Resources Required for Preparing Graph States

Peter Høyer, Mehdi Mhalla, Simon Perdrix

Resources required for preparing graph states

Peter Høyer[*]   Mehdi Mhalla[†]   Simon Perdrix[†]

Abstract

Graph states have become a key class of states within quantum computation. They form a basis for universal quantum computation, capture key properties of entanglement, are related to quantum error correction, establish links to graph theory, violate Bell inequalities, and have elegant and short graph-theoretical descriptions. We give here a rigorous analysis of the resources required for producing graphs states. Using a novel graph-contraction procedure, we show that any graph state can be prepared by a linear-size constant-depth quantum circuits, and we establish trade-offs between depth and width. We show that any minimal-width quantum circuit requires gates that acts on several qubits, regardless of the depth. We relate the complexity of preparing graph states to a new graph-theoretical concept, the local minimum degree, and show that it captures basic properties of graph states.

Keywords: Quantum Computing. Algorithms. Foundations of computing.

1   Introduction

What are the minimal resources required for universal quantum computation? This single question is one of the most fundamental questions related to building quantum computers, and it is one of the most studied questions within quantum computing. In 2000, in seminal work, Raussendorf and Briegel [15] proposed a new model for quantum computations. They show that if certain initial quantum states, called graph states, are provided, then the mere ability to perform one-qubit measurements suffices for quantum computations.

Graph states have been studied extensively within the last five years. The recent survey [11] by Hein *et al.* provides an excellent introduction to the area. These efforts have established several fundamental results on the universality of quantum computations based on graph states, physical implementations of graph states, the entanglement embodied by graph states, and have proved links to basic concepts within graph theory. In this paper, we study computational aspects of graph states. We study in particular the question of characterizing the resources required for producing graph states and we establish stronger links to graph theory.

We first and foremost prove that any graph state can be prepared in constant time. That is, given a classical description of a graph $G = (V, E)$, we can produce the corresponding graph state $|G\rangle$ by a constant-depth quantum circuit that has size linear in the input size $|V| + |E|$ and that consists only of one-qubit operations and control-not operations. This implies that all two-qubit operations ever required by any quantum algorithm can be conducted at the outset of the algorithm in parallel, after which all operations act only on one qubit. We also show that our circuit is robust against various alterations. If we for instance do not wish to conduct all two-qubit operations at the outset, they can be postponed, and if for instance we want to limit the number of qubits used, i.e., the size of the Hilbert space acted upon, we can trade width for depth without compromising the overall linear upper bound on the size of the circuit.

The ability to efficiently procedure arbitrary graph states has several advantages: it reduces the number of qubits involved in the computation, sometimes even quadratically, and hence decreases the possibilities of errors, it replaces two-qubit quantum operations by simple and reliable classical computations, and it allows tailoring the preparation to specific quantum algorithms such as Shor's factoring algorithm [1].

---
[*]Department of Computer Science, University of Calgary, Canada. hoyer@cpsc.ucalgary.ca

[†]Leiniz Laboratory, Grenoble, France. {mehdi.mhalla,simon.perdrix}@imag.fr

We then introduce a new graph-theoretical measure, the local minimum degree, denoted δ_{loc}, and show that it is intimately linked to the complexity of preparing graph states. For instance, we use it to prove that any measurement-based quantum circuit for preparing graph states requires either ancilla qubits or multi-qubit measurements that act on at least $\delta_{\text{loc}} + 1$ qubits (or both). We also establish that the local minimum degree is related to the entanglement in graph states, and we give a family of graphs for which the local minimum degree is large. Such families may be suitable for cryptographic purposes, though likely difficult to create in practice [10]. Other graph-theoretical measures related to graph states have recently and independently been considered in [12, 16, 18].

2 Graph states and signed graph states

A *graph state* on n qubits is a state that is a superposition over all basis states,

$$|G\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{q_\Gamma(x)} |x\rangle, \tag{1}$$

where Γ is the adjacency matrix of a graph $G = (V, E)$ on $n = |V|$ vertices and $q_\Gamma(x) = \sum_{i<j:(i,j)\in E} x_i x_j$. The quadractic form q_Γ satisfies that $q_\Gamma(x) = x^T \Gamma^{\text{upper}} x$ where Γ^{upper} is the upper-triangle of Γ obtained by setting entries $\Gamma_{i,j}$ with $i \geq j$ to zero, and where T denotes taking transpose.

