On Local Equivalence, Surface Code States and Matroids

Pradeep Sarvepalli* and Robert Raussendorf

Department of Physics and Astronomy, University of British Columbia, Vancouver V6T 1Z1, Canada
(Dated: April 5, 2010)

Recently, Ji et al disproved the LU-LC conjecture and showed that the local unitary and local Clifford equivalence classes of the stabilizer states are not always the same. Despite the fact this settles the LU-LC conjecture, a sufficient condition for stabilizer states that violate the LU-LC conjecture is missing. In this paper, we investigate further the properties of stabilizer states with respect to local equivalence. Our first result shows that there exist infinitely many stabilizer states which violate the LU-LC conjecture. In particular, we show that for all numbers of qubits $n \geq 28$, there exist distance two stabilizer states which are counterexamples to the LU-LC conjecture. We prove that for all odd $n \geq 195$, there exist stabilizer states with distance greater than two which are LU equivalent but not LC equivalent.

Two important classes of stabilizer states that are of great interest in quantum computation are the cluster states and stabilizer states of the surface codes. To date, the status of these states with respect to the LU-LC conjecture was not studied. We show that, under some minimal restrictions, both these classes of states preclude any counterexamples. In this context, we also show that the associated surface codes do not have any encoded non-Clifford transversal gates. We characterize the CSS surface code states in terms of a class of minor closed binary matroids. In addition to making connection with an important open problem in binary matroid theory, this characterization does in some cases provide an efficient test for CSS states that are not counterexamples.

I. INTRODUCTION

An important problem in quantum information theory is to understand and classify the equivalence classes of quantum states. Such a classification could potentially simplify certain tasks in processing of quantum information and improve our understanding of the role of entanglement in quantum computing, especially, in measurement based computation models. A special case of the problem that has attracted much attention in the quantum information community, is to classify the equivalence of stabilizer states under local unitary gates and local Clifford gates.

Given a pair of stabilizer states, it is not known whether there exists an efficient (i.e. polynomial time) algorithm to test if they are local unitary equivalent. However, local *Clifford* equivalence of a pair of stabilizer states can be efficiently tested [16]. With this fact in mind, it has been conjectured that two stabilizer states are local unitary equivalent if and only if they are local Clifford equivalent. This is the LU-LC conjecture [14]. If it were true, then the above test [16] for local Clifford equivalence would imply an efficient test for local unitary equivalence among stabilizer states.

The LU-LC conjecture has been verified in numerous special cases. Rains [12] showed that the automorphisms of the linear stabilizer codes, with distance greater than two, are all in the local Clifford group. This result was subsequently strengthened to include a larger class of sta-

bilizer states by Van den Nest et al [17] and Zeng et al [19]. Hein et al [5] classified the stabilizer states of up to seven qubits, and the LU-LC conjecture always holds in this domain. These findings gave increasing credence to the LU-LC conjecture.

However, as has recently been demonstrated by a 27-qubit counterexample, the LU-LC conjecture is false [6]. Due to the above motivation, this surprising result may easily be seen as a setback. In a more positive light, it also reminds us how intricate a place Hilbert space is, often defying our preconceptions.

LU-LC counterexamples now come into view as an object of study in their own right. Presently, only a small number of computer-generated LU-LC counterexamples are known, and we lack an understanding of them. A theory of LU-LC counterexamples, once established, should identify the property due to which stabilizer states fail to satisfy the LU-LC conjecture, and provide a classification of all LU-LC counterexamples.

In this work we begin to study counterexamples to the LU-LC conjecture in a systematic fashion. We ask two questions: (1) *Are there finitely or infinitely many LU-LC counterexamples?*, and (2) *Can LU-LC counterexamples be found among prominent families of stabilizer states?* Regarding the first question, to date only very few stabilizer states are known that violate the LU-LC conjecture. One may therefore suspect they are rare and even finite in number. In Section III of this paper we show that there exist infinitely many counterexamples to the LU-LC conjecture.

To address the second question, in Sections IV and V we shift our focus to two important classes of stabilizer states, the cluster states [13] and the surface code states

[1, 7]. The cluster states form a universal resource for measurement based quantum computation, and the surface codes are an important family of quantum codes with topological properties. We show that under minimal restrictions on the states, they cannot be counterexamples to the LU-LC conjecture.

These results have useful applications. Quantum codes with encoded non-Clifford transversal gates are much sought after in the context of fault tolerant quantum computation. Surface codes are of great interest because they are especially suited for fault tolerant computation and their potential for high thresholds. However, no non-Clifford transversal gates have been found for these codes since their discovery almost a decade ago. As a consequence of our results on LU-LC counterexamples, in Section V we show that under similar restrictions as for LU-LC equivalence, surface codes do not have any non-Clifford transversal gates. Hence, fault tolerant quantum computation with these codes must necessarily rely on other methods to realize any encoded non-Clifford gates.

II. BACKGROUND

Let $\mathcal{P}_n$ be the Pauli group over n qubits. Let $g = \otimes_{i=1}^n g_i$ be an element in $\mathcal{P}_n$. Then the support of g is defined as the subset of $\{1, \ldots, n\}$ for which $g_i \neq I$ i.e.

$$\mathrm{supp}(g) = \{i \mid g_i \neq I\}. \tag{1}$$

Given a stabilizer state $|\psi\rangle$ and its stabilizer $S(\psi)$, we say that $g \in S(\psi)$ is a minimal support element if there does not exist any element $h \in S(\psi)$ such that $\emptyset \neq \mathrm{supp}(h) \subset \mathrm{supp}(g)$. In other words, $\mathrm{supp}(g)$ does not strictly contain the support of any nontrivial element of S. We also say that g is a minimal element of $S(\psi)$, and $\mathrm{supp}(g)$ is a minimal support of $S(\psi)$. We define the weight of $g \in \mathcal{P}_n$ as

$$\mathrm{wt}(g) = |\{i \mid g_i \neq I\}| = |\mathrm{supp}(g)|. \tag{2}$$

The distance of a subgroup S in $\mathcal{P}_n$ is defined as

$$\min_{g \in S \setminus I} \mathrm{wt}(g), \tag{3}$$

where g is not the identity element of S. Often, we refer to the distance of a stabilizer state by which we mean the distance of its stabilizer $S(\psi)$.

Let $|\psi\rangle$ be a stabilizer state. Let $U(2^n)$ denote the group of $2^n \times 2^n$ unitary matrices. An element of $U(2^n)$ is local unitary if it is in the local unitary group $\mathcal{U}_n^l = U(2)^{\otimes^n}$. Two stabilizer states $|\psi\rangle$ and $|\psi'\rangle$ are said to be local unitary (LU) equivalent if $|\psi'\rangle = U|\psi\rangle$ for some $U \in \mathcal{U}_n^l$. If each U_i is also a diagonal matrix, then $|\psi\rangle$ and $|\psi'\rangle$ are diagonal local unitary (DLU) equivalent. We denote the local unitary equivalence class of a stabilizer state $|\psi\rangle$ by $\mathrm{LU}(\psi)$. The Clifford group over n qubits is the normalizer of the Pauli group in $U(2^n)$. In other words,

$$\mathcal{K}_n = \{U \in U(2^n) \mid U\mathcal{P}_n U^\dagger = \mathcal{P}_n\}. \tag{4}$$

The local Clifford group over n qubits is defined as $\mathcal{K}_n^l = \mathcal{K}_1^{\otimes^n}$. Two stabilizer states $|\psi\rangle$ and $|\psi'\rangle$ are local Clifford (LC) equivalent if there exists a $K \in \mathcal{K}_n^l$ such that $|\psi'\rangle = K|\psi\rangle$. We denote the local Clifford equivalence class of $|\psi\rangle$ by $\mathrm{LC}(\psi)$. The single qubit Clifford group $\mathcal{K}_1 = \langle \lambda I, H, P \rangle$ where λ is a complex scalar, while H and P denote the Hadamard gate and the phase gate $(\mathrm{diag}(1, i))$. We consider two elements of $\mathcal{K}_1$ equivalent if their action on the Pauli matrices (by conjugation) differs only by a scalar. Then we need only consider the action of six elements[21] in $\mathcal{K}_1$, namely—$\{I, H, P, HP, PH, HPH\}$. These can be identified with nonsingular 2×2 binary matrices over the binary field $\mathbb{F}_2$.

The action of local unitaries on the stabilizer provides an important handle in understanding the LU-LC equivalence classes of that state. In particular, the action of local unitaries on the minimal supports of a stabilizer state is of great significance. We state the relevant result below and refer the interested reader to [12] for further details.

Lemma 1. *If $U \in \mathcal{U}_n^l$ maps a stabilizer state $|\psi\rangle$ to another stabilizer state $|\psi'\rangle = U|\psi\rangle$, then U maps the minimal support elements of $S(\psi)$ to the minimal support elements of $S(\psi')$.*

If both the local equivalence classes of $|\psi\rangle$ are the same, then we indicate this by $\mathrm{LU}(\psi) = \mathrm{LC}(\psi)$. There are some conditions under which we can conclude that $\mathrm{LU}(\psi) = \mathrm{LC}(\psi)$. A sufficient condition due to van den Nest et al will be useful in this context. For proof and further details, please refer to [17, Theorem 1] and [17, Corollary 1].

Lemma 2 (Minimal Support Condition)**.** *Suppose that $|\psi\rangle$ is a n-qubit stabilizer state free from Bell pairs. Let its stabilizer be $S(\psi)$ and $M(\psi)$ be the group generated by the minimal support elements of $S(\psi)$. If all the Pauli matrices X, Y, Z occur on every qubit in $M(\psi)$, (i.e. for any $\alpha \in \{X, Y, Z\}$, and for any i, there exists some $\otimes_{j=1}^n g_j \in M(\psi)$ such that it $g_i = \alpha$), then $\mathrm{LU}(\psi) = \mathrm{LC}(\psi)$. In particular this condition holds if $S(\psi) = M(\psi)$.*

Remark: This is a slightly relaxed version of the result in [17, Theorem 1], instead of fully entangled stabilizer states we have stabilizer states that are free from Bell pairs. It can be shown that the original proof holds with this modified condition.

