Quantum Graph-State Synthesis with SAT

Sebastiaan Brand[1,*], Tim Coopmans[1] and Alfons Laarman[1]

[1]Leiden Institute of Advanced Computer Science, Leiden University, The Netherlands

Abstract

In quantum computing and quantum information processing, graph states are a specific type of quantum states which are commonly used in quantum networking and quantum error correction. A recurring problem is finding a transformation from a given source graph state to a desired target graph state using only local operations. Recently it has been shown that deciding transformability is already NP-hard. In this paper, we present a CNF encoding for both local and non-local graph state operations, corresponding to one- and two-qubit Clifford gates and single-qubit Pauli measurements. We use this encoding in a bounded-model-checking set-up to synthesize the desired transformation. For a completeness threshold, we provide an upper bound on the length of the transformation if it exists. We evaluate the approach in two settings: the first is the synthesis of the ubiquitous GHZ state from a random graph state where we can vary the number of qubits, while the second is based on a proposed 14 node quantum network. We find that the approach is able to synthesize transformations for graphs up to 17 qubits in under 30 minutes.

Keywords

Quantum computing, graph states, bounded model checking

1. Introduction

The creation, manipulation and transmission of quantum information brings into reach applications which are unfeasible or even impossible using classical computers, such as provably-secure communication [1, 2], more accurate clock synchronization [3], and chemistry applications [4]. Various questions regarding simulation, modeling and design of quantum computers and networks can be phrased using graph states, a subset of all possible states of a register of quantum bits (qubits) which can be described using graphs [5]. Additionally, graph states are crucial to a universal model of quantum computation called measurement-based quantum computing [6]. Furthermore, when augmented with a finite set of quantum operations called Clifford gates and single-qubit Pauli measurements, the graph-state formalism gives rise to efficient classical simulation of a large class of quantum circuits [7] and forms the basis for many quantum error correction schemes [8], a prerequisite for scaling up quantum computing with imperfect devices, as well as many quantum-networking applications [9, 5]. These applications have a focus on *local* quantum operations, i.e. on a single or few spatially-close qubits, for reasons regarding experimental implementation with imperfect devices.

14th International Workshop on Pragmatics of SAT (PoS 2023)

*Corresponding author.

s.o.brand@liacs.leidenuniv.nl (S. Brand); t.j.coopmans@liacs.leidenuniv.nl (T. Coopmans); a.w.laarman@liacs.leidenuniv.nl (A. Laarman)

0000-0002-7666-2794 (S. Brand); 0000-0002-9780-0949 (T. Coopmans); 0000-0002-2433-4174 (A. Laarman)

Given this wide applicability, graph-state transformations have been extensively studied from the theory standpoint for various sets of allowed local quantum operations [10, 11, 12, 13, 5, 14]. In this work, we specifically consider the following problem: given a source graph state, synthesize a desired target graph state using single-qubit Clifford gates and single-qubit Pauli measurement. This problem was shown before [15] to be equivalent to transforming the associated graphs under two graph operations: an edge-toggling operation called *local complementation* (LC), corresponding to single-qubit Cliffords, and *vertex deletion* (VD), corresponding to measurements. The decision problem (can a source graph be transformed to a target graph under LC+VD?) has been shown to be NP-complete [16], even when restricting the target graph to a practically-relevant scenario [17]. Although there exists an algorithm [15] (based on techniques from [18, 19]) which is fixed-parameter tractable (FPT) in the rank-width r of the graph, the authors of the algorithm themselves remark it is not useful in practice due to a giant FPT-prefactor equalling ten times repeated exponentiation with base 2 (i.e. $2^{2^{\cdots 2^{r}}}$) [16].

We tackle the problem of graph-state synthesis under LC+VD with bounded model checking (BMC) [20, 21]. To this end we present a Boolean encoding for graph states and the operations on them, and provide a completeness threshold for this problem. We also give an encoding for two-qubit graph operations, which together with single-qubit operations enable all possible Clifford operations [14]. This approach can be applied to arbitrary graphs, in contrast to special cases for which poly-time algorithms have been found [16, 22] or unsatisfiability can be determined analytically [23, 24]. We evaluate this approach in two settings of particular interest [16, 24]: first, we synthesize the ubiquitous Greenberger–Horne–Zeilinger (GHZ) state [25] from random graphs with varying number of qubits. Next, we target a 14 node quantum network proposal [26]. Within 30 minutes BMC finds transformations for graphs up to 17 nodes (qubits). In comparison, for transformations under single-qubit Clifford operations without measurements (a setting where deciding reachability is in P [27, 28] and counting reachable graphs is #P-complete [29]), various properties of equivalence classes have been explored up to 12 qubits [30, 31, 32].

Aside from graph problems which have been tackled with SAT-based methods [33, 34, 35, 36, 37, 38, 39, 40], SAT has also been used on problems in quantum computing. For example, synthesizing optimal Clifford circuits without measurements (closely related to graph-state synthesis under LC + flipping arbitrary edges, but without VD) has been tackled with BMC [41]. Without the optimality constraint (i.e. shortest circuit) this problem is in P [42], while the complexity with the optimality constraint is unknown. SAT-based techniques have also been applied to quantum circuit equivalence checking for a limited selection of circuits [43]. BMC specifically has been applied to Clifford circuit (without measurements) equivalence checking [44] (a problem that is also in P [45]), and SMT and planning based approaches have been used to map logical quantum circuits to physical quantum-chips [46, 47]. Unlike much previous work we include measurements, which for our problem raises the complexity from P to NP-complete.

