Nonthreshold quantum secret-sharing schemes in the graph-state formalism

Pradeep Sarvepalli*

School of Chemistry and Biochemistry, Georgia Institute of Technology, Atlanta, Georgia 30332, USA

(Received 2 June 2012; published 1 October 2012)

In a recent work, Markham and Sanders proposed a framework to study quantum secret-sharing (QSS) schemes using graph states. This framework unified three classes of QSS protocols, namely, sharing classical secrets over private and public channels, and sharing quantum secrets. However, previous work on graph-state secret sharing mostly focused on threshold schemes. In this paper, we focus on general access structures. We show how to realize a large class of arbitrary access structures using the graph-state formalism. We show an equivalence between $[[n,1]]$ binary quantum codes and graph-state secret-sharing schemes sharing one bit. We also establish a similar (but restricted) equivalence between a class of $[[n,1]]$ Calderbank-Shor-Steane codes and graph-state QSS schemes sharing one qubit. With these results we are able to construct a large class of graph-state quantum secret-sharing schemes with arbitrary access structures.

DOI: 10.1103/PhysRevA.86.042303 PACS number(s): 03.67.Dd, 03.67.Pp, 03.67.Ac

I. INTRODUCTION

Quantum secret sharing (QSS) [1,2] deals with the problem of sharing classical or quantum secrets using quantum information. Further, secret-sharing protocols could be used in the presence or absence of eavesdroppers. In Ref. [3], a graph-state formalism was proposed with a view to unifying all these variants under the same umbrella. This framework was useful in ways other than unifying the various quantum secret-sharing protocols. For instance, building upon this framework, researchers have been able to propose new secret sharing protocols [4] and make a connection with the measurement-based quantum computation model [5]. More recently, it has motivated research in graph-theoretic concepts such as weak odd domination [6].

The graph-state framework does in principle include nonthreshold access structures for quantum secrets. However, neither [3] nor subsequent works [4–7] provide any procedure to explicitly construct schemes with arbitrary access structures in the graph-state formalism. The graph-state framework for quantum secret-sharing approaches it from a perspective other than quantum error correction, in contrast to the theory as developed in Refs. [1,8,9]. But since any secret-sharing protocol is ultimately an error-correcting code, the graph-state schemes must be equivalent to those based on quantum codes, and the protocols in Ref. [3] must arise from codes. But no results are known in this direction.

The main contribution of this paper is to fill these gaps. We make transparent the connection between the graph-state framework and the protocols presented using quantum codes. We show an equivalence between $[[n,1]]$ binary quantum codes and graph-state protocols sharing one bit. We show a restricted equivalence between a class of $[[n,1]]$ Calderbank-Shor-Steane (CSS) codes and graph-state secret-sharing protocols sharing one qubit. We also translate many of the schemes developed using quantum codes into those based on the graph-state formalism.

We emphasize that our results are constructive and provide concrete details for the construction of the secret-sharing schemes as well as the associated details of recovery. We restrict ourselves to the qubit case in this paper, although as shown in Ref. [7] graph-state secret-sharing schemes can be extended to other alphabets.

II. BACKGROUND

A. Quantum secret sharing

We briefly review the pertinent ideas of quantum secret sharing. We assume that the reader is familiar with quantum codes and the stabilizer formalism [10,11]. In a secret-sharing scheme, a dealer distributes an encrypted secret to a collection of players. Then certain subsets of players can collaboratively reconstruct the secret. Those subsets which can recover the secret are called *authorized sets* and those that cannot are said to be *unauthorized sets*. The collection of authorized sets is called the *access structure* of the scheme, which we denote as Γ. For an access structure to be valid, it must be *monotonic*, i.e., any set that contains an authorized set must also be an authorized set. An authorized set is said to be minimal if any proper subset of it is unauthorized. The collection of minimal authorized sets is called the *minimal access structure*.

In a threshold scheme with threshold k, any subset consisting of k or more players can access the secret while those with fewer players cannot. We denote such a quantum threshold scheme on n players by $((k,n))$. In a general access structure, the authorized sets can be of different sizes and all subsets of that size need not be authorized. A collection of sets Γ_{gen} is said to generate the access structure Γ, if every authorized set contains some element of Γ_{gen}.

A secret-sharing scheme is said to be *perfect* if the unauthorized sets cannot extract any information about the secret. In this paper we are interested only in perfect secret-sharing schemes.

When the secret to be shared is classical, the dealer distributes a set of orthogonal quantum states that encode the secret. The following result, due to Gottesman, states the conditions that must be satisfied by authorized and unauthorized sets for sharing classical secrets through a QSS scheme.