A. Surface Code States

Let Γ be a graph with vertex set $V(\Gamma)$ and edge set $E(\Gamma)$. A cycle is an alternating sequence of vertices and edges such that every edge connects the adjacent vertices and only the first and last vertices are same. The length of a cycle is the number of edges in the cycle and a cycle of length n is called an n-cycle. A loop is an edge connecting

a vertex to itself, i.e., it is a 1-cycle. Not every graph can be drawn on the sphere so that the edges do not cross. However, by adding handles to the sphere we can draw the graph on the resulting surface so that the edges do not cross. The genus of the graph is the smallest number of handles that we need to add to the sphere so that it can embedded without edge crossings. Let the genus of the graph be g and assume that it is embedded on a surface of genus $g' \geq g$. We denote the set of faces of Γ by $F(\Gamma)$. The union of all the faces equals the surface on which the graph is embedded[22]. We can associate a stabilizer code to Γ. We identify qubits with the edges of the graph. Define the site operators and the face operators of Γ as:

$$A_v = \prod_{e \in \delta(v)} X_e; \quad B_f = \prod_{e \in \partial(f)} Z_e, \qquad (5)$$

where $\delta(v)$ is the set of edges incident on the vertex v and $\partial(f)$ is the set of edges that constitute the boundary of the face f. Let $S = \langle A_v, B_f \mid v \in V(\Gamma), f \in F(\Gamma) \rangle$, i.e, the group generated by the site operators and the face operators. We call the states stabilized by S as the surface code states of Γ and denote a surface code state of Γ as $|\psi_\Gamma\rangle$ to distinguish it from the graph state associated to Γ, where the vertices rather than the edges are associated to qubits.

Dual Graphs. Given a graph Γ, that is embedded on a surface, we can define a dual graph, denoted Γ^*. The dual graph is obtained as follows:

i) Each face f of Γ corresponds to a vertex f^* in Γ^*.
ii) Every vertex v of Γ corresponds to a face v^* in Γ^*.
iii) For each edge in Γ that is in the boundary of two faces f_1, f_2, connect the vertices f_1^* and f_2^* in Γ^*. In other words, if $e \in \partial(f_1) \cap \partial(f_2)$, then we place an edge between the vertices f_1^* and f_2^* in Γ^*.

We have the following correspondence between the Γ and Γ^*.

Γ	Γ^*
Edges	Edges
Faces	Vertices
Vertices	Faces

The edges in Γ are in 1-1 correspondence with the edges in Γ^* while the vertices are in correspondence with the faces of the dual graph. The edges incident on a vertex in Γ (Γ^*) are precisely the edges that form the boundary of the associated face in Γ^* (Γ). So the operator A_v is associated to a vertex and its incident edges in Γ, but it is associated to a cycle and its boundary edges in Γ^*. A set of edges is called an elementary cycle if it forms the boundary of a face in Γ. A set of edges of Γ which form a cycle in Γ^* is called a cocyle of Γ. A cocyle is called an elementary cocycle if it forms the boundary of a face in Γ^*. A loop is an edge connected to the same vertex. A coloop is a loop in the dual graph.

If Γ has no loops and has n edges and is embedded on a surface of genus g, the group generated by the site operators and the face operators contains $n - 2g$ generators

and it defines an $[[n, 2g]]$ surface code. There are 2^{2g} surface code states associated with an $[[n, 2g]]$ surface code. In this case, the supports of the encoded operators are defined by the nontrivial cycles and cocycles of Γ. For instance, when a graph of genus 2 is embedded on the torus we have an $[[n, 2]]$ surface code with 4 encoded operators; in general for a surface code on a surface of genus g we have $2g$ encoded operators. The support of the encoded Z operators is given by the cycles in Γ that wind across the holes of the torus and while that of encoded X operators are the cycles that wind around the holes of the torus in the dual graph. In other words the encoded operators are cycles and cocycles of Γ that are not homologous to any of the elementary cycles or cocycles.

When the graph has loops or when its genus is smaller than the genus of the surface on which it has been embedded, the number of encoded qubits can vary. For a graph with n edges and genus g that is embedded on a surface of genus $g' \geq g$, the stabilizer has $n - k$ generators and $2k$ encoded operators, where $k \leq 2g'$. Denote the encoded operators as $\mathcal{L} = \{\overline{X}_1, \overline{Z}_1, \ldots, \overline{X}_k, \overline{Z}_k\}$. The support of any encoded operators is a nontrivial cycle of the surface. These encoded operators allow us to specify each surface code state as follows. Let $\mathfrak{C}_1(\Gamma)$ and $\mathfrak{C}_1(\Gamma^*)$ be the set of homologically nontrivial cycles of Γ and Γ^* respectively. Then $\mathrm{supp}(\overline{X}_i) \in \mathfrak{C}_1(\Gamma^*)$ while $\mathrm{supp}(\overline{Z}_j) \in \mathfrak{C}_1(\Gamma)$. A CSS surface code state is stabilized by

$$S = \left\langle A_v, B_f, \overline{X}_1, \ldots, \overline{X}_l, \overline{Z}_{l+1}, \ldots, \overline{Z}_k \,\middle|\, \begin{matrix} v \in V(\Gamma) \\ f \in F(\Gamma) \end{matrix} \right\rangle, (6)$$

where we renumber the $\overline{X}_i$ and $\overline{Z}_j$ if necessary.

Before, we leave this section, we need one more result that relates minors of graphs and their duals. There are two basic operations we can perform on graphs:

1. Edge deletion
2. Edge contraction

The graph obtained from Γ by deleting an edge e is denoted as $\Gamma \setminus e$ while the graph obtained by edge contraction is denoted as Γ/e. A graph obtained from Γ by a sequence of edge deletions and contractions is called a (graph) minor of Γ. The following result on graph minors is well known.

Lemma 3. *Supposing we have a graph Γ and its dual Γ^* and $e \in E(\Gamma)$. The following relations hold:*
a. $(\Gamma \setminus e)^* = \Gamma^*/e$
b. $(\Gamma/e)^* = \Gamma^* \setminus e$

III. COUNTEREXAMPLES TO THE LU-LC CONJECTURE.

In this section, we address the first of the two questions we posed in the introduction, namely, are there finitely or infinitely many counterexamples to the LU-LC conjecture. We show that there are infinitely many counterexamples to the LU-LC conjecture and that a counterex-

ample exists for every odd length greater than 200. We prove these results constructively.

Suppose that Q is an $[[n, k, d]]$ quantum code. Let U be an encoded gate for the code, therefore $UQ = Q$. If in addition, $U = \otimes_{i=1}^{n} U_i$ then we say that it is a transversal encoded gate[23]. We need the following lemma; although straightforward, we include the proof for completeness.

Lemma 4. *Let $|\psi\rangle$ and $|\varphi\rangle$ be two stabilizer states that are diagonal local unitary (DLU) equivalent, i.e.,*

$$|\varphi\rangle = \bigotimes_{j=1}^{n} U_j |\psi\rangle, \text{ where } U_j = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta_j} \end{bmatrix}. \text{ Suppose that}$$

there exists an $[[m, 1, d]]$ quantum code Q, which has a transversal implementation for some U_j. Encode the jth qubit of $|\psi\rangle$ and $|\varphi\rangle$ using Q and denote the resulting states by $|\overline{\psi}\rangle$ and $|\overline{\varphi}\rangle$ respectively. Then $\mathrm{LU}(\overline{\psi}) = \mathrm{LU}(\overline{\varphi})$. If the transversal implementation of U_j consists of diagonal unitaries, then $|\overline{\psi}\rangle$ and $|\overline{\varphi}\rangle$ are also DLU equivalent.

Proof. Let us rewrite the state $|\psi\rangle$ as $|0\rangle_j |\psi^0\rangle_{\sim j} + |1\rangle_j |\psi^1\rangle_{\sim j}$, where the subscripts j and $\sim j$ denote the jth qubit and the remaining qubits respectively. Encoding the jth qubit by Q we obtain

$$|\overline{\psi}\rangle = |\overline{0}\rangle_j |\psi^0\rangle_{\sim j} + |\overline{1}\rangle_j |\psi^1\rangle_{\sim j}.$$

Since $|\varphi\rangle = U|\psi\rangle$ we have

$$
\begin{aligned}
|\varphi\rangle &= U_j|0\rangle_j \bigotimes_{\substack{i=1 \\ i\neq j}}^{n} U_i|\psi^0\rangle_{\sim j} + U_j|1\rangle_j \bigotimes_{\substack{i=1 \\ i\neq j}}^{n} U_i|\psi^1\rangle_{\sim j} \\
&= |0\rangle_j \bigotimes_{\substack{i=1 \\ i\neq j}}^{n} U_i|\psi^0\rangle_{\sim j} + e^{i\theta_j}|1\rangle_j \bigotimes_{\substack{i=1 \\ i\neq j}}^{n} U_i|\psi^1\rangle_{\sim j}.
\end{aligned}
$$

Encoding the jth qubit we obtain

$$|\overline{\varphi}\rangle = |\overline{0}\rangle_j \bigotimes_{\substack{i=1 \\ i\neq j}}^{n} U_i|\psi^0\rangle_{\sim j} + e^{i\theta_j}|\overline{1}\rangle_j \bigotimes_{\substack{i=1 \\ i\neq j}}^{n} U_i|\psi^0\rangle_{\sim j}$$

Let the transversal implementation of U_j for Q be $\overline{U}_j = \otimes_{i=1}^{m} \overline{U}_{j,i}$, then we can rewrite the above equation as

$$
\begin{aligned}
|\overline{\varphi}\rangle &= \overline{U}_j|\overline{0}\rangle_j \bigotimes_{\substack{i=1 \\ i\neq j}}^{n} U_i|\psi^0\rangle_{\sim j} + \overline{U}_j|\overline{1}\rangle_j \bigotimes_{\substack{i=1 \\ i\neq j}}^{n} U_i|\psi^0\rangle_{\sim j} \\
&= \overline{U}_j \bigotimes_{\substack{i=1 \\ i\neq j}}^{n} U_i(|\overline{0}\rangle_j|\psi^0\rangle_{\sim j} + |\overline{1}\rangle_j|\psi^0\rangle_{\sim j}) = \overline{U}|\overline{\psi}\rangle.
\end{aligned}
$$

Clearly, the states $|\overline{\psi}\rangle$ and $|\overline{\varphi}\rangle$ are LU equivalent. Further, they are DLU equivalent if U_j has a diagonal transversal implementation, i.e., each of the $\overline{U}_{j,i}$ is diagonal, for $1 \leq i \leq m$. $\square$

Lemma 5. *Let two stabilizer states $|\psi\rangle$ and $|\psi'\rangle = \otimes_{i=1}^{n} U_i |\psi\rangle$ be diagonal local unitary equivalent, where*

each U_i is a non-Clifford unitary. Then, all the minimal support elements of $S(\psi)$ and $S(\psi')$ must consist of Z-only operators. If in addition, $|\psi\rangle$ and $|\psi'\rangle$ are local Clifford equivalent, then they must also be diagonal local Clifford equivalent.