2. Preliminaries and problem definition

2.1. Quantum computing

We very briefly introduce quantum bits (qubits) and how to act on them with quantum gates and measurements (see [48] for a complete introduction). The state $|\psi\rangle$ of a single qubit is a complex 2-vector of unit norm, equalling the *computational-basis states* $|0\rangle = \begin{pmatrix}1 & 0\end{pmatrix}^\intercal$ or $|1\rangle = \begin{pmatrix}0 & 1\end{pmatrix}^\intercal$ or any linear combination of those, i.e. in general a single-qubit state is $|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle = \begin{pmatrix}\alpha_0 & \alpha_1\end{pmatrix}^\intercal$ for complex numbers α_0, α_1 satisfying $|\alpha_0|^2 + |\alpha_1|^2 = 1$ (here, $\intercal$ denotes vector transposition). A general n-qubit quantum state is represented as a complex vector of length 2^n with norm 1, e.g. $\begin{pmatrix}\frac{1}{\sqrt{2}} & \frac{i}{\sqrt{2}}\end{pmatrix}^\intercal$ and $\begin{pmatrix}\frac{2}{\sqrt{13}} & 0 & 0 & \text{-}\frac{3}{\sqrt{13}}\end{pmatrix}^\intercal$ are quantum states. The joint state of two separate quantum registers in states $|\phi\rangle, |\psi\rangle$ is $|\phi\rangle \otimes |\psi\rangle$, where $\otimes$ denotes the tensor product: given $r_V \times c_V$ matrix V and $r_W \times c_W$ matrix W, the $r_V r_W \times c_V c_W$ matrix $V \otimes W$ is

$$V \otimes W = \begin{pmatrix} V_{00}W & V_{01}W & \dots & V_{0c_V}W \\ \vdots & \vdots & \ddots & \\ V_{r_V0}W & V_{r_V1}W & \dots & V_{r_Vc_V}W \end{pmatrix}.$$

Given a bipartition $A \cup B = \{1, 2, \dots, n\}$, an n-qubit state $|\psi\rangle$ is called *separable over* A, B if we can write $|\psi\rangle = |\varphi\rangle_A \otimes |\phi\rangle_B$. It is *entangled* otherwise, a feature that has no classical analogue and is a prerequisite to many applications with a quantum advantage. For example $\begin{pmatrix}\frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0\end{pmatrix}^\intercal = \begin{pmatrix}\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\end{pmatrix}^\intercal \otimes \begin{pmatrix}1 & 0\end{pmatrix}^\intercal$ is not entangled, but $\begin{pmatrix}\frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}}\end{pmatrix}^\intercal$ is.

$$I = \begin{pmatrix}1 & 0 \\ 0 & 1\end{pmatrix} \quad T = \begin{pmatrix}1 & 0 \\ 0 & e^{i\pi/4}\end{pmatrix}$$

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1 \\ 1 & \text{-}1\end{pmatrix}$$

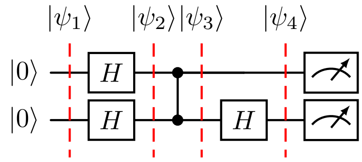
$$CZ = \begin{pmatrix}1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \text{-}1\end{pmatrix}$$

A quantum gate (always reversible) on n qubits is given by a $2^n \times 2^n$ unitary matrix and the output state can be found by matrix-vector multiplication, for example H (see right) which maps input $\begin{pmatrix}1 \\ 0\end{pmatrix}$ to output $\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1 \\ 1 & \text{-}1\end{pmatrix} \cdot \begin{pmatrix}1 \\ 0\end{pmatrix} = \begin{pmatrix}\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}}\end{pmatrix}$. An example universal gate set is shown on the right. The tensor product is used to apply gates in parallel to separate registers, e.g. $I \otimes H \otimes I$ is a 3-qubit gate performing a H on the second qubit and I on the first and third. The result of a two-qubit gate (e.g. controlled-Z (CZ), which maps e.g. $\begin{pmatrix}\frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}}\end{pmatrix}^\intercal$ to $\begin{pmatrix}\frac{1}{\sqrt{2}} & 0 & 0 & \text{-}\frac{1}{\sqrt{2}}\end{pmatrix}^\intercal$) between two non-adjacent qubits can be computed by swapping qubits: e.g. for qubits q_0, q_1, q_2, $CZ(q_0, q_2) = \text{SWAP}(q_1, q_2)CZ(q_0, q_1)\text{SWAP}(q_1, q_2)$, where $\text{SWAP}(q_1, q_2)$ replaces $|a\rangle \otimes |b\rangle \otimes |c\rangle \to |a\rangle \otimes |c\rangle \otimes |b\rangle$ for $a, b, c \in \{0, 1\}$. The gates H, T^2 together generate (under matrix multiplication and tensoring with I) the group of *single-qubit Clifford gates*, and H, T^2, CZ together generate all Clifford gates.

