following, we present two algorithm that detect if a code splits. The second approach detects and returns the splits in quadratic time (linear time for LDPC codes) in the number of qubits.

### 6.1 System solving approach

There is another equivalent way of defining splitting codes that we did not talk about the in splitting section.

**Proposition 14.**  $C = \text{CSS}(A, B)$  is a splitting code if there exists a diagonal matrix  $D$  with coefficients not all equal such that for all  $a \in A$  and  $b \in B$ ,  $aD \in A$  and  $bD \in B$ .

*Proof.* Starting by the easy direction, assuming that  $C$  splits on some support  $h$ , then both  $A, B$  split on  $h$ . Let us take  $D$  defined as  $D_{i,i} = 1$  if  $i \in h$  and 0 otherwise, since  $C$  splits we have that the coefficients of  $D$  are not all equal. Multiplication by  $D$  is just a projection onto  $h$ , so  $aD \in A$  and  $bD \in B$  for all  $a \in A$  and  $b \in B$ , as required.

In the other direction, let us first show that for any polynomial with integer coefficients  $P$ , we have  $aP(D) \in A$  and  $bP(D) \in B$  for any  $a, b \in A \times B$ . By assumption we have  $aD \in A$ , hence applying this rule again gives that for all  $s \in \mathbb{N}$ ,  $aD^s \in A$ . Finally, since  $A$  is linear, we get that for all polynomials  $P$  with integer coefficients,  $aP(D) \in A$ . The same reasoning applies to  $B$ .

Now, we also know that the coefficients of  $D$  are not all equal, hence there exists two non-empty complementary sets  $U, V$  of indices such that the values of  $D$  at indices in  $U$  and  $V$  are always different and  $U \cup V = \llbracket n \rrbracket$ . Consider  $P_U$  the interpolation polynomial such  $P_U(D_{i,i}) = 1$  if  $i \in U$  and 0 otherwise. Let  $P_V$  be defined the same way over  $V$ . We thus have  $(P_U + P_V)(D) = I_n$ . Thus  $AP_U(D) + AP_V(D) = AI_n = A$ , and  $AP_U(A) \subseteq A$ ,  $AP_V(A) \subseteq A$ . Calling  $A_U = AP_U(D)$  and  $A_V = AP_V(D)$  we see that  $A$  splits into  $A_U, A_V$  on support  $h = U$ , since  $P_U(D)$  and  $P_V(D)$  are orthogonal projections.

The same procedure splits  $B$  into  $B_U := BP_U(D)$  and  $B_V := BP_V(D)$ , which have the same supports  $h$  and  $\llbracket n \rrbracket \setminus h$ , so  $C$  splits as well.  $\square$

*Remark 6.* In our case, since we work with binary vectors, this is exactly the same definition as the one with the support  $h$  on which we project. But it still works in the non binary case, and might be more interesting. However, this definition is great as it gives a natural idea for an algorithm checking if a code splits.

For a code  $CSS(A, B)$  with generators and parity checks  $G_A, H_A, G_B, H_B$ , let us consider the following equation :

$$\begin{pmatrix} G_A & G_B \end{pmatrix} \begin{pmatrix} D & 0 \\ 0 & D \end{pmatrix} \begin{pmatrix} H_A \\ H_B \end{pmatrix} = 0 \quad (30)$$

when  $D$  is a diagonal matrix on  $n$  qubits. We know that  $D = \lambda I_n$  is always a solution of the equation as it preserves the codespace. Furthermore, if  $D$  is diagonal with coefficients not all equal, then it is in the solution space if and only if the code splits by [Proposition 14](#). This gives rise to the following algorithm.