Proof. By Lemma 1 we know that U maps the minimal support elements of $S(\psi)$ to minimal support elements of $S(\psi')$. The action of U on $S(\psi)$ is to transform it as $US(\psi)U^\dagger$. Although $US(\psi)U^\dagger$ need not necessarily be in the Pauli group, the minimal support elements must be in the Pauli group. Therefore, for any minimal support element $x \in S(\psi)$ we must have $UxU^\dagger \in \mathcal{P}_n$. But under the assumption that U_i is a non-Clifford diagonal unitary, only Z of all the Pauli matrices is mapped back to a Pauli matrix. Assuming that $U_i = \mathrm{diag}(1, e^{i\theta_i})$, a Pauli matrix is transformed under conjugation as $U\sigma U^\dagger$, where $\sigma \in \mathcal{P}_1$. If a minimal element in $S(\psi)$ contains either X or Y it cannot be mapped to a minimal element of $S(\psi')$ by an arbitrary non-Clifford diagonal unitary[24]. Therefore all the minimal support elements of $S(\psi)$ must be Z-only operators. Similarly the minimal support elements of $S(\psi')$ must be also Z-only operators.

Without loss of generality we can assume that the stabilizer matrix of $|\psi\rangle$ is given by

$$S(\psi) = \begin{bmatrix} I_k & P & Q & 0 \\ 0 & 0 & P^t & I_{n-k} \end{bmatrix}, \tag{7}$$

where we have slightly abused the notation to denote both the stabilizer and the stabilizer matrix by $S(\psi)$. Since the minimal elements are Z-only operators, any minimal element must be a minimal element[25] of the binary code generated by $\begin{bmatrix} P^t & I_{n-k} \end{bmatrix}$. Denote this code as C. Since the codewords of C correspond to the Z only elements in $S(\psi)$, we will sometimes refer to an element of C as also being in $S(\psi)$. We claim that every minimal element of C is also a minimal element of $S(\psi)$. Let a be a minimal codeword of C. Suppose that a, or the element in $S(\psi)$ corresponding to a, is not a minimal element of $S(\psi)$. There exists some minimal element $b \in S(\psi)$ such that $\emptyset \neq \mathrm{supp}(b) \subsetneq \mathrm{supp}(a)$. We have already seen that every minimal element of $S(\psi)$ consists of Z-operators only. If so, then there exists a codeword c in C such that $\mathrm{supp}(c) = \mathrm{supp}(b)$ and $\mathrm{supp}(c) \subsetneq \mathrm{supp}(a)$ contradicting the assumption that a was a minimal element of C. Therefore, every minimal element of C is also a minimal element of $S(\psi)$.

We claim that the minimal elements of $S(\psi)$ span all the qubits i.e.,

$$\bigcup_{\substack{x \in S(\psi): \\ x \text{ is minimal}}} \mathrm{supp}(x) = \{1, 2, \dots, n\}. \tag{8}$$

To see this assume that there is some $j \in \{1, 2, \dots, n\}$ that is not in the support of any minimal element $x \in S(\psi)$. As the minimal elements are Z-only operators, it must necessarily follow that jth column of C is an all zero

column. Without loss of generality, assume that this is the first column. Then it implies that s_1, the first row of the stabilizer matrix in equation (7) must be of the form $s_1 = (1, 0, \ldots, 0 | q_{11}, q_{12}, \ldots, q_{1k}, 0, \ldots, 0)$ in order that it commute with $S(\psi)$ [26]. Then s_1 has support only in the first k qubits and not being a Z-only operator must be non-minimal. Therefore the support of some minimal element must be strictly contained in the first k qubits. But note that C is generated by $\begin{bmatrix} P^t & I_{n-k} \end{bmatrix}$, thus every minimal element has nonzero support in the last $n - k$ qubits. Therefore no minimal support can be strictly in the support of s_1, thereby making s_1 a minimal element and giving us a contradiction. Hence equation (8) must hold.

Since $|\psi\rangle$ and $|\psi'\rangle$ are also local Clifford equivalent, there exists a local Clifford unitary $K = \otimes_{i=1}^n K_i$ such that $|\psi'\rangle = K|\psi\rangle$; each of the $K_i \in \mathcal{K}_1$. If g is some minimal element in $S(\psi)$, then $g_i = Z$ for $i \in \text{supp}(g)$. The local Clifford unitary also maps the minimal elements of $S(\psi)$ to the minimal elements of $S(\psi')$. Therefore $K_i g_i K_i^\dagger = Z$ for $i \in \text{supp}(g)$. There are six possibilities [27] for the local Clifford unitaries—$\{I, H, P, HP, PH, HPH\}$. Of these only if $K_i \in \{I, P\}$ can the above requirement of mapping a minimal element to a minimal element is satisfied. So if $i \in \text{supp}(x)$ for some minimal element $x \in S(\psi)$, the associated Clifford unitary is diagonal. Because equation (8) holds, we know every i occurs in the support of some minimal element, therefore K_i is a diagonal local Clifford for all i. Thus $|\psi\rangle$ and $|\psi'\rangle$ are diagonal local Clifford equivalent. $\square$

A statement similar to second part of the previous lemma was attributed to Zeng in [6]. With this preparation, we are now ready to give a constructive method to generate new counterexamples to the LU-LC conjecture.

Theorem 6. *Let $|\psi\rangle$ be a CSS stabilizer state and $|\psi'\rangle$ another stabilizer state satisfying the following conditions:*
6.a $|\psi'\rangle = \otimes_{i=1}^n U_i|\psi\rangle$ i.e. $\text{LU}(\psi') = \text{LU}(\psi)$
6.b U_i is a diagonal non-Clifford unitary for all i
6.c $\text{LC}(\psi') \neq \text{LC}(\psi)$
6.d There exists an $[[m, 1, d]]$ CSS code such that some U_i, say U_n, as an encoded gate, has a diagonal non-Clifford transversal implementation i.e. $\overline{U}_n = \otimes_{j=1}^m F_j$ where F_j is a non-Clifford diagonal unitary.

Then encoding the nth qubit with the $[[m, 1, d]]$ code results in encoded states $|\overline{\psi'}\rangle = \otimes_{j=1}^{n+m-1} U_i'|\overline{\psi}\rangle$ where each of the $U_i' = U_i$ for $1 \leq i \leq n - 1$ and $U_i' = F_{i-n+1}$ $n \leq i \leq n + m - 1$ which satisfy 6.a–c.

Proof. By [2], see also [18, Theorem 5], we know that any stabilizer state can be represented in a "standard from". In particular, a stabilizer state $|\psi\rangle$ in standard form can be associated to a subspace S_ψ and a quadratic form $q_\psi(x)$ such that

$$|\psi\rangle = \sum_{x \in S_\psi} (-1)^{q_\psi(x)} |x\rangle.$$

Throughout this proof, we neglect the normalizing factors for convenience. We assume that both $|\psi\rangle$ and $|\psi'\rangle$ are in standard form. In the present case, as the states $|\psi\rangle$ and $|\psi'\rangle$ are diagonal local unitary equivalent, the same subspace S is associated to both of them, and we can assume that $|\psi\rangle$ is associated to the trivial form $q_\psi(x) \equiv 0$ and $|\psi'\rangle$ is associated to the quadratic form $q(x)$.

We can write $q(x) = \tilde{q}(x) + q_n(x)$ as the sum of two quadratic forms $\tilde{q}(x)$ and $q_n(x)$ where

$$\tilde{q}(x) = \sum_{1 \leq i < j < n} q_{ij} x_i x_j \text{ and } q_n(x) = \sum_{j=1}^{n-1} q_{jn} x_j x_n.$$

We slightly abuse the notation and write $\tilde{q}(x)$, although $\tilde{q}(\cdot)$ does not explicitly depend on x_n. Further we note that if $x_n = 0$, then $\tilde{q}(x) = q(x_1, \ldots, x_{n-1}, x_n = 0)$, so we can rewrite the states $|\psi\rangle$ and $|\psi'\rangle$ using $\tilde{q}(x)$ and $q_n(x)$ as

$$|\psi\rangle = \sum_{\substack{x \in S \\ x_n = 0}} |x_1 \cdots x_{n-1}\rangle|0\rangle + \sum_{\substack{x \in S \\ x_n = 1}} |x_1 \cdots x_{n-1}\rangle|1\rangle,$$

$$|\psi'\rangle = \sum_{\substack{x \in S \\ x_n = 0}} (-1)^{\tilde{q}(x)} |x_1 \cdots x_{n-1}\rangle|0\rangle +$$
$$\sum_{\substack{x \in S \\ x_n = 1}} (-1)^{\tilde{q}(x) + q_n(x)} |x_1 \cdots x_{n-1}\rangle|1\rangle.$$

Assume that we encode the nth qubit of $|\psi\rangle$ and $|\psi'\rangle$ using an $[[m, 1, d]]_2$ CSS code Q to obtain the encoded states $|\overline{\psi}\rangle$ and $|\overline{\psi'}\rangle$. We assume that Q is derived from classical codes C and D where $C \subset D \subseteq \mathbb{F}_2^m$. The logical states of Q are given by

$$|\overline{0}\rangle = \sum_{x \in C} |x\rangle \text{ and } |\overline{1}\rangle = \sum_{x \in D \setminus C} |x\rangle = \sum_{x \in C} |x + X_e\rangle,$$

where $X_e = (a_1, \ldots, a_m)$ is any element in $D \setminus C$. It is in effect the encoded X operator of Q, strictly speaking $(a_1, \ldots, a_m | 0, \ldots, 0)$ is the binary representation of encoded X operator. Let $Z_e = (b_1, \ldots, b_m)$ be any vector in $C^\perp \setminus D^\perp$. Note that if $c \in C$, then $c \cdot Z_e = 0$ while $c \cdot Z_e = 1$ for any $c \in D \setminus C$, in particular this is true for $c = X_e$.