A computational-basis measurement is a non-reversible operation which projects a single qubit state $\alpha_0 |0\rangle + \alpha_1 |1\rangle$ to one of $|0\rangle, |1\rangle$ with probability $|\alpha_0|^2$ or $|\alpha_1|^2$. For example, measuring a qubit $|\psi\rangle = \sqrt{1/3}\,|0\rangle + \sqrt{2/3}\,|1\rangle$ yields the state $|0\rangle$ with probability $1/3$ and the state $|1\rangle$ with probability $2/3$. Any n-qubit state $|\psi\rangle$ can be written as $|\psi\rangle = \alpha |0\rangle \otimes |\psi_0\rangle + \beta |1\rangle \otimes |\psi_1\rangle$ where $|\alpha|^2$ ($|\beta|^2$) is the probability of finding the first qubit in the $|0\rangle$ ($|1\rangle$) state after measuring it (for expressing measurement on the other qubits, swap qubits first). A Pauli measurement equals a computational-basis measurement preceded by a single-qubit Clifford gate. Sequences of quantum operations are typically visualized in a quantum circuit (see Fig. 1).

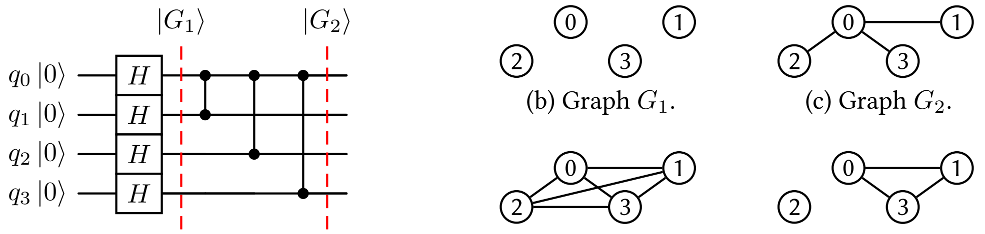
2.2. Graph states and graph-state reachability

Graph states are a subset of all quantum states. An n-qubit graph state $|G\rangle$ is represented by an undirected simple graph $G = (V, E)$ with $|V| = n$ vertices and no self-loops (where V is



$$|\psi_1\rangle = |0\rangle \otimes |0\rangle = |00\rangle$$
$$|\psi_2\rangle = (H \otimes H)\,|\psi_1\rangle = \tfrac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |10\rangle)$$
$$|\psi_3\rangle = CZ\,|\psi_2\rangle = \tfrac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)$$
$$|\psi_4\rangle = (I \otimes H)\,|\psi_3\rangle = \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Figure 1: An example 2-qubit quantum circuit. Operations are applied from left to right. The controlled-Z (CZ) gate is visualized as . As is common, we write $|01\rangle$ as shorthand for $|0\rangle \otimes |1\rangle$, $|01\rangle = |0\rangle \otimes |1\rangle$, etc. Measuring both qubits at the end gives $|00\rangle$ or $|11\rangle$ with equal probability.



(a) Circuit generating $|G_2\rangle$. (b) Graph G_1. (c) Graph G_2. (d) $G_3 = LC_0(G_2)$. (e) $G_4 = VD_2(G_3)$.

Figure 2: The circuit in 2a generates the state $|G_2\rangle$, corresponding to the graph in 2c. Examples of local complementation and vertex deletion are shown in 2d and 2e.

the vertex set and $E \subseteq V \times V$ the edge set), constructed as starting from the state $H^{\otimes n}|0\rangle^{\otimes n}$, followed by a CZ gate on each pair of qubits $(u, v) \in E$. An example is given in Fig. 2. From here on we say 'graph' to mean 'undirected simple graph without self-loops'. Intuitively, the graph G captures information about the entanglement between the qubits, where two qubits are entangled if they are (directly or indirectly) connected in the graph.

The two graph transformations corresponding to single-qubit quantum operations are:

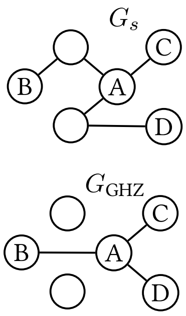
- *Local complementation* LC_k on vertex $k \in V$ transforms $G = (V, E)$ into $LC_k(G) = (V, E')$ where E' is obtained from E by flipping the edges in the neighborhood of k, i.e. for all $u, v \in \mathcal{N}_k$, if $(u, v) \in E$ then $(u, v) \notin E'$ and if $(u, v) \notin E$ then $(u, v) \in E'$. Here, the neighborhood $\mathcal{N}_k$ is the set of all vertices adjacent to k, i.e. $\mathcal{N}_k = \{v \mid (k, v) \in E\}$. For any graphs G and G', $|G'\rangle$ is reachable from $|G\rangle$ using only single-qubit Clifford operations if and only if G' is reachable from G using local complementations. More specifically, the graph state $|LC_k(G)\rangle$ equals the resulting quantum state when applying a certain sequence of single-qubit Clifford operations to $|G\rangle$ (see [10] for details).
- *Vertex deletion* VD_k of vertex $k \in V$ transforms $G = (V, E)$ to $VD_k(G) = (V, E')$ with $E' = E \setminus \{(v, k) \mid v \in V\}$, i.e. k becomes *isolated* (all edges adjacent to k are removed). Vertex deletion of vertex k implements measurement on qubit k: for each graph G, the graph state $|VD_k(G)\rangle$ is single-qubit Clifford equivalent to $|G\rangle$ at which a computational-basis measurement has been performed on qubit k [12].