---

**Algorithm 1** Split testing

---

**Require:** Generator and parity checks  $G_A, H_A$  and  $G_B, H_B$  of the codes  $A, B$

**Ensure:** Detect if the code splits

- 1:  $S \leftarrow \text{System\_Solving} \left( \begin{pmatrix} G_A & G_B \end{pmatrix} \begin{pmatrix} D & 0 \\ 0 & D \end{pmatrix} \begin{pmatrix} H_A \\ H_B \end{pmatrix} = 0 \right)$ .
  - 2:  $d \leftarrow \dim(S)$
  - 3: **return**  $d > 1$  ?
- 

This algorithm has complexity  $\mathcal{O}(n^\omega)$  which represent the time complexity of solving a system on  $2n$  qubits ( $2 \leq \omega < 3$ ). This algorithm is intuitive after seeing this new definition but it is not optimal. The graph theoretical approach will give the splits explicitly in quadratic time.

## 6.2 Graph theoretical approach

In [1] the author develops a method to identify if a matrix is "reducible" where  $F$  being reducible means that it either has a column of zeros or that there is an invertible map  $U$  and a permutation  $P$  such that

$$F = \begin{pmatrix} F_1 & 0 \\ 0 & F_2 \end{pmatrix}.$$

In our case, the definition of reducibility is the same as the definition of splitting of classical codes. Now to adapt in our case, we need to obtain the splits of  $X$ ,  $Z$  stabilizers but also compare them and find a common split. If such a split exists then the code splits.

The following algorithms follows the method from [1] to find if a matrix splits. Intuitively, each qubit represent a vertex, and we draw an edge between two qubits if there exists a stabilizer in which they both appear in the row reduced version of the  $X$  and  $Z$  stabilizer generators. To make it easier and more efficient we consider another graph which is the Tanner graph: instead of having each edge labeled by a stabilizer, qubits have an edge to a stabilizer if they appear in them. We then get the connected components of this graph. Each connected component represents a part of the split of the code as well as the stabilizer it concerns. We can then extract the qubits from those components if we only care about the splits. The proof of correctness of this approach can be derived from the one in [1].

Given generators of its stabilizer group represented as a  $r \times n$  matrix, this algorithm returns in time  $\mathcal{O}(n + \omega \times n)$  the split decomposition of a CSS code, where  $\omega$  is the maximal number of qubits in a stabilizer of the generator. Hence for LDPC codes, this algorithm is linear, while it is quadratic in general.

---

### Algorithm 2 Common Block Diagonalization

---

**Require:** Stabilizer matrix  $S = \begin{bmatrix} S_X & 0 \\ 0 & S_Z \end{bmatrix}$

**Ensure:** Partition of columns for common block diagonalization

- 1:  $S'_X \leftarrow \text{Row\_Reduced\_Form}(S_X)$
- 2:  $S'_Z \leftarrow \text{Row\_Reduced\_Form}(S_Z)$

3:  $S \leftarrow \begin{bmatrix} S'_X & 0 \\ 0 & S'_Z \end{bmatrix}$

- 4:  $G \leftarrow \text{Tanner\_Graph}(S')$
  - 5:  $C \leftarrow \text{Connected\_components}(G)$
  - 6: Blocks  $\leftarrow \text{Blocks\_From\_Connected\_Components}(C)$
  - 7: **return** Blocks
- 

---

### Algorithm 3 Tanner\_Graph

---

**Require:** Matrix  $F$  ( in symplectic form )

**Ensure:** Bipartite graph  $G$  with edges between  $r_i$  and  $c_j$  if  $F_{i,j} = 1$  or  $F_{i,j+n} = 1$ .

- 1: Initialize graph  $G = (R, C, E)$  where  $R$  are row vertices,  $C$  are column vertices, and  $E$  are edges
  - 2: **for** each entry  $F_{ij}$  in  $F$  **do**
  - 3:   **if**  $F_{ij} = 1$  **or**  $F_{i,j+n} = 1$  **then**
  - 4:     Add edge  $(r_i, c_j)$  to  $E$
  - 5:   **end if**
  - 6: **end for**
  - 7: **return**  $G$
- 

## Acknowledgements

We thank Adam Wills and Rachel Zhang for helpful discussions on the connections between our results. We also thank Arthur Pesah for introducing us to the addressability problem and for helpful discussions.