Then we can write the encoded states $|\overline{\psi}\rangle$ and $|\overline{\psi'}\rangle$ as

$$
\begin{aligned}
|\overline{\psi}\rangle &= \sum_{\substack{x\in S\\x_n=0}} |x_1\cdots x_{n-1}\rangle|\overline{0}\rangle + \sum_{\substack{x\in S\\x_n=1}} |x_1\cdots x_{n-1}\rangle|\overline{1}\rangle \\
&= \sum_{\substack{x\in S\\x_n=0}} |x_1\cdots x_{n-1}\rangle \sum_{y\in C} |y\rangle + \\
&\qquad \sum_{\substack{x\in S\\x_n=1}} |x_1\cdots x_{n-1}\rangle \sum_{y\in C} |y+X_e\rangle \\
|\overline{\psi'}\rangle &= \sum_{\substack{x\in S\\x_n=0}} (-1)^{\tilde{q}(x)}|x_1\cdots x_{n-1}\rangle|\overline{0}\rangle + \\
&\qquad \sum_{\substack{x\in S\\x_n=1}} (-1)^{\tilde{q}(x)+q_n(x)}|x_1\cdots x_{n-1}\rangle|\overline{1}\rangle \\
&= \sum_{\substack{x\in S\\x_n=0}} (-1)^{\tilde{q}(x)}|x_1\cdots x_{n-1}\rangle \sum_{y\in C} |y\rangle + \\
&\qquad \sum_{\substack{x\in S\\x_n=1}} (-1)^{\tilde{q}(x)+q_n(x)}|x_1\cdots x_{n-1}\rangle \sum_{y\in C} |y+X_e\rangle
\end{aligned}
$$

Let $E = (e_1,\ldots,e_n) \in S$ be a vector such that $e_n = 1$. Denote by $\overline{E} = (e_1,\ldots,e_{n-1})$, the vector obtained by dropping the nth coordinate. As the encoded states are also stabilizer states we can associate a subspace $\overline{S}$ to them as

$$\overline{S} = \langle S_0 \oplus C, (\overline{E}|X_e)\rangle$$

where $(\overline{E}|X_e) = (e_1,\ldots,e_{n-1},a_1,\ldots,a_m)$ and

$$S_0 = \{(x_1,\ldots,x_{n-1}) \mid x \in S \text{ and } x_n = 0\}$$

Additionally, we can associate a quadratic form $\overline{q}(\cdot)$ to $|\overline{\psi'}\rangle$ as

$$\overline{q}(x_1,\ldots,x_{n-1},y_1,\ldots,y_m) = \sum_{1\le i<j<n} q_{ij}x_i x_j +$$
$$\sum_{j=1}^{n-1} q_{jn}x_j(b_1 y_1 + \cdots + b_m y_m),$$

where $(b_1,\ldots,b_m) \in C^\perp \setminus D^\perp$. Although, $\overline{q}$ does not explicitly depend on x_n we write $\overline{q}(x,y)$ for $\overline{q}(x_1,\ldots,x_{n-1},y_1,\ldots,y_m)$. If $x\in S$ and $x_n = 0$, then y must be in C. Then $b_1 y_1 + \cdots + b_m y_m = Z_e\cdot y = 0$ as $Z_e \in C^\perp$ and $\overline{q}(x,y)$ reduces to $\tilde{q}(x) = q(x)|_{x_n=0}$. If $x\in S$ and $x_n = 1$, then we must have $y\in D\setminus C$ giving $b_1 y_1 + \cdots + b_m y_m = Z_e\cdot y = 1$. In this case $\overline{q}(x,y)$ reduces to $\tilde{q}(x)+q_n(x) = q(x)|_{x_n=1}$. Thus

$$|\overline{\psi'}\rangle = \sum_{x\in S_0\oplus C}(-1)^{\overline{q}(x)}|x\rangle + \sum_{x\in(S_0\oplus C)+(\overline{E}|X_e)}(-1)^{\overline{q}(x)}|x\rangle$$

By assumption the code C has a diagonal non-Clifford transversal implementation of $\overline{U}_i$; without loss of generality we can assume that $i = n$. Then by Lemma 4,

the states $|\overline{\psi}\rangle$ and $|\overline{\psi'}\rangle$ are diagonal LU equivalent. This proves that $|\overline{\psi}\rangle$ and $|\overline{\psi'}\rangle$ satisfy 6.a and 6.b.

We claim that $|\overline{\psi}\rangle$ and $|\overline{\psi'}\rangle$ are not LC equivalent. Suppose that they are LC equivalent. Then by Lemma 5, $|\overline{\psi}\rangle$ and $|\overline{\psi'}\rangle$ are DLC equivalent. In such a case there exist complex numbers $c_j \in \langle i\rangle$, $1\le j\le n+m-1$ such that

$$\prod_{j=1}^{n+m-1} c_j^{s_j} = (-1)^{\overline{q}(s)} \text{ for all } s\in\overline{S}.$$

Alternatively, letting $s = (x|y)$, we must have

$$\prod_{j=1}^{n-1} c_j^{x_j} \prod_{j=1}^{m} c_{j+n-1}^{y_j} = (-1)^{\overline{q}(x,y)} \tag{9}$$
$$= (-1)^{\tilde{q}(x)+\sum_{j=1}^{n-1} q_{jn}x_j(b_1 y_1+\cdots+b_m y_m)},$$

for all $(x|y)\in\overline{S}$. Consider an $s\in S_0\oplus C\subset\overline{S}$, in particular let $s = (x|y)$ where $y=0$ and x is any element such that $(x_1,\ldots,x_{n-1},0)\in S$. Then equation (9) reduces to

$$\prod_{j=1}^{n-1} c_j^{x_j} = (-1)^{\overline{q}(x,0)} = (-1)^{\tilde{q}(x)} \tag{10}$$
$$= (-1)^{q(x)} \text{ for all } (x_1,\ldots,x_{n-1},0)\in S. \tag{11}$$

If $s = (x|y)$ is in $\overline{S}\setminus(S_0\oplus C)$, then $(x_1,\ldots,x_{n-1},1)\in S$ and $y\in D\setminus C$. Choosing $y = \overline{X}$, we get

$$\prod_{j=1}^{n-1} c_j^{x_j}\prod_{j=1}^{m} c_{j+n-1}^{y_j} = (-1)^{\tilde{q}(x)+\sum_{j=1}^{n-1}q_{jn}x_j(b_1 y_1+\cdots+b_m y_m)}$$
$$= (-1)^{\tilde{q}(x)+\sum_{j=1}^{n-1}q_{jn}x_j(Z_e\cdot X_e)}$$
$$= (-1)^{\tilde{q}(x)+\sum_{j=1}^{n-1}q_{jn}x_j}$$
$$= (-1)^{\tilde{q}(x)+\sum_{j=1}^{n-1}q_{jn}x_j x_n}$$

Letting $C_j = c_j$ for $1\le j<n$ and $C_n = \prod_{j=n}^{n+m-1} c_j^{y_j}$ we obtain

$$\prod_{i=1}^{n} C_i^{x_i} = (-1)^{q(x)} \text{ for all } (x_1,\ldots,x_{n-1},1)\in S. \tag{12}$$

Since $c_j\in\langle i\rangle$, C_j are also in $\langle i\rangle$. Together equations (11) and (12) imply that for all $x\in S$, there exist $C_j\in\langle i\rangle$ such that

$$\prod_{j=1}^{n} C_j^{x_j} = (-1)^{q(x)} \text{ for all } x\in S.$$

It follows that the states $|\psi\rangle$ and $|\psi'\rangle$ are diagonal local Clifford equivalent, (see [6]). But this contradicts that $|\psi\rangle$ and $|\psi'\rangle$ are not local Clifford equivalent. Therefore it must be that $|\overline{\psi}\rangle$ and $|\overline{\psi'}\rangle$ are not LC equivalent. Thus they furnish another counterexample for the LU-LC conjecture. $\square$

We point out that the assumption that $|\psi\rangle$ is a CSS stabilizer state in Theorem 6 is not really a limitation, because of the following reason. Supposing that $|\psi\rangle$ and $|\psi'\rangle$ are both not CSS stabilizer states. Let us associate them to two distinct quadratic forms $q_\psi(x)$ and $q_{\psi'}(x)$, as the states are not local Clifford equivalent.

$$|\psi\rangle = \sum_{x \in S} (-1)^{q_\psi(x)} |x\rangle \text{ and } |\psi'\rangle = \sum_{x \in S} (-1)^{q_{\psi'}(x)} |x\rangle.$$

We can consider the following states $|\varphi\rangle$ and $|\varphi'\rangle$ instead of $|\psi\rangle$ and $|\psi'\rangle$.

$$|\varphi\rangle = \sum_{x \in S} |x\rangle \text{ and } |\varphi'\rangle = \sum_{x \in S} |x\rangle (-1)^{q(x)} |x\rangle,$$

where $q(x) = q_\psi(x) + q_{\psi'}(x) = \sum_{1 \le i < j \le n} q_{ij} x_i x_j$. The states $|\varphi\rangle$ and $|\varphi'\rangle$ are related by the same local diagonal unitaries as $|\psi\rangle$ and $|\psi'\rangle$, i.e., $|\varphi'\rangle = \otimes_{i=1}^{n} U_i |\varphi\rangle$. Further, they are also a pair of states that violate the LU-LC conjecture. If they are not, then $|\varphi'\rangle$ and $|\varphi\rangle$ are LC equivalent. But by Lemma 5 they are also DLC equivalent which in turn implies the DLC equivalence of $|\psi\rangle$ and $|\psi'\rangle$ contradicting that $|\psi\rangle$ and $|\psi'\rangle$ are not LC equivalent. We can see that $|\varphi\rangle$ and $|\varphi'\rangle$ satisfy the conditions 6.a–d. Consequently, we can use these states to generate new counterexamples in Theorem 6.

Additionally, we could also lift the assumption on the use of a CSS code in Theorem 6, provided the non-CSS $[[m, 1, d]]$ code has a non-Clifford transversal gate that can be implemented using diagonal non-Clifford gates. An alternate proof of Theorem 6 seems to be possible based on [16].

Corollary 7. *There are infinitely many stabilizer states for which the LU-LC conjecture does not hold. In particular, there exist stabilizer states which are LU equivalent but not LC equivalent under the following conditions:*
a. distance two and $n \ge 28$
b. distance ≥ 3 and odd length $n \ge 195$

Proof. We note that the 27 qubit counterexample provided in [6] provides a starting point for the application of Theorem 6. In this case the two locally equivalent stabilizer states are related by diagonal non-Clifford unitaries and are odd powers of the T gate where $T = \mathrm{diag}(1, e^{i\pi/4})$. We know that the T gate has a diagonal non-Clifford transversal implementation for the $[[15, 1, 3]]$ Reed-Muller code, while $\sqrt{T} = \mathrm{diag}(1, e^{i\pi/8})$ has a diagonal non-Clifford implementation for the $[[31, 1, 3]]$ Reed-Muller code and the $[[2, 1, 1]]$ code. So all these codes permit a transversal implementation of the T gate. In fact their transversal implementations use T gate on each qubit. So we can concatenate with either code to obtain a new counterexample of length 41 and 57 and 28 respectively. The resulting state obtained by encoding with any of these code also satisfies 6.d in addition to the conditons 6.a–c. If we repeatedly use the $[[2, 1, 1]]$ code, then we obtain distance two counterexamples for any $n \ge 28$.