For technical reasons, it is sometimes convenient to associate signs to graph states. Given any graph state $|G\rangle$ and any subset $S \subseteq V$ the *signed graph state* $|G; S\rangle$ is the state

$$|G; S\rangle = \mathsf{Z}_S |G\rangle, \tag{2}$$

where $\mathsf{Z}_S = \bigotimes_{v \in S} \mathsf{Z}_v$ where Z_v denotes that the local operator $\mathsf{Z} = |0\rangle\langle 0| - |1\rangle\langle 1|$ acts on qubit v. We sometimes omit the signs when they are not essential for the discussion. We use similar abbreviated notation, $\mathsf{X}_S = \bigotimes_{v \in S} \mathsf{X}_v$ and $\mathsf{Y}_S = \bigotimes_{v \in S} \mathsf{Y}_v$, for the two other pauli-operators $\mathsf{X} = |1\rangle\langle 0| + |0\rangle\langle 1|$ and $\mathsf{Y} = \sqrt{-1}|1\rangle\langle 0| - \sqrt{-1}|0\rangle\langle 1|$.

Proposition 1 *For all graphs $G = (V, E)$ and all non-empty subsets $S \subseteq V$,*

$$\langle G; S | G \rangle = 0,$$

and hence $\langle G; S | G; S' \rangle = 0$ for all distinct subsets $S, S' \subseteq V$, and the $2^{|V|}$ states $\{|G; S\rangle\}_{S \subseteq V}$ form an orthonormal basis.

3 Preparation of graph states

There is a simple algorithm for preparing the graph state $|G\rangle$ corresponding to any graph $G = (V, E)$ on $n = |V|$ vertices with $m = |E|$ edges. We first prepare n qubits in a superposition of all 2^n basis states,

$$|\Psi_0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle,$$

by applying for instance the Hadamard operator $\mathsf{H} = \frac{1}{\sqrt{2}} \big(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1| \big)$ on each of the n qubits in the initial state $|0\rangle$. Each of the qubits corresponds to a vertex of G. We then modify the phases of the basis states by applying a sequence of m two-qubit operations, producing the graph state $|G\rangle$,

$$|G\rangle = \prod_{(u,v) \in E} \Delta_u(\mathsf{Z}_v) |\Psi_0\rangle. \tag{3}$$

2

For each edge $(u, v) \in E$, we apply the controlled phase change operator defined by

$$\Delta_u(Z_v) = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| - |11\rangle\langle 11|$$

on the two qubits labelled by the endpoints u, v of the edge. These m two-qubit operations are diagonal and thus commute, allowing us to apply them in any order of our choosing. Summarizing, we can prepare any graph state $|G\rangle$ using n single-qubit operations and m two-qubit $\Delta(Z)$ operations. Considering this simple algorithm a quantum circuit, we can prepare a graph state by a circuit on n qubits of size $n+m$ and depth $m+1$ using only single-qubit and two-qubit operations.

The depth of the circuit may be improved by parallelizing the two-qubit operations by choosing an edge coloring of G [1]. An *edge coloring* using χ' colors is a mapping $c : E \rightarrow \{1, 2, \ldots, \chi'\}$ satisfying that if two distinct edges e and e' share one endpoint, then they are assigned different colors. Any graph has an edge coloring using at most $\Delta(G) + 1$ colors, where $\Delta(G)$ is the maximum degree of the vertices in G, and we can find such an edge coloring in time polynomial in n and m, for instance by Vizing's (classical) algorithm [19]. This implies that we can arrange the m two-qubit operations in our circuit such that it has depth at most $\Delta(G) + 2$.

Proposition 2 ([1]) *Any graph state $|G\rangle$ can be prepared by a quantum circuit consisting of single-qubit and two-qubit operations of size $O(n + m)$ and depth $O(\Delta(G))$ acting on n qubits, where $\Delta(G)$ is the maximum degree of any vertex in G.*

The above proposition implies that graphs of bounded degree can be prepared by constant depth quantum circuits. In particular, two-dimensional cluster states, which is the common name for graph states arising from two-dimensional grid graphs, can be prepared by constant depth quantum circuits. We now extend this result and prove that arbitrary graphs can prepared in constant depth.

Theorem 3 (Constant depth graph state preparation) *For any graph G, we can prepare some signed graph state $|G; S\rangle$ by a constant depth quantum circuit consisting of single-qubit and two-qubit operations of size $O(n + m)$ acting on $n + O(m)$ qubits.*

A key idea in our proof is to embed G as an induced minor of a larger graph of bounded degree, and then utilize that taking induced minors can be obtained by Pauli measurements.

We consider four types of substructures of a graph $G = (V, E)$. A *deletion of a vertex* $v \in V$ in G is the graph $G \setminus v$ obtained from G by deleting v and all edges incident to v. A *deletion of an edge* $e \in E$ in G is the graph $G \setminus e$ obtained from G by simply deleting the edge e. A *contraction of an edge* $(u, v) \in E$ in G is the graph $G/(u, v)$ obtained from G by introducing edges between v and each vertex in $N_G(u) \setminus N_G(v)$, and then deleting u and all its incident edges. A graph G is an *induced subgraph* of G' if G is isomorphic to a graph that can be obtained from G' by vertex deletions. It is a *subgraph* of G' if we can obtain a graph isomorphic to G by edge deletions. It is a *minor* of G' if it is isomorphic to a graph that can be obtained from G' by edge deletions and edge contractions, and it is an *induced minor* of G' if it is isomorphic to a graph that can be obtained from G' by vertex deletions and edge contractions. Any induced subgraph is also a subgraph, and any induced minor is also a minor.