---

**Algorithm 4** Blocks\_From\_Connected\_Components

---

**Require:** Connected components  $C$

**Ensure:** Column index for the block diagonalization of the matrix

```

1: Blocks  $\leftarrow \emptyset$ 
2: for  $C_i$  in  $C$  do
3:   block $_i \leftarrow \emptyset$ 
4:   for  $c_j$  column vertex in  $C_i$  do
5:     block $_i \leftarrow \text{block}_i \cup \{j\}$ 
6:   end for
7:   Blocks  $\leftarrow \text{Blocks} \cup \{\text{block}_i\}$ 
8: end for
9: return Blocks

```

---

S. Jaques acknowledges the support of the Natural Sciences and Engineering Research Council of Canada (NSERC), funding reference number RGPIN-2024-03996.

## References

1. Burniston, John: Pre-Privacy Amplification: A Post-Processing Technique for Quantum Key Distribution with Application to the Simplified Trusted Relay. Master's thesis (2023), <http://hdl.handle.net/10012/19329>
2. Calderbank, A.R., Shor, P.W.: Good quantum error-correcting codes exist. *Phys. Rev. A* **54**, 1098–1105 (Aug 1996). <https://doi.org/10.1103/PhysRevA.54.1098>, <https://link.aps.org/doi/10.1103/PhysRevA.54.1098>
3. Grassl, M., Roetteler, M.: Leveraging automorphisms of quantum codes for fault-tolerant quantum computation. In: 2013 IEEE International Symposium on Information Theory. pp. 534–538 (2013). <https://doi.org/10.1109/ISIT.2013.6620283>
4. He, Z., Vaikuntanathan, V., Wills, A., Zhang, R.Y.: Quantum codes with addressable and transversal non-clifford gates (2025), <https://arxiv.org/abs/2502.01864>
5. Leverrier, A., Zemor, G.: Quantum tanner codes. In: 2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS). pp. 872–883. IEEE Computer Society, Los Alamitos, CA, USA (nov 2022). <https://doi.org/10.1109/FOCS54457.2022.00117>, <https://doi.ieeecomputersociety.org/10.1109/FOCS54457.2022.00117>
6. Lin, T.C.: Transversal non-clifford gates for quantum ldpc codes on sheaves (2024), <https://arxiv.org/abs/2410.14631>
7. Malcolm, A.J., Glaudell, A.N., Fuentes, P., Chandra, D., Schotte, A., DeLisle, C., Haenel, R., Ebrahimi, A., Roffe, J., Quintavalle, A.O., Beale, S.J., Lee-Hone, N.R., Simmons, S.: Computing efficiently in qldpc codes (2025), <https://arxiv.org/abs/2502.07150>
8. Panteleev, P., Kalachev, G.: Asymptotically good quantum and locally testable classical ldpc codes. In: Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing. p. 375–388. STOC 2022, Association for Computing Machinery, New York, NY, USA (2022). <https://doi.org/10.1145/3519935.3520017>, <https://doi.org/10.1145/3519935.3520017>
9. Patra, A., Barg, A.: Targeted clifford logical gates for hypergraph product codes (2024), <https://arxiv.org/abs/2411.17050>
10. Quintavalle, A.O., Webster, P., Vasmer, M.: Partitioning qubits in hypergraph product codes to implement logical gates. *Quantum* **7**, 1153 (Oct 2023). <https://doi.org/10.22331/q-2023-10-24-1153>, <https://doi.org/10.22331/q-2023-10-24-1153>
11. Rains, E.: Nonbinary quantum codes. *IEEE Transactions on Information Theory* **45**(6), 1827–1832 (1999). <https://doi.org/10.1109/18.782103>
12. Zhu, G., Sikander, S., Portnoy, E., Cross, A.W., Brown, B.J.: Non-clifford and parallelizable fault-tolerant logical gates on constant and almost-constant rate homological quantum ldpc codes via higher symmetries. *ArXiv abs/2310.16982* (2023), <https://api.semanticscholar.org/CorpusID:264490902>