If we use a combination of $[[15, 1, 3]]$ and $[[31, 1, 3]]$ and repeatedly apply Theorem 6 to these states to obtain a series of stabilizer states of length $27 + 14i + 30j$ which are LU-equivalent but not LC-equivalent. It remains to show that all the odd lengths beyond $n \ge 195$ can be attained by this concatenation. Now assume that we have concatenated i times with $[[15, 1, 3]]$ and j times with $[[31, 1, 3]]$ to obtain $n(i, j) = 27 + 14i + 30j$ length counterexamples. We can ignore the offset due to 27 and consider the linear combinations of $14i + 30j = 2c$. A solution for this equation is $i_0 = -2c$ and $j_0 = c$. We know from number theory, see [8, Theorem 5.1], that there exist infinitely many solutions for this equation given by

$$i = i_0 + 15k \text{ and } j = j_0 - 7k,$$

where k is an integer. Since we are interested in only those combinations for which $i, j \ge 0$, we require that

$$15k \ge -i_0 \text{ and } 7k \le j_0.$$

This implies that

$$2c/15 \le k \le c/7$$

Assuming that $c = 7q + r$, where $0 \le r \le 6$, we find that

$$(14q + 2r)/15 \le k \le q + r/7.$$

An integral solution of $k = q$ is possible if $(14q + 2r)/15 \le q$ i.e. $q \ge 2r$ or $q \ge 12$. Thus we obtain $i = i_0 + 15q = -2c + 15q$ and $j = j_0 - 7q = c - 7q = r$. We obtain $2c = 14q + 2r \ge 14 \cdot 12 = 168$. So for all odd lengths $n \ge 27 + 168 = 195$, there exists a counterexample to the LU-LC conjecture. $\blacksquare$

IV. LU-LC EQUIVALENCE OF CLUSTER STATES

Stabilizer states can be derived from graphs in two important ways. In one method we associate the edges to qubits. Such stabilizer states will be studied in the next section. In this section we study stabilizer states wherein the qubits are identified with the vertices of a graph. Such states are also termed graph states. A special class of these graph states are the cluster states. We turn our attention to cluster states and consider their equivalence classes. Our interest in cluster states stems from the fact that the cluster states form a universal resource for measurement based quantum computation.

Lemma 8. *Let Γ be an $m \times n$ rectangular grid, where $m, n \ge 5$. Then the local unitary and local Clifford equivalence classes of the graph state $|G\rangle$ are the same.*

Proof. The stabilizer of the graph state is given by

$$S = \langle K_v \mid v \in V(\Gamma) \rangle \text{ where } K_v = X_v \prod_{y \in N(x)} Z_y,$$

and $N(x)$ denotes the neighbors of x. If a generator K_v is not a minimal support element of S, then there exists a linear combination of the generators $\{K_v\} \cup \{K_x \mid x \in N(v)\}$ such that its support is strictly contained in $\text{supp}(K_v)$. We partition the vertices of the graph into three different sets:

1. V_i: vertices that are not connected to the boundary at all
2. V_o: vertices on the boundary of the grid
3. V_m: vertices which are connected to the boundary by at least one edge

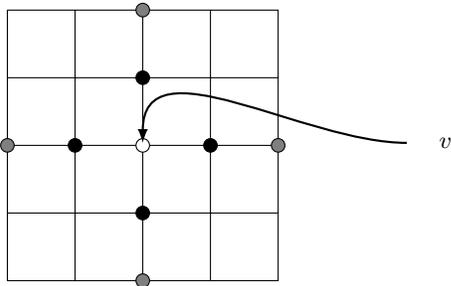Consider a generator K_v, where $v \in V_i$.

FIG. 1: v inside the boundary and without neighbor(s) on the boundary

Let $N(v) = \{a, b, c, d\}$, then we can see that every neighbor of v is connected to a vertex which is not connected to the remaining three neighbors of v. So any linear combination involving K_v, K_a, K_b, K_c, K_d will have a support outside $\text{supp}(K_v)$ unless it is equal to K_v.

Next consider a vertex on the boundary of Γ. Since $m, n \geq 5$, we need to consider three cases shown below when v is on the corner of the grid, when one of v's neighbors is a corner and when no neighbor is a corner.
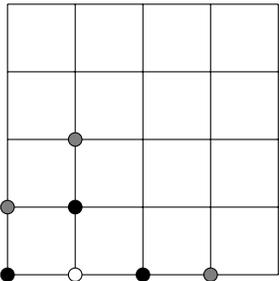

FIG. 2: v on the boundary with neighbor(s) on a corner

Finally, when v is in V_m, then we need to consider the following cases depending on whether v has one or two neighbors on the boundary of the grid.
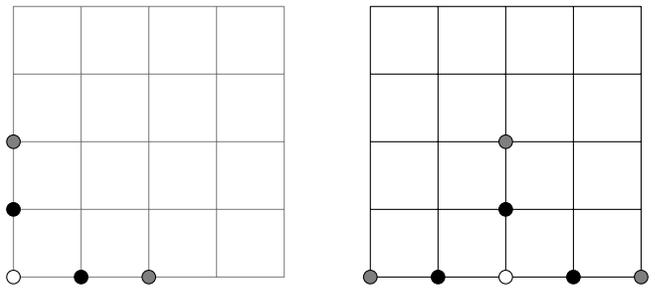

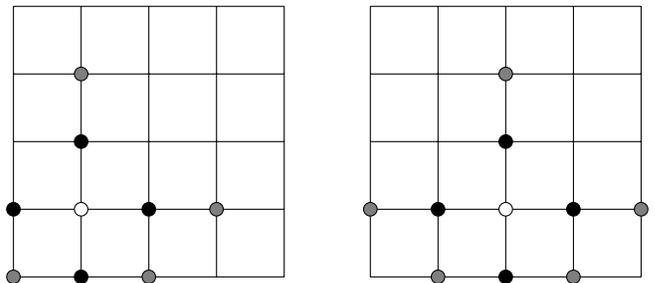FIG. 3: v on the boundary and without neighbors on a corner

FIG. 4: v inside the boundary but with at least one neighbor on the boundary

It can be easily verified that in each of the above cases, whenever there is a linear combination of the generators in the support of v, the resulting linear combination always has support outside $\text{supp}(v)$ unless the combination is trivially equal to K_v. Thus every generator K_v is a minimal element in S. Thus $M(|G\rangle) = S$ itself and by Lemma 2, we have $\text{LU}(|G\rangle) = \text{LC}(|G\rangle)$. $\square$

Zeng et al., [19] showed that if a graph Γ has no 3 or 4 cycles, then $\text{LU}(|G\rangle) = \text{LC}(|G\rangle)$. From this it follows that the graph states associated to honeycomb (i.e., hexagonal) lattices also satisfy the LU-LC conjecture. These results for the cluster states and the hexagonal lattices are somewhat surprising in that these states are universal resources for measurement based quantum computation.

V. LU-LC EQUIVALENCE OF SURFACE CODE STATES

In this section we show that surface code states cannot be counterexamples to the LU-LC conjecture. These results prepare the way to make the connection to matroids. We consider surface codes derived from connected graphs that have no loops or coloops. Additionally, we require the graphs to have no 2-cycles or 2-cocycles and are thus free from Bell pairs. The following lemma is known in the context of surface codes, but we record it for our later use.

Lemma 9. *Let $|\psi\rangle$ be a surface code state associated to a graph Γ without loops or coloops. Let g be an element*

in $C(S(\psi))$, the centralizer of $S(\psi)$ such that g consists of only Z (or X) operators alone. Then $\text{supp}(g)$ is an union of cycles (or cocycles) in Γ. In particular, the face (vertex) operators of Γ generate only union of cycles (cocycles) of Γ.

Proof. Assume that g is a Z-only operator in $C(S(\psi))$ such that its support is not a cycle in Γ. Since g consists of only Z operators it must be generated by the face operators of Γ and the encoded Z operators of the surface code associated to Γ. If the support of g is not an union of cycles then there exists a vertex v such that an odd number of the edges of $\text{supp}(g)$ are incident on v. Then the vertex operator A_v (consisting of X operators alone) does not commute with g as it overlaps with g over odd number of qubits. Therefore g cannot be an element of $C(S(\psi))$, as all elements in $C(S(\psi))$ commute with vertex operators. By a similar argument but considering the dual graph we can also show that all the X-only operators in $C(S(\psi))$ must be cycles in Γ^*. □

Requiring that Γ has no coloops is equivalent to stating that it has no cut set of size one. Lemma 9 can be extended to include graphs with loops and coloops, however this is sufficient for us. In the following we often denote the stabilizer of a quantum code Q by $S(Q)$. Given a subset $\omega \subseteq \{1, 2, \ldots, n\}$, and an abelian subgroup $S \leq C(S(Q))$ we denote by $A_\omega^S = |\{g \in S : \text{supp}(g) = \omega\}|$.

Lemma 10. *Suppose Q is a surface code associated to a graph Γ without cycles or cocycles of length ≤ 2. Let S be an abelian subgroup of $C(S(Q))$ that contains $S(Q)$. Then for any $A_v \in S$ and $B_f \in S$ we there exist minimal elements $\{g_1^v, \ldots, g_{k_v}^v\} \subset S$ and $\{h_1^f, \ldots, h_{k_f}^f\} \subset S$ such that*

i) *Each g_i^v is a X-only operator and $\text{supp}(A_v) = \cup_{i=1}^{k_v}\text{supp}(g_i^v)$.*
ii) *$A_{\text{supp}(g_i^v)}^S = 1$.*
iii) *Each h_i^f is a Z-only operator and $\text{supp}(B_f) = \cup_{i=1}^{k_f}\text{supp}(h_i^f)$.*
iv) *$A_{\text{supp}(h_i^f)}^S = 1$.*

Further, for any $j \in \{1, 2, \ldots, n\}$, there exists some A_v and B_f such that $j \in \text{supp}(A_v) \cap \text{supp}(B_f)$, where $n = |E(\Gamma)|$, the total number of qubits.