The next two lemmas provide our main technical tools for generating the graph state $|G\rangle$.

Lemma 4 (Vertex deletion) *Let $v \in V$ be any vertex. Conducting a Z measurement of the qubit v maps $|G\rangle$ to $|G \setminus v\rangle$ and thus corresponds to deleting the vertex v.*

Proof We first note that for any $S \subseteq V$,

$$|G; S\rangle = \frac{1}{\sqrt{2}}\big(|G \setminus v; S\rangle|0\rangle_v + |G \setminus v; S\Delta N_G(v)\rangle|1\rangle_v\big)$$
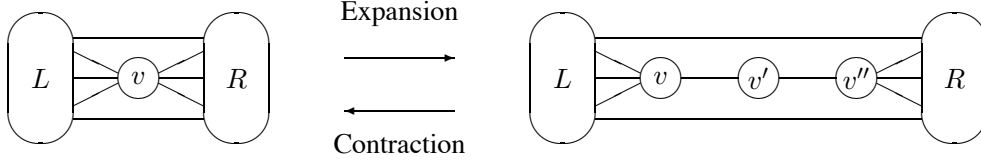
3

Figure 1: Embedding G as an induced minor of a bounded degree graph $\tilde{G}$ by repeated applications of graph expansions. Conducting X measurements of qubits v' and v'' contracts the two edges (v, v') and (v', v'').

which follows from Eqs. 2 and 3. If qubit v is Z-measured (that is, measured in the basis of the eigenvectors of the Pauli operator Z), the resulting state is thus either $|G \setminus v; S\rangle$ or $|G \setminus v; S\Delta N_G(v)\rangle$ (where Δ denotes the symmetric difference), and hence is equal to $|G \setminus v\rangle$ up to (known) signs. $\qquad\square$

Lemma 5 (Edge contraction) *Let $v, v', v'' \in V$ so that $N_G(v') = \{v, v''\}$ and $N_G(v) \cap N_G(v'') = \{v'\}$. Conducting an X measurement of each of the two qubits v' and v'' maps $|G\rangle$ to $|G/(v, v')/(v', v'')\rangle$ and thus corresponds to contracting the two edges (v, v') and (v', v'').*

Proof Let $v, v', v'' \in V$ be as in the lemma. For any subset $S \subseteq V$,

$$|G; S\rangle = \frac{\mathsf{Z}_S}{2} \sum_{k,l \in \{0,1\}} \left(\mathsf{Z}_{v''}^k \mathsf{Z}_{N_G(v) \setminus \{v'\}}^l |G/vv'/v'v''\rangle \right) \left(|0\rangle + \mathsf{Z}_{v'}^l |1\rangle \right)_{v'} \left(|0\rangle + \mathsf{Z}_{v''}^k |1\rangle \right)_{v''}$$

and hence, if qubits v' and v'' are X-measured, the resulting state is $|G/(v, v')/(v', v'')\rangle$ up to (known) signs. $\qquad\square$

Proof of Theorem 3 We first embed G as an induced minor of a larger graph $\tilde{G}$ of bounded degree by repeatedly expanding any vertex v of degree $d \geq 4$ into three vertices v, v', v'' of strictly smaller degrees, as illustrated in Figure 1. Formally, we partition the neighborhood $N_G(v)$ of v in two sets L and R of sizes $\lceil \frac{d}{2} \rceil$ and $\lfloor \frac{d}{2} \rfloor$, respectively. We then set $\hat{V} = V \cup \{v', v''\}$ and $\hat{E} = E \setminus (\{v\} \times R) \cup \{(v, v'), (v', v'')\} \cup (\{v''\} \times R)$. We set $\hat{G} = (\hat{V}, \hat{E})$, and recursively expand any vertex v of $\hat{G}$ till all vertices have degree at most three. The thus obtained graph $\tilde{G}$ will have $O(m)$ vertices and maximum degree three.

We first prepare the graph state $|\tilde{G}\rangle$ by a constant-depth circuit on $O(m)$ qubits by applying Proposition 2, and then apply Lemma 5 to contract $|\tilde{G}\rangle$ to $|G\rangle$ by applying X measurements on all vertices introduced during the expansion of G to $\tilde{G}$. The X measurements commute and can thus all be conducted in parallel by a circuit of depth one. $\qquad\square$

Proposition 2 and Theorem 3 give two linear-size circuits for preparing any graph state, up to signs. The former has small width and large depth, the latter large width and small depth. We can trade width for depth in the above construction, without compromising the overall size of the circuit, by stopping the expansion once all vertices have degree at most T.