And although not the primary focus of this work, we can also consider two-qubit operations:

- Given a subset of pairs of nodes $D \subseteq V \times V$ (for convenience $u < v$ for $(u, v) \in D$), G can be transformed into G' by *edge flips* among D and local complementations on vertices in V if and only if $|G\rangle$ can be transformed into $|G'\rangle$ using two-qubit Clifford operations on the qubit pairs in D and single-qubit Clifford on qubits in V [14-Th.1].

Rather than generating a graph state from scratch using CZ gates (as in Figs. 2a to 2c) a problem of interest for e.g. quantum networking is to obtain a particular graph from an existing graph *using only single-qubit operations* (LC+VD, and $D = \emptyset$). Below is a practical example.

Example 2.1. *Alice is part of a 6-node quantum network and wants to run a quantum secret sharing scheme [9] between herself and three other parties, each having one qubit. For this she needs a 4-qubit Greenberger–Horne–Zeilinger (GHZ) state [25], given by G_{GHZ} on the right. However, generating $|G_{GHZ}\rangle$ using CZ-gates (Figs. 2a to 2c)) requires generating entanglement [49, 50-Fig.2.4], which is a time-consuming probabilistic process [51]. At some point in time the network is a state $|G_s\rangle$. Because single-qubit operations (LC+VD on the graph) are much easier to perform than entanglement generation, Alice wants to know whether a given G_s can be transformed into G_{GHZ} using only LC+VD.*



This motivates the problem we will study in this work, posed before in [16] for single-qubit operations (LC+VD and $D = \emptyset$) and in [14] for multi-qubit operations (LC+VD and $D \neq \emptyset$).

Definition 2.1 (Graph-state synthesis)**.** Given source and target graphs $G_s = (V, E_s)$ and $G_t = (V, E_t)$, find (if it exists) a sequence of local complementations and vertex deletions on any $v \in V$ (and also edge flips on $(u, v) \in D$ for some given $D \subseteq V \times V$ in case multi-qubit Clifford operations are allowed on D) which transforms G_s into G_t.

We remark that if $D = V \times V$, any graph can be trivially synthesized because an edge may be added or removed between any pair of nodes (Figs. 2a to 2c). We also remark that we are not necessarily interested in the shortest sequence of graph transformations, as any sequence of LC+VD translates into at most one single-qubit Clifford and one measurement per qubit.

3. SAT encoding

As seen in the previous section, quantum operations on graph states can be expressed through graph transformations. In this section, we give Boolean encodings for these operations, as well as an encoding for the transition relation as a whole. The encoding of a single transformation step from graph G to G' uses variables $\vec{x}$ for G and $\vec{x}'$ for G'. We encode a graph as follows.

Definition 3.1 (Graph encoding)**.** An undirected graph G of n vertices is encoded as a conjunction over $n(n-1)/2$ literals x_{uv} ($\neg x_{uv}$), for $(u, v) \in \mathbb{U} = \{(u, v) \in V \times V \mid u < v\}$, indicating there is (not) an edge between nodes u and v.

3.1. Encoding of graph transformations

The Boolean encoding for deleting a vertex k, denoted VD_k, is given in Eq. (1). All edges (u, v) connected to k are set to false ($\neg x'_{uv}$) while all others remain unchanged ($x'_{uv} \leftrightarrow x_{uv}$).

$$\mathsf{VD}_k = \bigwedge_{(u,v)\in\mathbb{U}} \begin{cases} \neg x'_{uv} & \text{if } u = k \text{ or } v = k \\ x'_{uv} \leftrightarrow x_{uv} & \text{otherwise.} \end{cases} \tag{1}$$

The encoding for performing a local complementation on vertex k, denoted LC_k, is given in Eq. (2) and can be read as follows: if vertices u, v are in the neighborhood of k ($x_{uk} \wedge x_{vk}$) then the value of the edge (u, v) is flipped ($x'_{uv} \leftrightarrow \neg(1 \oplus \neg x_{uv})$.

$$\mathsf{LC}_k = \bigwedge_{(u,v)\in\mathbb{U}} \begin{cases} x'_{uv} \leftrightarrow \neg((x_{uk} \wedge x_{vk}) \oplus \neg x_{uv}) & \text{if } u \neq k \text{ and } v \neq k \\ x'_{uv} \leftrightarrow x_{uv} & \text{otherwise.} \end{cases} \tag{2}$$

To encode edge flips on a selection of edges D (Def. 2.1), we take D to be an indexed set $D = \{(u_1, v_1), (u_2, v_2), \dots\}$ with $u_i < v_i$. Given this indexed set, the constraint in Eq. (3) encodes an edge flip of (u_i, v_i).

$$\mathsf{EF}_i = \bigwedge_{(u,v)\in\mathbb{U}} \begin{cases} x'_{uv} \oplus x_{uv} & \text{if } u = u_i \text{ and } v = v_i \\ x'_{uv} \leftrightarrow x_{uv} & \text{otherwise} \end{cases} \tag{3}$$

In order to combine the transition relations LC_k, VD_k, and EF_i into a single CNF formula we use a construction similar to the BMC encoding of different concurrent threads in [52]: we add $\lceil \log_2(\max(|V|, |D|) + 1)\rceil$ variables $\vec{y}$ for the binary encoding of $k \in V$ or $i \in \{1, \dots, |D|\}$, and two variables $\vec{z}$ to indicate whether a given operation is a local complementation ($\vec{z} = 0$), a vertex deletion ($\vec{z} = 1$), or an edge flip ($\vec{z} = 2$). For example the constraint $\vec{y} = 3 \wedge \vec{z} = 1$ represents vertex deletion of node 3. Using these additional variables, we encode all local complementations, vertex deletions, and edge flips as in Eqs. (4) to (6).