Proof. If A_v is minimal then i) holds trivially for A_v by letting $g_1^v = A_v$. Suppose that A_v is a non-minimal element in S. There exists a minimal element $g_1^v \neq I$ in S such that $\text{supp}(g_1^v) \subsetneq \text{supp}(A_v)$. Now as Q is a CSS code, g_1^v can be written as $g_1^v = g_x g_z$, for some $g_x, g_z \in C(S(Q))$ where both g_x and g_z are not simultaneously trivial. It follows that the supports of both g_x and g_z must be strictly contained in the support of A_v. In particular, $\text{supp}(g_z) \subsetneq \text{supp}(A_v)$. By Lemma 9, g_z must be a cycle of Γ. However, all the edges of g_z being a subset of $\text{supp}(A_v)$ must be incident on the same vertex. Then $\text{supp}(g_z)$ can be cycle only if it contains 2-cycles. But this contradicts that Γ does not have 2-cycles.

Therefore, $g_z = I$ and $g_x = g_1^v \neq I$. Now consider the element $g' = A_v g_1^v$, it is an X-only operator whose support is given by $\text{supp}(A_v) \setminus \text{supp}(g_1^v)$. Now g' is either minimal or not. If it is minimal then by relabeling $g' = g_2^v$ we can write $\text{supp}(A_v) = \text{supp}(g_1^v) \cup \text{supp}(g_2^v)$ and we are done. On the other hand if g' is not minimal, we can repeat the same process as with A_v and we will eventually end up with a set of elements $\{g_1^v, \ldots, g_{k_v}^v\}$ such that $\text{supp}(A_v) = \cup_{i=1}^{k_v}\text{supp}(g_i^v)$. This shows that i) holds.

Let $\omega = \text{supp}(g_i^v)$. Suppose that $A_\omega^S \neq 1$. Then there exists a $g_i' \in S$ such that $g_i' \neq g_i$ and $\text{supp}(g_i') = \omega$. Since $\omega \subsetneq \text{supp}(A_v)$, it follows that g_i' is also a minimal element within the support of A_v. But we have already seen that every minimal element in the support of A_v must consist of X-only operators. Therefore $g_i' = g_i^v$ contradicting that $g_i' \neq g_i^v$. Thus $A_{\text{supp}(g_i^v)}^S = 1$, proving ii).

We claim that $j \in \{1, 2, \ldots, n\}$ occurs in the support of A_v for some $v \in V(\Gamma)$. Since an edge is incident on at most two vertices, if $j \notin \text{supp}(A_v)$ for any $v \in V(\Gamma)$, this means that both ends of the edge associated to j must be incident on the same vertex. This implies that Γ has loops contrary to our assumptions. So every j occurs in the support of some site operator A_v.

By a similar argument but working in the dual graph Γ^*, we can show that $\text{supp}(B_f) = \cup_{i=1}^{k_f}\text{supp}(h_i)$ for some Z-only minimal elements in S and that j occurs in the support of some face operator B_f as long as there are no coloops. □

Theorem 11. *Let Q be the surface code associated to a graph Γ cycles or cocycles of length ≤ 2. Let $S(Q)$ be the stabilizer of Q and $C(S(Q))$, the centralizer of S. Then for any surface code (stabilizer) state $|\psi\rangle$ we have $\text{LU}(\psi) = \text{LC}(\psi)$.*

Proof. The stabilizer of a general surface code state is a subgroup of $C(S(Q))$ and contains $S(Q)$.

$$S(\psi) = \left\langle S, L_1, L_2, \ldots, L_k \middle| \begin{array}{c} L_i \in C(S(Q)) \setminus SZ(S(Q)) \\ \text{and } L_i L_j = L_j L_i \end{array} \right\rangle,$$

where k is such that $S(\psi)$ is the stabilizer of $|\psi\rangle$. Let $n = |E(\Gamma)|$, the total number of qubits. From Lemma 10, we know that every vertex operator and face operator are such that there exist X-only minimal elements $\{g_1, \ldots, g_{k_v}\} \in S(\psi)$ and Z-only minimal elements $\{h_1, \ldots, h_{k_f}\} \in S(\psi)$ such that $\cup_{i=1}^{k_v}\text{supp}(g_i) = \text{supp}(A_v)$ and $\text{supp}(B_f) = \cup_{i=1}^{k_f}\text{supp}(h_i)$. Since for every j we have $j \in \text{supp}(A_v) \cap \text{supp}(B_f)$ for some $v \in V(\Gamma)$ and $f \in F(\Gamma)$, there exist minimal elements g, h such that $g_j = X$ and $h_j = Z$. This means that on every qubit, all three X, Y, Z occur on every qubit in $M(\psi)$. Since there are no 2-cycles or 2-cocycles, $S(\psi)$ cannot contain elements of the form $X_i X_j$ or $Z_i Z_j$. Since Q is a CSS code if $X_i Z_j$ or $X_i Y_j$ are in $C(S(Q))$, then it follows that Γ has loops or coloops, contradicting the assumptions on Γ. Thus $|\psi\rangle$ is free of Bell pairs. By Lemma 2, it follows that $\text{LU}(\psi) = \text{LC}(\psi)$. □

A. Application: On the Existence of Non-Clifford Transversal Gates

From the point of fault tolerant quantum computing (encoded) transversal gates are very desirable for quantum codes. Transversal gates within the Clifford group can be found using the symmetries of the stabilizer. Transversal gates outside the Clifford group are known only for a handful of quantum codes, the prominent being the quantum Reed-Muller codes [19]. The primary motivation for non-Clifford transversal gates was to find a universal set of encoded transversal gates. That such a universal set does not exist for stabilizer codes has been shown in [20] and a similar result for general quantum codes was proved in [3].

Finding transversal gates outside the Clifford group has turned to be very difficult. In fact, Rains [11] has shown that non-Clifford transversal gates do not exist for $GF(4)$-linear quantum codes. Surface codes are purely additive quantum codes, and in this section we show that under some restrictions, surface codes preclude the existence of non-Clifford transversal gates.

Lemma 12. *[20, Lemma 1] Let Q be a stabilizer code. If $U = U_1 \otimes \cdots \otimes U_n$ is a logical gate for Q, then $U_\omega \rho_\omega(Q) = \rho_\omega(Q) U_\omega$ for all $\omega \subseteq \{1, 2, \ldots, n\}$, where $U_\omega = \otimes_{i \in \omega} U_i$,*

$$\rho_\omega = \frac{1}{B_\omega(Q)} \sum_{\substack{s \in S(Q) \\ \mathrm{supp}(s) \subseteq \omega}} \mathrm{Tr}_{\bar{\omega}}(s); \qquad (13)$$

$$B_\omega(Q) = |\{s \in S(Q) : \mathrm{supp}(s) \subseteq \omega\}| \qquad (14)$$

for all ω. More generally, if Q' is another stabilizer code such that U is a local equivalence from Q to Q', then $U_\omega \rho_\omega(Q) = \rho_\omega(Q') U_\omega$,

Theorem 13. *Let Q be a surface code such that the associated graph does not have any cycles or cocycles of length ≤ 2. Then Q does not have any transversal encoded non-Clifford gate, $U = U_1 \otimes U_2 \otimes \cdots \otimes U_n$.*

Proof. We assume that Q is derived from a graph Γ. Let g be a site operator or face operator. By Lemma 10, we know that $\mathrm{supp}(g) = \cup_{i \in k_g} \mathrm{supp}(m_i^g)$, for some minimal elements $\{m_1^g, \ldots, m_{k_g}^g\} \subset S(Q)$. Let $\omega = \mathrm{supp}(m_i^g)$, then we have that $A_\omega^S(Q) = 1$. Now computing ρ_ω as given by (14) we have

$$\rho_\omega = \frac{1}{2} \sum_{\substack{s \in S(Q) \\ \mathrm{supp}(s) \subseteq \omega}} s = \frac{1}{2} \left(\mathrm{Tr}_{\bar{\omega}}(I) + \mathrm{Tr}_{\bar{\omega}}(m_i^g) \right).$$

By Lemma 12, $\rho_\omega = U_\omega \rho_\omega U_\omega^\dagger$ i.e.,

$$\frac{1}{2} \left(\mathrm{Tr}_{\bar{\omega}}(I) + \mathrm{Tr}_{\bar{\omega}}(m_i^g) \right) = \frac{1}{2} \left(\mathrm{Tr}_{\bar{\omega}}(I) + U_\omega \mathrm{Tr}_{\bar{\omega}}(m_i^g) U_\omega^\dagger \right)$$

and we obtain $\mathrm{Tr}_{\bar{\omega}}(m_i^g) = U_\omega \mathrm{Tr}_{\bar{\omega}}(m_i^g) U_\omega^\dagger$. Since m_i^g has no support outside ω we can conclude that $m_i^g = U m_i^g U^\dagger$.

We have shown so far that any transversal encoded gate of Q maps every minimal operator whose support lies in the support of a site or face operator to itself under conjugation. We now show that this restriction implies that U must be such that every U_i is a Clifford unitary. If U is a non-Clifford encoded gate, then there exists a $j \in \{1, 2, \ldots, n\}$ such that $U_j \notin \mathcal{K}_1$.

By Lemma 10, there exist a site operator A_v and a face operator B_f such that $j \in \mathrm{supp}(A_v) \cap \mathrm{supp}(B_f)$. This implies the existence of an X-only minimal operator g and a Z-only minimal operator h such that $UgU^\dagger = g$ and $UhU^\dagger = h$. Hence,

$$U_j g_j U_j^\dagger \propto g_j \text{ and } U_j h_j U_j^\dagger \propto h_j, \text{ up to a scalar.}$$

Since g is an X-only operator $g_j = X$ and h a Z-only operator $h_j = Z$. This implies that

$$U_j X U_j^\dagger \propto X \text{ and } U_j Z U_j^\dagger \propto Z, \text{ up to a scalar.}$$

Thus $U_j \in \mathcal{K}_1$ contrary to the assumption that it is not in $\mathcal{K}_1$. Thus there exists no transversal encoded non-Clifford gate for the surface codes under the assumptions stated. $\qquad \square$

VI. MATROIDS AND SURFACE CODE STATES

Matroids are useful mathematical structures that find applications in many areas such as graph theory, optimization, error-correcting codes, cryptography. However, matroids are yet to find comparable applications in quantum information theory. One of our goals is to characterize surface code states in terms on matroids. With the results of Section V in hand we make the connection to matroids by showing how to associate a matroid to every CSS surface code state. We call matroids arising from CSS surface code states "surface code matroids". Two key operations on matroids are deletion and contraction. We show that the matroids that are obtained by these minor operations are also surface code matroids in that they can be associated to surface code states. The surface code matroids are in this sense minor closed and can be characterized in terms of a list of excluded minors. We refer the reader to [9] for an introduction to matroids.