Theorem 6 (Small depth graph state preparation) *For any graph G, we can prepare some signed graph state $|G; S\rangle$ by a quantum circuit consisting of single-qubit and two-qubit operations of size $O(n + m)$ and depth $O(T)$ acting on $n + O(m/T)$ qubits, for any integer T.*

In the above theorems, we can replace the unitary operations by projective measurements. Any single-qubit unitary operation can be simulated using two single-qubit projective measurements, one two-qubit projective measurement, and one ancilla qubit [14]. Similarly, a two-qubit control-not operation can be simulated

using two single-qubit projective measurements, two two-qubit projective measurements, and one ancilla qubit [14]. In Theorem 6, we may thus replace the unitary operations by projective measurements. We re-use the ancilla qubits in each of the $\Theta(T)$ layers of the circuit so that the the total number of additional ancilla qubits required by the simulation is only $O(m/T)$.

Theorem 7 (Measurement-based preparation) *For any graph G, we can prepare some signed graph state $|G; S\rangle$ by a quantum circuit consisting of single-qubit and two-qubit projective measurements of size $O(n+m)$ and depth $O(T)$ acting on $n + O(m/T)$ qubits, for any integer T.*

In the standard circuit for graph preparation, in which each of the $O(m)$ layers of the circuit consists of exactly one gate, we may similarly replace the unitary operations by projective measurements, yielding that any graph state can be prepared using $n + 1$ qubits by single-qubit and two-qubit projective measurements. We require only one ancilla qubit for iteratively simulating each of the $O(m)$ two-qubit operations.

Proposition 8 (Measurement-based preparation using one ancilla qubit) *For any graph G, we can prepare some signed graph state $|G; S\rangle$ by a quantum circuit consisting of single-qubit and two-qubit projective measurements of size $O(n + m)$ and depth $O(m)$ acting on $n + 1$ qubits.*

It would be interesting to extend Theorem 3 and its corollaries to incorporate noise and errors, for instance as discussed for cluster states in [6].

4 Circuits and local complementation

The circuit constructions for preparation of graph states given above are based on the concept of graph minors. To improve the constructions further, we require the additional concept of local complementation in graphs. A local complementation is a graph operation that maps one graph into another. Kotzig first showed that the class of circle graphs are closed under local complementation (see [8, 4]) and it was then used by Bouchet [5] to give a characterization of circle graphs.

A *local complementation* of a graph G at a vertex $v \in V$ is the operation which replaces the subgraph of G induced by the neighborhood $N_G(v)$ of v by its complement. We denote the thus obtained graph by $G \star v$. Local complementation defines an equivalence relation. We say two graphs G_1 and G_2 are *locally equivalent* if one can be obtained from the other by a sequence of local complementations, and write $G_1 \approx_{\text{loc}} G_2$.

A *pivoting* on a edge $(u, v) \in E$ is the operation that maps G to $G \star u \star v \star u$. This operation is well-defined as $G \star u \star v \star u = G \star v \star u \star v$, and we denote it by $G \wedge (u, v)$. Following Oum [13], we say a graph H is a *vertex minor* of G if H can be obtained from G by vertex deletions and local complementations. A graph H is a *pivot minor* of G if H can be obtained from G by vertex deletions and pivotings.

The most important property of local complementation for this paper, is that it can be implemented by local quantum operations. Let G and G' be two locally equivalent graphs, $G \approx_{\text{loc}} G'$. Then there exists a tensor product $\mathsf{U} = \bigotimes_{v \in V} \mathsf{U}^{(v)}$ of n single-qubit unitary operations $\mathsf{U}^{(v)}$ such that $|G'\rangle = \mathsf{U}|G\rangle$. This implies that if $\mathcal{C}$ is a circuit that maps $|\Psi_0\rangle$ to $|G'\rangle$, then $\mathsf{U}\mathcal{C}$ is a circuit that maps $|\Psi_0\rangle$ to $|G\rangle$. Thus, any two locally equivalent graphs can be implemented by circuits of the same depths, up to an additive constant of 1.

Let $\delta(G) = \min\{\deg_G(v) : v \in V\}$ denote the minimum degree of any vertex in G, where $\deg_G(v)$ denotes the degree of v in G. Let $\delta_{\text{loc}}(G) = \min\{\delta(G') : G' \approx_{\text{loc}} G\}$ denote the minimum degree achievable by local complementations. We refer to δ_{loc} as the *local minimum degree of G*. Similarly, let $m_{\text{loc}}(G) = \min\{|E'| : (V, E') \approx_{\text{loc}} G\}$ denote the minimum total number of edges achievable by local complementations. Unfortunately, there is no known polynomial-time algorithm for computing either of the two quantities $\delta_{\text{loc}}(G)$ and $m_{\text{loc}}(G)$, given a graph G as input. The thus far best result in this direction is a result of Bouchet [2] stating that the problem of deciding if two graphs are locally equivalent is polynomial-time computable. Van den Nest [17] gives in his Ph.D. thesis a short description of Bouchet's algorithm.