$$R_{\mathsf{LC}}(\vec{x}, \vec{x}') = \bigwedge_{k\in V} \Big[(\vec{y} = k \wedge \vec{z} = 0) \rightarrow \mathsf{LC}_k(\vec{x}, \vec{x}')\Big] \tag{4}$$

$$R_{\mathsf{VD}}(\vec{x}, \vec{x}') = \bigwedge_{k\in V} \Big[(\vec{y} = k \wedge \vec{z} = 1) \rightarrow \mathsf{VD}_k(\vec{x}, \vec{x}')\Big] \tag{5}$$

$$R_{\mathsf{EF}}(\vec{x}, \vec{x}') = \bigwedge_{i\in\{1,\dots,|D|\}} \Big[(\vec{y} = i \wedge \vec{z} = 2) \rightarrow \mathsf{EF}_i(\vec{x}, \vec{x}')\Big] \tag{6}$$

Additionally we add an identity transition $R_{\mathsf{Id}}(\vec{x}, \vec{x}') = (\vec{z} = 3) \rightarrow \mathsf{Id}(\vec{x}, \vec{x}')$ to ensure that if a transformation of length d exists, a transformation of length $d' \geq d$ also exists (to avoid searching over all d), and we appropriately constrain the unused values of $\vec{y}$ and $\vec{z}$ by adding $C = (\vec{y} < |V| \vee z = 2) \wedge (\vec{y} < |D| \vee z \neq 2)$. Finally, we obtain the the global transition relation in Eq. (7). When converted to CNF this formula has $m + n(n-1)$ variables and $\leq 3.5n^3 + 2mn^2 + 0.5n^2 + 0.5|D|n^2$ clauses, where $n = |V|$ and $m = \lceil \log_2(\max(|V|, |D|) + 1)\rceil$.

$$R_{\text{global}}(\vec{x}, \vec{x}') = R_{\mathsf{LC}} \wedge R_{\mathsf{VD}} \wedge R_{\mathsf{EF}} \wedge R_{\mathsf{Id}} \wedge C \tag{7}$$

We use the transition relation specified in Eq. (7) in a bounded-model-checking set-up, i.e. we create Eq. (8) below, where $S(\vec{x}_1)$ encodes a source graph G_s, $T(\vec{x}_d)$ a target graph G_t, and d is the search depth.

$$S(\vec{x}_1) \wedge \bigwedge_{i=1}^{d-1} R_{\text{global}}(\vec{x}_i, \vec{x}_{i+1}) \wedge T(\vec{x}_d) \tag{8}$$

The formula is satisfiable if and only if a sequence of operations of at most d steps exists which transforms G_s into G_t. In Section 3.2, we prove an upper bound on the required depth d.

3.2. Completeness threshold

To provide a completeness threshold for graph-state synthesis under LC+VD, we use the following observations to bound the search depth.

1. If G_s can be transformed to G'_s under LC, a transformation exists of at most M local complementations, where $M = 3(|V| - s)/2$ with $s = |V| (\text{mod } 2)$ [27-§4].
2. If G_s can be transformed into G_t under LC+VD, then vertex deletion needs to be performed on exactly the Δ vertices which are isolated in G_t.[1]
3. For $k \in V$, LC_k after VD_k leaves the graph unchanged, i.e. $LC_k(VD_k(G)) = VD_k(G)$.
4. For $j, k \in V$ and $j \neq k$, LC_j and VD_k commute, i.e. $LC_j(VD_k(G)) = VD_k(LC_j(G))$.

From points 3 and 4, it follows that all vertex deletions (measurements) can be postponed until after the local complementations (single-qubit Clifford gates). We then get that if G_s can be transformed into G_t under LC+VD, it can be transformed by a circuit of the form given in Fig. 3, taking at most M local complementations and Δ vertex deletions.

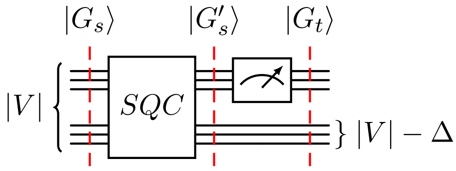


Figure 3: Graph-state transformation circuit under LC+VD.

4. Empirical evaluation

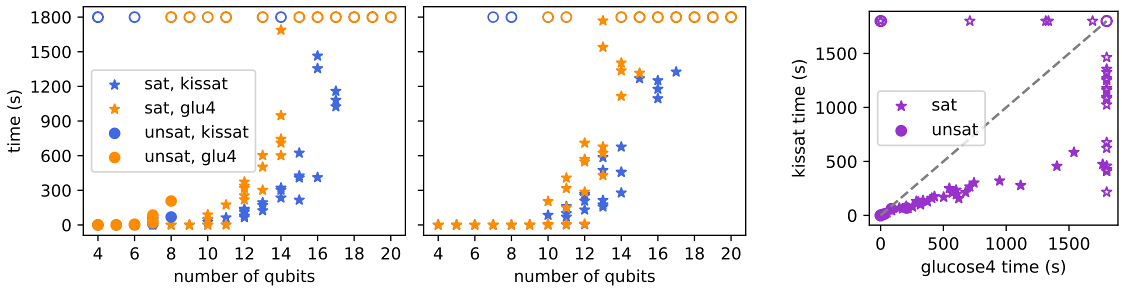
We evaluate our approach in two settings: synthesizing a GHZ state from random graphs for an increasing number of qubits, and synthesis of graphs based on a proposal of a 14 node quantum network in the Netherlands [26]. For all experiments, we perform binary search over d up to the completeness threshold specified in Section 3.2. In our current setup, the solver is restarted for every different d. Experiments[2] were run on Ubuntu 18 with an AMD Ryzen 7 5800x CPU. Two different SAT solvers, Glucose 4 [53] and Kissat [54], have been used.