A. Surface Code Matroids

Having defined surface code states, we now associate a matroid to a surface code state $|\psi_\Gamma\rangle$ in a canonical fashion. Recall that a CSS surface code state is stabilized by

$$S(\psi_\Gamma) = \left\langle A_v, B_f, \overline{X}_1, \ldots, \overline{X}_l, \overline{Z}_{l+1}, \ldots, \overline{Z}_k \middle| \begin{matrix} v \in V(\Gamma) \\ f \in F(\Gamma) \end{matrix} \right\rangle,$$

where we assume that the encoded X operators $\overline{X}_i$ are X-only operators and the encoded Z operators $\overline{Z}_i$ are Z-

only operators. In matrix form $S = \begin{bmatrix} S_X & 0 \\ 0 & S_Z \end{bmatrix}$. Since a CSS stabilizer state is completely determined by S_X or S_Z, we can define the CSS surface code states in terms of $\{A_v \mid v \in V(\Gamma)\} \cup \{\overline{X}_1, \ldots, \overline{X}_l\}$ or $\{B_f \mid f \in F(\Gamma)\} \cup \{\overline{Z}_{l+1}, \ldots, \overline{Z}_k\}$. Let the vertex-edge incidence matrix of Γ be $\mathbb{I}_{V(\Gamma)}$. Denote by $\mathfrak{C}(\Gamma)$ the cycles of Γ. If $B \subseteq \mathfrak{C}(\Gamma)$, the we denote its edge incidence matrix by $\mathbb{I}_B$. The supports of the encoded X and encoded Z operators are cycles in Γ^* and Γ respectively. Denote by $C(\Gamma^*)$, the cycles in Γ^* that correspond to $\{\overline{X}_1, \ldots, \overline{X}_l\}$. We can write S_X in terms of these incidence matrices as

$$S_X = \begin{bmatrix} \mathbb{I}_{C(\Gamma^*)} \\ \mathbb{I}_{V(\Gamma)} \end{bmatrix}, \tag{15}$$

where $C(\Gamma^*) \subseteq \mathfrak{C}(\Gamma^*)$. The surface code matroid of $|\psi_\Gamma\rangle$ is defined as the vector matroid of S_X and we shall denote it as $\mathcal{M}(\psi_\Gamma)$. In other words, $\mathcal{M}(\psi_\Gamma)$ is determined by all the trivial cycles of Γ^* and a subset of the nontrivial cycles of Γ^*. Note that $\mathbb{I}_{V(\Gamma)}$ contains some dependent rows. However, the matroid associated does not change when we add dependent rows to the matrix representing the matroid.

The vector matroid associated to S_Z is the dual matroid of the vector matroid of S_X. Since S_Z is determined by $\{B_f \mid \in F(\Gamma)\} \cup \{\overline{Z}_{l+1}, \ldots, \overline{Z}_k\}$, by duality we see that

$$\mathcal{M}(\psi_\Gamma)^* = \begin{bmatrix} \mathbb{I}_{C'(\Gamma)} \\ \mathbb{I}_{V(\Gamma^*)} \end{bmatrix}, \tag{16}$$

where $C'(\Gamma)$ is a subset of $\mathfrak{C}(\Gamma)$.

Lemma 14. *Let $\mathcal{M}(\psi_\Gamma)$ be a surface code matroid with ground set $E(\Gamma)$. Then any minor of $\mathcal{M}(\psi_\Gamma)$ is also a surface code matroid. Furthermore,*
a. $\mathcal{M}(\psi_\Gamma) \setminus e = \mathcal{M}(\psi_{\Gamma \setminus e})$
b. $\mathcal{M}(\psi_\Gamma)/e = \mathcal{M}(\psi_{\Gamma/e})$
where $|\psi_{\Gamma \setminus e}\rangle$ and $\psi_{\Gamma/e}$ are some surface code states of $\Gamma \setminus e$ and Γ/e respectively.

Proof. Since M is a surface code matroid, there exists a graph Γ embedded on some surface Σ, such that the surface code matroid $\mathcal{M}(\psi_\Gamma)$ can be represented as

$$\mathcal{M}(\psi_\Gamma) = \begin{bmatrix} \mathbb{I}_{C(\Gamma^*)} \\ \mathbb{I}_{V(\Gamma)} \end{bmatrix},$$

where $C(\Gamma^*)$ is some subset of the nontrivial (homological) cycles of $\mathfrak{C}(\Gamma^*)$. We shall show that both the matroid deletion and contraction operations on $\mathcal{M}(\psi_\Gamma)$ result in surface code matroids. First let us consider the deletion operation. This corresponds to the deletion of a column of $\mathcal{M}(\psi_\Gamma)$. We show that this is equivalent to the deletion of the edge associated to that column. Without loss of generality assume that the first column is deleted. Assume that this column is associated to the edge e in Γ. Deleting the column corresponding to e, the matrix $I_{V(\Gamma)}$

gives the incidence matrix of $\mathbb{I}_{V(\Gamma \setminus e)}$. Deleting an edge in Γ corresponds to contracting an edge in Γ^*, see Lemma 3. So any cycle $c \in C(\Gamma^*)$ that contains e continues to be a cycle in Γ^*/e unless c is a coloop. If c is a coloop, then contracting e removes the row corresponding to c in $I_{C(\Gamma^*)}$ The cycles in $C(\Gamma^*)$ are also in Γ^*/e which is obtained by contracting the edge e in Γ^*. Denote this subset of cycles in Γ^*/e by $C(\Gamma^*/e)$. In either case deleting the column in $I_{C(\Gamma^*)}$ gives a matrix which is the incidence matrix of cycles in $C(\Gamma^*/e)$. Since $\Gamma^*/e = (\Gamma \setminus e)^*$, $\mathcal{M}(\psi_\Gamma) \setminus e$ can be identified with

$$\mathcal{M}(\psi_\Gamma) \setminus e = \begin{bmatrix} \mathbb{I}_{C(\Gamma^*/e)} \\ \mathbb{I}_{V(\Gamma \setminus e)} \end{bmatrix} = \begin{bmatrix} \mathbb{I}_{C((\Gamma \setminus e)^*)} \\ \mathbb{I}_{V(\Gamma \setminus e)} \end{bmatrix} = \mathcal{M}(\psi_{\Gamma \setminus e}),$$

which shows that the $\mathcal{M}(\psi_\Gamma) \setminus e$ is a surface code matroid.

Next let us consider the matroid contraction of $\mathcal{M}(\psi_\Gamma)$. This corresponds to a projection of the matrix representing $\mathcal{M}(\psi_\Gamma)$ by removing a column as well as a row. If e is not a loop, then it is incident on two vertices u and v and the incidence matrix $\mathbb{I}_{V(\Gamma)}$ contains precisely two rows r_u and r_v that have a '1' in the column corresponding to e. We can replace one of the rows say r_v by their sum $r_u + r_v$. Then this row corresponds to the incidence vector of the vertex obtained by contracting along e. The remaining row r_u corresponds a cycle c in Γ^*. Suppose there is a cycle c' in $C(\Gamma^*)$ such that it contains e, then this cycle can be replaced by another cycle c'' that is obtained by the combination of c and c'. This does not affect $\mathcal{M}(\psi_\Gamma)$, therefore we can assume that all the cycles in $C(\Gamma^*)$ do not contain e. Hence, the cycles in $C(\Gamma^*)$ are also in $\Gamma^* \setminus e$ which is obtained by deleting the edge e in Γ^*. The matroid minor $\mathcal{M}(\psi_\Gamma)/e$ is obtained by removing the row r_u in $\mathcal{M}(\psi_\Gamma)$ and deleting the column corresponding to e, which is now all zero except in the row r_u, because of the elimination operations performed earlier.

Suppose that e is a loop, then the column corresponding to e in $\mathbb{I}_{V(\Gamma)}$ is an all zero column. If all the cycles in $C(\Gamma^*)$ do not contain e, then this column is all zero column and we can simply delete it. Therefore, we have $\mathcal{M}(\psi_\Gamma)/e = \mathcal{M}(\psi_{\Gamma \setminus e}) = \mathcal{M}(\psi_{\Gamma/e})$, where we used the fact that $\Gamma \setminus e = \Gamma/e$, when e is a loop. On the other hand if some cycle $c \in C(\Gamma^*)$ contains e, then we replace every other cycle c' in $C(\Gamma^*)$ that contains e by another cycle c'' such that the row space of $\mathbb{I}_{C(\Gamma^*)}$ does not change. At this point only one cycle in $C(\Gamma^*)$ contains e. Denote these cycles that do not contain e as $C(\Gamma^* \setminus e)$. We obtain $\mathcal{M}(\psi_\Gamma)/e$ by removing the row corresponding to c and deleting the column corresponding to e.

Whether e is loop or not, on contracting the edge e, $\mathbb{I}_{V(\Gamma)}$ gives $\mathbb{I}_{V(\Gamma/e)}$, the vertex-edge incidence matrix of Γ/e, while $\mathbb{I}_{C(\Gamma^*)}$ gives $\mathbb{I}_{C(\Gamma^* \setminus e)}$, cycle-edge incidence matrix of $C(\Gamma^* \setminus e)$. Thus the matroid minor $\mathcal{M}(\psi_\Gamma)/e$ is given by

$$\mathcal{M}(\psi_\Gamma)/e = \begin{bmatrix} \mathbb{I}_{C(\Gamma^* \setminus e)} \\ \mathbb{I}_{V(\Gamma/e)} \end{bmatrix} = \begin{bmatrix} \mathbb{I}_{C((\Gamma/e)^*)} \\ \mathbb{I}_{V(\Gamma/e)} \end{bmatrix} = \mathcal{M}(\psi_{\Gamma/e}).$$

This completes the proof that the minor of a surface code matroid is also a surface code matroid. $\square$

A family of matroids $\mathcal{F}$ is said to be minor closed, if every minor of a matroid in $\mathcal{F}$ is also in $\mathcal{F}$. The preceding Lemma, therefore gives us the following result.

Corollary 15. *Surface code matroids are minor closed family of matroids.*

Corollary 15 establishes a connection with an important, albeit difficult, problem in matroid theory. A consequence of the structure theory of binary matroids is that any class of minor closed binary matroids is characterized by a finite set of excluded minors [4]. Thus all CSS surface code states can be characterized by a finite set of CSS states. However, finding these CSS states or equivalently the excluded minors of the surface code matroids appears to be a difficult task. Fortunately, for some restricted classes we can do so and derive some useful results.