The quantity m_{loc} is related to the size of any quantum circuit preparing a graph state. Suppose we could find a polynomial-time algorithm that given any graph, outputs a locally equivalent graph of minimum total degree. Then in Theorems 3, 6 and 7, we could replace m by m_{loc}, and still have polynomial-time constructable quantum circuits. However, currently no such result is in sight.

We now show that δ_{loc} is related to the usage of ancilla qubits in the circuits for preparing graph states. To prove this, we first give three equivalent definitions of δ_{loc}, the first graph theoretical, the second combinatorial, and the third algebraic. We require the following notation and concepts.

For any subset $X \subseteq V$ of vertices, let $\text{Odd}_G(X) = \{u \in V \setminus X \ : \ N_G(u) \cap X = 1 \mod 2\}$ denote the set of vertices that is adjacent to an odd number of vertices in X in G. Similarly, let $\text{Even}_G(X) = \{u \in V \setminus X \ : \ N_G(u) \cap X = 0 \mod 2\}$. We say that the vertices in $\text{Odd}_G(X)$ are *odd neighbors* of X in G, and that the vertices in $\text{Even}_G(X)$ are *even neighbors* of X in G.

The cut-matrix of a subset $X \subseteq V$ of vertices is the submatrix $\Gamma_G(X, V \setminus X)$ indexed by $X \times (V \setminus X)$ of the adjacency matrix Γ_G of G. The cut-rank $\text{Cutrk}(X)$ of X is the rank of its cut-matrix, where we define the rank over GF(2). The cut-rank of X is invariant under local complementation [3], though the null-space of $\Gamma_G(X, V \setminus X)$ may change under local complementation. It was used by Bouchet [2] and others under the name "connectivity function", and coined the cut-rank by Oum [13]. We say that a set of vertices $L \subseteq V$ is *local* if $L = X \cup \text{Odd}_G(X)$ for some subset $X \subseteq L$. Note that a local set L does not have full cut-rank, and that $\{v\} \cup N_G(v)$ is local for any vertex $v \in V$.

Lemma 9 *Any local set L is invariant under local complementation. Moreover, for all $y \in L$, there exists a graph G' locally equivalent to G such that $\{y\} \cup \text{Odd}_{G'}(\{y\}) \subseteq L$.*

Proof Suppose that $L = X \cup \text{Odd}_G(X)$. We consider how the three-way partition $V = X \cup \text{Odd}_G(X) \cup \text{Even}_G(X)$ changes under local complementation at a vertex $v \in V$. Let $G' = G \star v$. Then the three-way partition changes as follows.

	X'	$\text{Odd}_{G'}(X')$	$\text{Even}_{G'}(X')$
$v \in \text{Even}_G(X)$	X	$\text{Odd}_G(X)$	$\text{Even}_G(X)$
$v \in \text{Odd}_G(X)$	$X \cup \{v\}$	$\text{Odd}_G(X) \setminus \{v\}$	$\text{Even}_G(X)$
$v \in X$ and $|N_X(v)|$ is odd	$X \setminus \{v\}$	$\text{Odd}_G(X) \cup \{v\}$	$\text{Even}_G(X)$
$v \in X$ and $|N_X(v)|$ is even	X	$\text{Odd}_G(X)$	$\text{Even}_G(X)$

The forth and last column implies that any local set L is invariant under local complementation, and thus only the internal structure of L changes. By the second row, we can move vertex y into X, if $y \in \text{Odd}_G(X)$. By the third row, we can move vertices out of X as long as there exists a vertex in X having an odd number of neighbors in X. If all vertices in X have an even number of neighbors in X, and if any vertex in X has a neighbor z in $\text{Even}_G(X)$, then a local complementation at z creates at least two vertices in X having an odd number of neighbors in X. One of these must be a vertex different from y. Thus, by a sequence of local complementations, we can map G to some graph G' in which there are no edges between X and $\text{Even}_{G'}(X)$, and in which $y \in X$. Hence $N_{G'}(y) \subseteq L$ and thus $\{y\} \cup \text{Odd}_{G'}(\{y\}) \subseteq L$. $\square$

Corollary 10 *Let $x \in V$ be any vertex of degree $d = \deg_G(x)$. Then for all neighbors $y \in N_G(x)$, there exists a graph G' locally equivalent to G for which $N_{G'}(y) = (N_G(x) \cup \{x\}) \setminus \{y\}$. In particular, all neighbors of x can be locally reduced to having degree d.*

Theorem 11 (Characterization of local minimum degree) *For any graph G, the local minimum degree $\delta_{\text{loc}}(G)$ is equal to*

1. $\min\{\delta(G') \ : \ G' \approx_{\text{loc}} G\}$.