We first evaluate our approach in a setting where the target states are 4-qubit GHZ states (see Example 2.1), matching the target states in the empirical evaluation in [16]. GHZ states are used in a large number of applications such as quantum secret sharing [9] (see also Example 2.1), anonymous transfer [55] and conference key agreement [56]. The polynomial time algorithm presented in [16] can only be applied when the source graph has special properties (specifically it needs to have rank-width 1). To evaluate our method we replace the restricted random graphs used in [16] with more general Erdős-Rényi random graphs, which have also been used in other work concerning graph-state synthesis [57, 58]. Results are shown in Fig. 4. With a timeout of 30 minutes Kissat can synthesize transformations for graphs up to 17 qubits. Determining unreachability, which we do using the completeness threshold, can be done up to 8 qubits by Glucose within this timeout.

Next, we evaluate our approach on the specific quantum network architecture proposed in [26-Fig.3] (visualized in Fig. 5a). As source states, we consider graphs with nodes from this network, and random edges as follows: $(u, v) \in E$ with probability p^d, where d is the distance

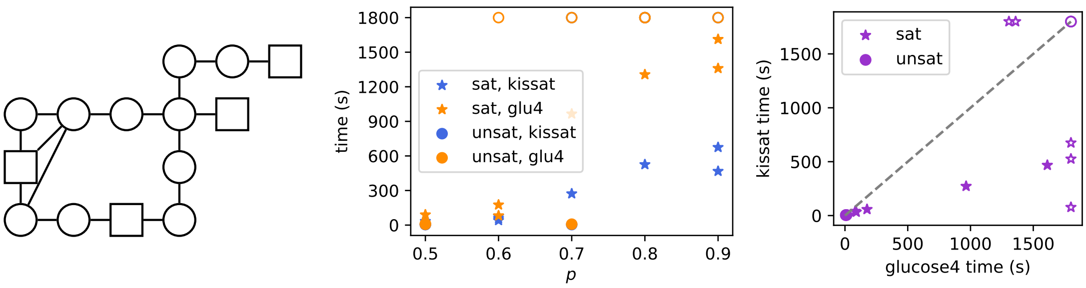
[1] Without loss of generality, we assume G_s has no isolated vertices. If G_s has isolated vertices which are not isolated in G_t, then G_t is trivially unreachable under LC+VD.

[2] Reproducible experiments are available online at https://github.com/sebastiaanbrand/graph-state-synthesis.



(a) Synthesis under LC+VD (left) and LC+VD+limited EF (right)   (b) Solver comparison

Figure 4: The total SAT solver time for BMC with binary search over the depth up the completeness threshold (see Section 3.2). For each number of qubits we run on three Erdős-Rényi random graphs with $p = 0.8$, with a 4-qubit GHZ state as target, with only LC+VD on the left, and LC+VD+EF on a random set D with $|D| = \frac{1}{2}|V|$ on the right. 4b shows the difference between the solvers for the data points from both the left and right plot in 4a. Open symbols indicate timeouts. Solid spheres indicate unreachability at the depth of the completeness threshold. The largest solved instance is for 17 qubits at $d = 16$, which has a formula with ∼2400 variables and ∼300,000 clauses (see above Eq. (7) for $d = 1$).



(a) Network from [26-Fig.3].   (b) Synthesis under LC+VD   (c) Solver comparison

Figure 5: The 14-node quantum network proposed in [26-Fig.3], and the SAT solver time to synthesize a transformation into a GHZ state for different amounts of entanglement (p) in the network. Open circles indicate timeouts. Solid spheres indicate unreachability as at the depth of the completeness threshold.

(number of hops + 1) between the nodes, motivated by the fact that generating entanglement over larger distances is harder [51]. The target state is a GHZ state between the main network nodes (squares in Figure 5a). Fig. 5b shows the results for varying p. A higher p corresponds to a larger amount of entanglement in the network. We observe that for fixed number of nodes, the time it takes to synthesize a transformation increases with the density of the source graph.

Acknowledgments

This work was supported by the NEASQC project, funded by European Union's Horizon 2020, Grant Agreement No. 951821, and by the Dutch National Growth Fund, as part of the Quantum Delta NL programme.

References

[1] C. H. Bennett, G. Brassard, Quantum cryptography: Public key distribution and coin tossing, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing 175 (1984). doi:10.1016/j.tcs.2014.05.025.

[2] A. K. Ekert, Quantum cryptography based on Bell's theorem, Phys. Rev. Lett. 67 (1991) 661–663. URL: http://link.aps.org/doi/10.1103/PhysRevLett.67.661. doi:10.1103/PhysRevLett.67.661.

[3] R. Jozsa, D. S. Abrams, J. P. Dowling, C. P. Williams, Quantum clock synchronization based on shared prior entanglement, Physical Review Letters 85 (2000) 2010.