B. A Class of Surface Code Matroids

In conjunction with Corollary 15 we can state Theorem 11 in a slightly more useful way in that we can eliminate many CSS stabilizer states from being counterexamples to the LU-LC conjecture. Some of the surface code matroids can be related to well studied classes of matroids, namely graphic and cographic matroids. A binary matroid is graphic if and only if it does not have a minor in the set $\{F_7, F_7^*, \mathcal{M}^*, \mathcal{M}^*(K_5), \mathcal{M}^*(K_{3,3})\}$, where F_7 and F_7^* are the Fano matroid and its dual; $\mathcal{M}(K_5)$, and $\mathcal{M}(K_{3,3})$ are the matroids of the complete graph K_5 and complete bipartite graph $K_{3,3}$ while $\mathcal{M}^*(K_5)$, and $\mathcal{M}^*(K_{3,3})$ are their dual matroids; definitions of these matroids can be found in [10].

Let Γ be a graph and as before denote by $\mathfrak{C}(\Gamma)$ the set of all cycles of Γ and let $\mathbb{I}_{V(\Gamma)}$ be the vertex-edge incidence matrix of Γ. The rowspace of $I_{V(\Gamma)}$ is called the cut space of Γ. The incidence matrix of all the cycles of Γ is denoted as $\mathfrak{C}(\Gamma)$. The row space of $\mathbb{I}_{\mathfrak{C}(\Gamma)}$ is called the flow space of Γ. The cut space and the flow space of Γ are orthogonal to each other, more precisely $\mathbb{I}_{V(\Gamma)}\mathbb{I}_{\mathfrak{C}(\Gamma)}^t = 0$. The supports of site operators form a spanning set for the cut space, while the supports of the face operators and the encoded Z-operators are a spanning set for the flow space. Since $\mathbb{I}_{V(\Gamma)}$ and $\mathbb{I}_{\mathfrak{C}(\Gamma)}$ are orthogonal we can define a stabilizer code with the stabilizer matrix

$$S = \left[\begin{array}{c|c} B(C) & \mathbf{0} \\ \hline \mathbf{0} & B(F) \end{array} \right], \qquad (17)$$

where $B(C)$ is a basis of the cut space and $B(F)$ is a basis of the flow space. Such stabilizer states are sometimes called cut-flow states. A cut-flow state is precisely the CSS surface code state that is stabilized by site operators,

the face operators and the encoded Z operators. In other words

$$S = \langle A_v, B_f, \overline{Z}_1, \ldots, \overline{Z}_g \mid v \in V(\Gamma), f \in F(\Gamma) \rangle.$$

The key observation is that the vector matroid associated to $\mathbb{I}_{V(\Gamma)}$ is precisely the cycle matroid of Γ and denoted as $\mathcal{M}(\Gamma)$. In other words, $\mathcal{M}(\Gamma)$ is a surface code matroid that is also a cycle matroid. The vector matroid associated to $\mathbb{I}_{\mathfrak{C}(\Gamma)}$ is called the bond matroid of Γ and denoted as $\mathcal{M}^*(\Gamma)$. The matroids $\mathcal{M}(\Gamma)$ and $\mathcal{M}^*(\Gamma)$ are duals of each other.

Theorem 11 implies the following corollary that makes a useful connection to binary matroids.

Corollary 16. *Let C be an $[n, k, d \geq 3]_2$ classical code with dual distance $d^\perp \geq 3$. Let $|C\rangle = \sum_{c \in C} |c\rangle$ be the CSS stabilizer state derived from C with the stabilizer matrix $S = \left[\begin{array}{c|c} G & \mathbf{0} \\ \hline \mathbf{0} & H \end{array} \right]$, where G and H are the generator and parity check matrices of C. If the vector matroid associated to G is either graphic or cographic, then $|C\rangle$ cannot be a counterexample to the LU-LC conjecture.*

Proof. We note that the matroids associated to G and H are dual to each other. If the vector matroid of G is graphic, then there exists a graph Γ and a surface Σ on which Γ can be embedded such that the cycle matroid of Γ is the vector matroid of G. Since the bond matroid of Γ is the dual of cycle matroid, it is given by the vector matroid of H. It follows that $|C\rangle$ is a cut-flow state. Since $d \geq 3$ and $d^\perp \geq 3$, it follows that Γ does not have cycles or cocycles of length ≤ 2; thus Theorem 11 is applicable to $|C\rangle$. Therefore, $\mathrm{LU}(|\mathrm{C}\rangle) = \mathrm{LC}(|\mathrm{C}\rangle)$ and $|C\rangle$ cannot be a counterexample to the LU-LC conjecture.

Similarly, if the vector matroid of G is cographic, then vector matroid of H is graphic and we can conclude that the state stabilized by $\left[\begin{array}{c|c} H & \mathbf{0} \\ \hline \mathbf{0} & G \end{array} \right]$ cannot be counterexample to the LU-LC conjecture. But this state is local Clifford equivalent to $|C\rangle$, therefore $|C\rangle$ cannot be a counterexample either. $\square$

Corollary 16 gives us a very simple test to rule a large class of CSS stabilizer states, in particular all the cut-flow states. So to test whether a given code C can give rise to a counterexample we simply have to test if the associated matroid is graphic or cographic. Graphic and cographic matroids are characterized by finite number of excluded minors. In Corollary 16 we test to see if G or H are graphic. This test can be performed in polynomial time for binary matroids, see [15].

Further, Corollary 16 implies that a CSS counterexample for the LU-LC conjecture must necessarily be induced by a nongraphic and noncographic matroid. However, a CSS stabilizer state whose associated matroid is neither graphic nor cographic is not necessarily a counterexample to the LU-LC conjecture. An interesting albeit difficult

problem would be to find the excluded minors of the surface code matroids as it would give a sufficient condition for a general CSS state to be ruled out as a counterexample.

While these associations with matroids are interesting we note that the matroids whose CSS states are LU-LC equivalent are not minor closed. However, characterizing the largest class of matroids which are minor closed might be an interesting problem and provide an insight into those states which preserve this property.

VII. SUMMARY

In this paper we have have given a constructive method to compose new counterexamples for the LU-LC conjecture. We have also investigated the equivalence classes of two important classes of stabilizer states–the surface code states and cluster states. This allows us to rule out the existence of encoded non-Clifford transversal gates for surface codes. Additionally, we have been able to make a connection with the theory of binary matroids, opening the possibility to approach this topic from a different vantage point.

Acknowledgment

[1] S. Bravyi and A. Y. Kitaev. Quantum codes on a lattice with boundary. eprint: quant-ph/9811052, 1998.

[2] J. Dehaene and B. De Moor. Clifford group, stabilizer states, and linear and quadratic operations over GF(2). *Physical Review A*, 68(042318), 2003.

[3] B. Eastin and E. Knill. Restrictions on transversal encoded quantum gate sets. *Phys. Rev. Lett.*, 102(110502), 2009.

[4] J. Geelen. Binary matroid minors. Applications of Matroid Theory and Combinatorial Optimization to Information and Coding Theory. [Online] http://robson.birs.ca/~09w5103/geelen_09w5103_talk.pdf, 2009.

[5] M. Hein, J. Eisert, and H. J. Briegel. Multiparty entanglement in graph states. *Physical Review A*, 69(062311), 2004.

[6] Z. Ji, J. Chen, Z. Wei, and M. Ying. The LU–LC conjecture is false. arXiv:0709.1266, 2008.

[7] A.Y. Kitaev. Fault-tolerant quantum computation by anyons. *Annals. of Physics*, 303:2–30, 2003.

[8] I. Niven, H. S. Zuckerman, and H. L. Montgomery. *An Introduction to the Theory of Numbers*. John Wiley & Sons, Inc., New York, 2001.

[9] J. Oxley. What is a matriod? [Online] http://www.math.lsu.edu/~oxley/survey4.pdf, 2004.

[10] J. G. Oxley. *Matroid Theory*. Oxford University Press, New York, 1992.

[11] E.M. Rains. Nonbinary quantum codes. *IEEE Trans. Inform. Theory*, 45:1827–1832, 1999.

[12] E.M. Rains. Quantum codes of minimum distance two. *IEEE Trans. Inform. Theory*, 45(1):266–271, 1999.

[13] R. Raussendorf and H. Briegel. Quantum computing via measurements only. *Phys. Rev. Lett.*, 86(5188), 2001.

[14] D. Schlingemann. Local equivalence of graph states. In O. Krueger and R. F. Werner, Some Open Problems in Quantum Information Theory, arXiv:quant-ph/0504166, 2005.

[15] W. T. Tutte. An algorithm for determining whether a given binary matroid is graphic. *Proceedings of the American Mathematical Society*, 11(6):905–917, 1960.

[16] M. van den Nest, J. Dehaene, and B. De Moor. An efficient algorithm to recognize local Clifford equivalence of graph states. *Physical Review A*, 70(034302), 2004.

[17] M. van den Nest, J. Dehaene, and B. De Moor. Local unitary versus local Clifford equivalence of stabilizer states. *Physical Review A*, 71(062323), 2005.

[18] M. van den Nest and D. Gross. The LU–LC conjecture, diagonal local operations and quadratic forms over GF(2). *Quantum Information and Computation*, 8:263–281, 2008. arXiv:0707.4000.

[19] B. Zeng, H. Chung, A. W. Cross, and I. L. Chuang. Local unitary versus local Clifford equivalence of stabilizer and graph states. *Physical Review A*, 75(032325), 2007.

[20] B. Zeng, A. Cross, and I. L. Chuang. Transversality and universality for additive quantum codes. arXiv:0706.1382, 2007.

[21] Up to a scalar.

[22] Topologically, the surface is the union of the faces and the graph (the vertices and the edges) since the edges and the vertices do not belong to the faces.

[23] Transversal gates can also be defined for more than one block of a code, but we will not need these general transversal gates in this paper.

[24] The action of $\text{diag}(1, e^{i\theta})$ on $\mathcal{P}_1$ is to fix I and Z while $X \mapsto \text{diag}(e^{-i\theta}, e^{i\theta})X$ and $Y \mapsto \text{diag}(e^{-i\theta}, e^{i\theta})Y$. Since the diagonal unitaries are non-Clifford, $\theta_i \notin \langle \pi/2 \rangle$, the only way we can ensure that the minimal elements remain within the Pauli group is to enforce that minimal elements consist of only Z-operators.

[25] A minimal element of C is a codeword $c \in C$ such that there is no nonzero codeword x in C such that $\text{supp}(x) \subsetneq \text{supp}(c)$.

[26] Recall that two elements of the Pauli group commute if and only if their binary representations say $(a|b)$, $(c|d)$ are orthogonal with respect to the symplectic inner product, i.e., $a \cdot d + b \cdot c = 0$.

[27] This is modulo sign. Recall that the action of Clifford group on a single qubit can be identified with the group of nonsingular 2×2 matrices over $\mathbb{F}_2$.