2. $\min\big\{|L| : L \text{ is nonempty and local}\big\} - 1$.

3. $\min\big\{|X| : \mathrm{Cutrk}(X) < |X|\big\} - 1$.

Proof We first show that the quantity in (1) is an upper bound on the quantity in (2). Let $y \in V$ be a vertex of degree $\delta_{\mathrm{loc}}(G)$ in $G' \approx_{\mathrm{loc}} G$. Then $\{y\} \cup N_{G'}(y)$ is local. Similarly, we show that the quantity in (2) is an upper bound on the quantity in (3). Let $L = X \cup \mathrm{Odd}_G(X)$ be local. Then $\chi_X \Gamma_G[L, V \setminus L] = 0$, where χ_X is the indicator function of X in L, and thus L does not have full cutrank. Finally, we show that the quantity in (3) is an upper bound on the quantity in (1). Let $X \subset V$ be a set that does not have full cutrank. Let $Y \subseteq V \setminus X$ be such that $\chi_Y \Gamma[X, V \setminus X] = 0$. Then $\mathrm{Odd}_G(Y) \subset X$. By Lemma 9, for all $y \in Y$, there is a graph G' locally equivalent to G such that $\deg_{G'}(y) \leq |X| - 1$. $\qquad\square$

By Theorem 11, for any fixed integer d, there exists a polynomial-time algorithm for deciding if $\delta_{\mathrm{loc}} > d$. If d is part of the input, no polynomial-time algorithm is known. Though plausible, it is not known whether the concept of cut-rank is helpful in computing δ_{loc} in polynomial time. One result in this direction is by Oum [13], who gives a polynomial-time algorithm that given any two disjoint non-empty sets of vertices $A, B \subset V$ as input, computes the value $\min\{\mathrm{Cutrk}(Z) : X \subseteq Z \subseteq V \setminus B\}$ by greedily searching for blocking sequences as introduced by Geelen [9].

We now use the above characterization to show that if no ancilla qubits are available for preparing a graph state, then joint projective measurements on at least $\delta_{\mathrm{loc}}(G) + 1$ qubits are required. As a consequence, for all graphs for which $\delta_{\mathrm{loc}} > 1$, there does not exist a measurement-based preparation using only single-qubit and two-qubit projective measurements without the use of ancilla qubits.

Theorem 12 (Lower bound on measurement-based preparation) *Let G be any graph. Any preparation of $|G\rangle$ by a quantum circuit acting on n qubits and consisting of projective measurements requires measurements acting on $\delta_{\mathrm{loc}}(G) + 1$ qubits.*

Proof By contradiction. Assume the last measurement of the preparation acts on at most $\delta_{\mathrm{loc}}(G)$ qubits X and that it produces the signed graph state $|G; S\rangle$. Let W be the observable describing this measurement. Then $\mathsf{W}|G; S\rangle = |G; S\rangle$, and thus $\langle G; S|\mathsf{W}|G; S\rangle = 1$.

Let $U \subseteq X$ be any subset of the measured vertices X. Since $|X| \leq \delta_{\mathrm{loc}}(G)$, subset X has full cutrank by Theorem 11, and thus there exists a subset $Y \subseteq V \setminus X$ such that $\chi_U = \Gamma[X, V \setminus X]\chi_Y$. The operator X_Y acts only on qubits not in X, and thus commutes with W. In addition, $\mathsf{Z}_{\mathrm{Odd}(Y)}\mathsf{X}_Y|G; S\rangle = \pm|G; S\rangle$, and hence

$$1 = \langle G; S|\mathsf{W}|G; S\rangle = \langle G; S|\mathsf{X}_Y \mathsf{W}\mathsf{X}_Y|G; S\rangle = \langle G; S|\mathsf{Z}_{\mathrm{Odd}(Y)}\mathsf{W}\mathsf{Z}_{\mathrm{Odd}(Y)}|G; S\rangle$$
$$= \langle G; S|\mathsf{Z}_U \mathsf{W}\mathsf{Z}_U|G; S\rangle = \langle G; S\Delta U|\mathsf{W}|G; S\Delta U\rangle.$$

It follows that W acts trivially on $|G; S\Delta U\rangle$ for all subsets $U \subseteq X$. Since these $2^{|X|}$ states are pairwise orthogonal, W is the identity, which is a contradiction. $\qquad\square$

It is natural to consider recursive methods for preparing a graph state G, for instance by partitioning the vertex set V into parts which then are considered individually. The next lemma states that deleting any one vertex or edge may decrease the local degree by at most one.