[4] Y. Cao, J. Romero, J. P. Olson, M. Degroote, P. D. Johnson, M. Kieferová, I. D. Kivlichan, T. Menke, B. Peropadre, N. P. D. Sawaya, S. Sim, L. Veis, A. Aspuru-Guzik, Quantum chemistry in the age of quantum computing, Chemical Reviews 119 (2019) 10856–10915. URL: https://doi.org/10.1021/acs.chemrev.8b00803. doi:10.1021/acs.chemrev.8b00803.

[5] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Nest, H.-J. Briegel, Entanglement in graph states and its applications, arXiv preprint quant-ph/0602096 (2006).

[6] R. Raussendorf, H. J. Briegel, A one-way quantum computer, Phys. Rev. Lett. 86 (2001) 5188–5191. URL: https://link.aps.org/doi/10.1103/PhysRevLett.86.5188. doi:10.1103/PhysRevLett.86.5188.

[7] S. Anders, H. J. Briegel, Fast simulation of stabilizer circuits using a graph-state representation, Physical Review A 73 (2006) 022334.

[8] D. Gottesman, Stabilizer codes and quantum error correction, arXiv:quant-ph/9705052 (1997).

[9] M. Hillery, V. Bužek, A. Berthiaume, Quantum secret sharing, Physical Review A 59 (1999) 1829.

[10] M. Van den Nest, J. Dehaene, B. De Moor, Graphical description of the action of local Clifford transformations on graph states, Phys. Rev. A 69 (2004) 022316. doi:10.1103/PhysRevA.69.022316.

[11] M. Van den Nest, Local equivalence of stabilizer states and codes (phd thesis) (2005).

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

[13] Z. Ji, J. Chen, Z. Wei, M. Ying, The lu-lc conjecture is false, arXiv preprint arXiv:0709.1266 (2007).

[14] M. Englbrecht, T. Kraft, B. Kraus, Transformations of stabilizer states in quantum networks, Quantum 6 (2022) 846.

[15] A. Dahlberg, S. Wehner, Transforming graph states using single-qubit operations, Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 376 (2018) 20170325.

[16] A. Dahlberg, J. Helsen, S. Wehner, How to transform graph states using single-qubit operations: computational complexity and algorithms, Quantum Science and Technology 5 (2020) 045016.

[17] A. Dahlberg, J. Helsen, S. Wehner, Transforming graph states to Bell-pairs is NP-complete, Quantum 4 (2020) 348.

[18] B. Courcelle, S.-i. Oum, Vertex-minors, monadic second-order logic, and a conjecture by

seese, Journal of Combinatorial Theory, Series B 97 (2007) 91–126.
[19] B. Courcelle, J. Engelfriet, Graph Structure and Monadic Second-Order Logic: A Language-Theoretic Approach, Encyclopedia of Mathematics and its Applications, Cambridge University Press, 2012. doi:10.1017/CBO9780511977619.
[20] E. Clarke, A. Biere, R. Raimi, Y. Zhu, Bounded model checking using satisfiability solving, Formal methods in system design 19 (2001) 7–34.
[21] A. Biere, A. Cimatti, E. M. Clarke, O. Strichman, Y. Zhu, Bounded model checking., in: Handbook of satisfiability, IOS press, 2009, pp. 457–481.
[22] F. Hahn, A. Pappa, J. Eisert, Quantum network routing and local complementation, npj Quantum Information 5 (2019) 76.
[23] F. Hahn, A. Dahlberg, J. Eisert, A. Pappa, Limitations of nearest-neighbor quantum networks, Physical Review A 106 (2022) L010401.
[24] J. de Jong, F. Hahn, N. Tcholtchev, M. Hauswirth, A. Pappa, Extracting maximal entanglement from linear cluster states, arXiv preprint arXiv:2211.16758 (2022).
[25] D. M. Greenberger, M. A. Horne, A. Zeilinger, Going beyond bell's theorem, in: Bell's theorem, quantum theory and conceptions of the universe, Springer, 1989, pp. 69–72.
[26] J. Rabbie, K. Chakraborty, G. Avis, S. Wehner, Designing quantum networks using preexisting infrastructure, npj Quantum Information 8 (2022) 5.
[27] A. Bouchet, An efficient algorithm to recognize locally equivalent graphs, Combinatorica 11 (1991) 315–329.
[28] M. van den Nest, J. Dehaene, B. de Moor, Efficient algorithm to recognize the local Clifford equivalence of graph states, Physical Review A 70 (2004) 034302.
[29] A. Dahlberg, J. Helsen, S. Wehner, Counting single-qubit Clifford equivalent graph states is #P-complete, Journal of Mathematical Physics 61 (2020) 022202.
[30] L. E. Danielsen, M. G. Parker, On the classification of all self-dual additive codes over gf (4) of length up to 12, Journal of Combinatorial Theory, Series A 113 (2006) 1351–1367.
[31] A. Cabello, L. E. Danielsen, A. J. López-Tarrida, J. R. Portillo, Optimal preparation of graph states, Physical Review A 83 (2011) 042314.
[32] J. C. Adcock, S. Morley-Short, A. Dahlberg, J. W. Silverstone, Mapping graph state orbits under local complementation, Quantum 4 (2020) 305.
[33] M. J. Heule, S. Szeider, A SAT approach to clique-width, ACM Transactions on Computational Logic (TOCL) 16 (2015) 1–27.
[34] M. Samer, H. Veith, Encoding treewidth into SAT, in: Theory and Applications of Satisfiability Testing-SAT 2009: 12th International Conference, SAT 2009, Swansea, UK, June 30-July 3, 2009. Proceedings 12, Springer, 2009, pp. 45–50.
[35] A. Schidler, S. Szeider, A SAT approach to twin-width, in: 2022 Proceedings of the Symposium on Algorithm Engineering and Experiments, SIAM, 2022, pp. 67–77.
[36] R. Ganian, N. Lodha, S. Ordyniak, S. Szeider, SAT-encodings for treecut width and treedepth, in: 2019 Proceedings of the Twenty-First Workshop on Algorithm Engineering and Experiments, SIAM, 2019, pp. 117–129.
[37] N. Lodha, S. Ordyniak, S. Szeider, SAT-encodings for special treewidth and pathwidth, in: Theory and Applications of Satisfiability Testing–SAT 2017: 20th International Conference, Melbourne, VIC, Australia, August 28–September 1, 2017, Proceedings 20, Springer, 2017, pp. 429–445.

[38] N. Lodha, S. Ordyniak, S. Szeider, A SAT approach to branchwidth, in: Theory and Applications of Satisfiability Testing–SAT 2016: 19th International Conference, Bordeaux, France, July 5-8, 2016, Proceedings 19, Springer, 2016, pp. 179–195.
[39] N. Lodha, S. Ordyniak, S. Szeider, A SAT approach to branchwidth, ACM Transactions on Computational Logic (TOCL) 20 (2019) 1–24.
[40] B. Courcelle, I. A. Durand, On using SAT solvers for graph computations (2022).
[41] S. Schneider, L. Burgholzer, R. Wille, A SAT encoding for optimal Clifford circuit synthesis, in: Proceedings of the 28th Asia and South Pacific Design Automation Conference, 2023, pp. 190–195.
[42] S. Aaronson, D. Gottesman, Improved simulation of stabilizer circuits, Physical Review A 70 (2004) 052328.
[43] S. Yamashita, I. L. Markov, Fast equivalence-checking for quantum circuits, in: 2010 IEEE/ACM International Symposium on Nanoscale Architectures, IEEE, 2010, pp. 23–28.
[44] L. Berent, L. Burgholzer, R. Wille, Towards a SAT encoding for quantum circuits: A journey from classical circuits to Clifford circuits and beyond, arXiv:2203.00698 (2022).
[45] M. Amy, Towards large-scale functional verification of universal quantum circuits, arXiv preprint arXiv:1805.06908 (2018).
[46] B. Tan, J. Cong, Optimal layout synthesis for quantum computing, in: Proceedings of the 39th International Conference on Computer-Aided Design, 2020, pp. 1–9.
[47] I. Shaik, J. van de Pol, Optimal layout synthesis for quantum circuits as classical planning, arXiv preprint arXiv:2304.12014 (2023).
[48] M. A. Nielsen, I. Chuang, Quantum computation and quantum information, American Association of Physics Teachers, 2002.
[49] J. Eisert, K. Jacobs, P. Papadopoulos, M. B. Plenio, Optimal local implementation of nonlocal quantum gates, Physical Review A 62 (2000) 052317.
[50] N. Nickerson, Practical fault-tolerant quantum computing., Ph.D. thesis, Imperial College London, 2015.
[51] N. Sangouard, C. Simon, H. de Riedmatten, N. Gisin, Quantum repeaters based on atomic ensembles and linear optics, Rev. Mod. Phys. 83 (2011) 33–80. URL: https://link.aps.org/doi/10.1103/RevModPhys.83.33. doi:10.1103/RevModPhys.83.33.
[52] I. Rabinovitz, O. Grumberg, Bounded model checking of concurrent programs, in: Computer Aided Verification: 17th International Conference, CAV 2005, Edinburgh, Scotland, UK, July 6-10, 2005. Proceedings 17, Springer, 2005, pp. 82–97.
[53] G. Audemard, L. Simon, On the Glucose SAT solver, International Journal on Artificial Intelligence Tools 27 (2018) 1840001.
[54] A. Biere, M. Fleury, Gimsatul, IsaSAT and Kissat entering the SAT Competition 2022, in: T. Balyo, M. Heule, M. Iser, M. Järvisalo, M. Suda (Eds.), Proc. of SAT Competition 2022 – Solver and Benchmark Descriptions, volume B-2022-1 of *Department of Computer Science Series of Publications B*, University of Helsinki, 2022, pp. 10–11.
[55] M. Christandl, S. Wehner, Quantum anonymous transmissions, in: Advances in Cryptology-ASIACRYPT 2005: 11th International Conference on the Theory and Application of Cryptology and Information Security, Chennai, India, December 4-8, 2005. Proceedings 11, Springer, 2005, pp. 217–235.
[56] J. Ribeiro, G. Murta, S. Wehner, Fully device-independent conference key agreement,

Physical Review A 97 (2018) 022307.
[57] B. Li, S. E. Economou, E. Barnes, Photonic resource state generation from a minimal number of quantum emitters, npj Quantum Information 8 (2022) 11.
[58] S.-H. Lee, H. Jeong, Graph-theoretical optimization of fusion-based graph state generation, arXiv preprint arXiv:2304.11988 (2023).