Lemma 13 *For any graph $G = (V, E)$, any vertex $u \in V$, and any edge $e = (v, w) \in E$, $\delta_{\mathrm{loc}}(G \setminus v) \geq \delta_{\mathrm{loc}}(G) - 1$ and $\delta_{\mathrm{loc}}(G \setminus e) \geq \delta_{\mathrm{loc}}(G) - 1$.*

Proof Let $X \subseteq V \setminus \{u\}$ be any set of vertices satisfying that $\mathrm{Cutrk}_{G\setminus u}(X) < |X|$. Then $\mathrm{Cutrk}_G(X \cup \{u\}) \leq \mathrm{Cutrk}_{G\setminus u}(X) + 1 < |X \cup \{u\}|$. Now, let $X \subseteq V$ be any set of vertices satisfying that $\mathrm{Cutrk}_{G\setminus e}(X) < |X|$, and consider an edge $e = (v, w) \in E$. Firstly, if $v, w \in X$ or $v, w \notin X$, then $\mathrm{Cutrk}_G(X) = \mathrm{Cutrk}_{G\setminus e}(X)$. Secondly, if $v \in X$ and $w \notin X$, then $\mathrm{Cutrk}_G(X \cup \{w\}) = \mathrm{Cutrk}_{G\setminus e}(X \cup \{w\}) \leq \mathrm{Cutrk}_{G\setminus e}(X) + 1 < |X| + 1 = |X \cup \{w\}|$. $\qquad\square$
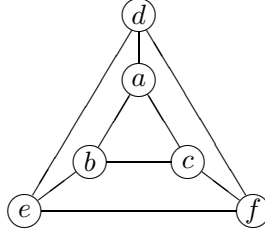
Figure 2: The prism graph P on six vertices. Tracing out vertices b and e from $|G\rangle$ creates a separable mixed state.

Suppose we are given an oracle $\mathcal{O}_\delta$ that given any graph G returns $\delta_{\mathrm{loc}}(G)$. Then there exists a deterministic algorithm that given any graph G outputs a graph G' locally equivalent to G with $\delta(G') = \delta_{\mathrm{loc}}(G)$. The algorithm runs in time polynomial in n and uses at most a linear number of oracle queries. The proof is given in Appendix A.

Theorem 14 *The following two computational problems are polynomially equivalent: (1) computing $\delta_{\mathrm{loc}}(G)$ and (2) finding a graph G' with $G' \equiv G$ and $\delta(G') = \delta_{\mathrm{loc}}(G)$.*

5   Bi-separability and δ_{loc}

An n-qubit state ρ is *bi-separable* if there exists a partition A, B of V such that ρ can be written on the form $\rho = \sum_{i=1}^{k} \alpha_i \rho_i^A \otimes \rho_i^B$ for a finite set of density operators ρ_i^A, ρ_i^B and non-negative weights α_i, where each ρ_i^A acts on A only and each ρ_i^B acts on B only. In this section, we refer to bi-separability simply as separability.

Theorem 15 *For any graph state $|G\rangle$, there exists a subset $U \subseteq V$ of vertices of size $\delta_{\mathrm{loc}}(G)$ such that the reduced density operator $\rho = \mathrm{Tr}_U(|G\rangle\langle G|)$ is separable.*

Proof Let G' be a graph that is locally equivalent to G and contains a vertex v of degree $d = \delta_{\mathrm{loc}}(G)$. We show that the state ρ obtained from $|G'\rangle\langle G'|$ by tracing out the d qubits corresponding to the neighbors $N_{G'}(v)$ of v is separable. We do this by giving a procedure for preparing ρ that preserves separability.

Let $H = G' \setminus N_{G'}(v)$ be the subgraph of G' obtained by removing the neighbors $N_{G'}(v)$ of v. The subgraph H consists of (at least) two components, $\{v\}$ and the rest. The graph state $|H\rangle$ is thus separable and can be written on the form $|v\rangle|H \setminus \{v\}\rangle$.

Consider we first prepare the separable pure state $|H\rangle$. Now for each neighbor $w \in N_{G'}(v)$ in turn, we randomly flip an unbiased coin. If the outcome of the coinflip is head, we apply a (single-qubit) σ_z operation on each of the qubits of $|H\rangle$ corresponding to the neighbors $N_{G'}(w) \cap H$ of w. If the outcome of the coinflip is tail, we do not alter the state. This maps the state $|v\rangle|H \setminus \{v\}\rangle$ to some other pure state $|v\rangle|H'\rangle$ that is also separable with respect to the same partitioning of vertices. We take sum of the density operators $|v\rangle|H'\rangle\langle H'|\langle v|$ over all 2^d possible outcomes, yielding a density operator ρ' that is separable with respect to the same partitioning. The density operator ρ' is the same as the density operator ρ obtained by tracing out the neighbors $N_{G'}(v)$ of v in G', and thus ρ is separable. $\square$

The upper bound of $\delta_{\mathrm{loc}}(G)$ on separability in Theorem 15 is tight for some graphs, but not all. An example for which the bound is not tight is the prism graph P on six vertices, illustrated in Figure 2. On the one hand, any local set in P has size at least 4, and hence its local minimum degree is (at least) 3 by Theorem 11. On the other hand, if we trace out qubits b and e in $|P\rangle$, the remaining state is separable across the cut $(\{a,d\}, \{c,f\})$. One way of seeing this, is to first delete the edge (b,e), do a local complementation on b and then e, deleting b and e, and noticing that the remaining graph consists of two components, $\{a,d\}$ and $\{c,f\}$. It would be

interesting to explore the relationship between δ_{loc} and separability further, and also to consider k-separability and full separability [7].

We show in Appendix B that there exists a natural family of graphs for which δ_{loc} is polynomial in the input graph. It seems plausible that this family of graphs contains entanglement that is very robust against quantum operations acting on a sublinear number of qubits, and thus could be useful in for instance quantum cryptography and quantum communication complexity.

Corollary 16 *There exists a constant $c > 0$ and a family of graphs G for which $\delta_{\mathrm{loc}}(G) \in \Omega(|G|^c)$.*

References

[1] P. Aliferis and D. W. Leung. Computation by measurements: A unifying picture. *Physical Review A*, 70:062314, 2004.

[2] A. Bouchet. Diagraph decompositions and eulerian systems. *SIAM J. Algebraic Discrete Methods*, 8:323–337, 1987.

[3] A. Bouchet. Connectivity of isotropic systems. In *Combinatorial Mathematics: Proc. of the Third International Conference*, volume 555 of *Ann. New York Acad. Sci.*, pages 81–93, 1989.

[4] A. Bouchet. κ-transformations, local complementations and switching. In *Cycles and rays: Basic structures in finite and infinite graphs*, volume C 301 of *NATO Adv. Sci. Inst. Ser.*, pages 41–50. Kluwer Acad. Publ., Dordrecht, 1990.

[5] A. Bouchet. Circle graph obstructions. *J. Comb. Theory Ser. B*, 60(1):107–144, 1994.

[6] L. M. Duan and R. Raussendorf. Efficient quantum computation with probabilistic quantum gates. *Phys. Rev. Lett.*, 95:080503, 2005.

[7] J. Eisert and D. Gross. *Lectures on Quantum Information*, chapter Multi-particle entanglement. Wiley-VCH, Berlin, 2006.

[8] H. de Fraysseix. Local complementation and interlacement graphs. *Discrete Mathematics*, 33(1):29–35, 1981.

[9] J. F. Geelen. *Matchings, Matroids and Unimodular Matrices*. PhD thesis, Univ. Waterloo, 1995.

[10] K. Goyal, A. McCauley, and R. Raussendorf. Purification of large bi-colorable graph states, May 2006. quant-ph/0605228.

[11] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest, and H. J. Briegel. Entanglement in graph states and its applications. In *Proc. of the Int. School of Physics "Enrico Fermi" on "Quantum Computers, Algorithms and Chaos"*, July 2005. quant-ph/0602096.

[12] I. Markov and Y. Shi. Simulating quantum computation by contracting tensor networks. In *Ninth Workshop on Quantum Information Processing*, Jan. 2006. (No proceedings).

[13] S.-i. Oum. Approximating rank-width and clique-width quickly. In D. Kratsch, editor, *Graph-Theoretic Concepts in Computer Science, WG 2005*, volume 3787 of *Lecture Notes in Computer Science*, pages 49–58. Springer, 2005.

[14] S. Perdrix. State transfer instead of teleportation in measurement-based quantum computation. *International Journal of Quantum Information*, 3(1):219–224, 2005.

[15] R. Raussendorf and H. J. Briegel. A one-way quantum computer. *Physical Review Letters*, 86:5188–5191, May 2001.

[16] Y. Shi, L. M. Duan, and G. Vidal. Classical simulation of quantum many-body systems with a tree tensor network. (In completion), Feb. 2006.

[17] M. Van den Nest. *Local equivalence of stabilizer states and codes*. PhD thesis, Faculty of Engineering, K. U. Leuven, Belgium, May 2005.

[18] M. Van den Nest, A. Miyake, W. Dür, and H. J. Briegel. Universal resources for measurement–based quantum computation, Apr. 2006. quant-ph/0604010.

[19] V. G. Vizing. On an estimate of the chromatic class of a p-graph. *Metody Diskret. Analiz.*, 3:25–30, 1964. In Russian.