*pradeep.sarvepalli@gatech.edu

Proposition 1 *(access conditions for classical secrets* [8]*).* Suppose we have a set of orthonormal states $|\psi_i\rangle$ encoding a classical secret. Then a set T is an unauthorized set if and only if

$$\langle\psi_i|F|\psi_i\rangle = c(F) \tag{1}$$

independent of i for all operators F on T. The set T is authorized if and only if

$$\langle\psi_i|E|\psi_j\rangle = 0 \quad (i \neq j) \tag{2}$$

for all operators E on the complement of T.

If we are to share a quantum secret, then the access structure, in addition to being monotonic, must also satisfy the no-cloning theorem [1]. This implies that no two authorized sets are disjoint. In this case the access structure must satisfy the conditions of Proposition 1 for any state in the space spanned by the encoded states $|\psi_i\rangle$; see [8, Theorem 1].

B. Review of graph-state formalism for quantum secret sharing

In Ref. [3], the quantum secret-sharing protocols were classified as follows:

(i) CC: This protocol deals with the sharing of classical secrets, assuming secure channels between the dealer and players.

(ii) CQ: In this protocol we share classical secrets where we assume that the channels between the dealer and players are susceptible to eavesdropping.

(iii) QQ: This protocol shares quantum secrets using quantum channels which may be public or private.

In this paper we restrict our attention to CC and QQ protocols.

Let G be a graph with vertex set $V(\mathsf{G})$. We denote the neighbors of a vertex $v \in V(G)$ as N_v. We denote the graph obtained by deleting the vertex v from G by $\mathsf{G} \setminus v$. The graph state defined on G is denoted $|\mathsf{G}\rangle$. Recall that the graph state is a stabilizer state and satisfies $K_v|\mathsf{G}\rangle = |\mathsf{G}\rangle$, where

$$K_v = X_v \prod_{u\in N_v} Z_u \quad \text{for all } v \in V(\mathsf{G}). \tag{3}$$

We use the notation $K_A = \prod_{i\in A} K_i$. The stabilizer of $|\mathsf{G}\rangle$ is denoted as $S(|\mathsf{G}\rangle)$. The stabilizer matrix of $|\mathsf{G}\rangle$ is of the form $[I \mid A_{\mathsf{G}}]$, where A_{G} is the adjacency matrix of G.

In the CC quantum secret-sharing protocol, the secret bit s is encoded as

$$\mathcal{E} : s \mapsto Z_A^s|\mathsf{G}\rangle, \tag{4}$$

where $Z_A^s = \prod_{i\in A} Z_i^s$. We denote a CC protocol using the graph G and encoding using the set A by (G, A). An authorized set ω can recover the secret either by performing a joint measurement of an appropriate operator $M \in S(|\mathsf{G}\rangle)$ or by local measurements and combining these results classically (after classical communication), in other words through local operations and classical communication (LOCC).

The QQ protocol can be viewed as an extension of the CC protocol (G, A) where the dealer has the capability to encode a quantum secret. In effect the dealer must realize the following map:

$$\mathcal{E} : a|0\rangle + b|1\rangle \mapsto a|\mathsf{G}\rangle + bZ_A|\mathsf{G}\rangle. \tag{5}$$

In the QQ protocol, the dealer adds an additional ancilla qubit whose state is the secret to be shared. The dealer then encodes this state by a procedure similar to teleportation. Following this the dealer might have to perform some correction operations on the encoded state to ensure that the secret has been properly teleported. The dealer then distributes the qubits to the players. In this setting, authorized subsets of players can reconstruct the secret by means of suitable nonlocal operations. A QQ protocol on an arbitrary graph does not lead to a perfect secret-sharing scheme. In this paper we are concerned only with perfect QQ protocols.

In Ref. [5], the graph-state secret-sharing schemes were characterized in terms of graphical conditions. Define the odd neighborhood of a set $S \subseteq V(\mathsf{G})$ as

$$\text{Odd}(S) = \{v \in V(\mathsf{G}) \text{ such that } |N_v \cap S| = 1 \bmod 2\}. \tag{6}$$

Proposition 2 *(Authorized sets for CC protocol* [5]*).* For the CC classical secret-sharing protocols (G,A) of [3], the secret can be accessed by a set S if there exists $D \subseteq S$ such that

$$D \cup \text{Odd(D)} \subseteq \text{S}, \tag{7}$$

$$|D \cap A| = 1 \bmod 2. \tag{8}$$

Proposition 3 *(Unauthorized sets for CC protocol* [5]*).* For the CC classical secret-sharing protocols of [3] on G, the secret cannot be accessed by a set S if there exists a $K \in V(G) \setminus S$ such that

$$\text{Odd(K)} \cap \text{S} = \text{A} \cap \text{S}. \tag{9}$$

The authors of [5] proved that these two conditions were sufficient and made the observation that it was an open question which graphs satisfy them. That these conditions are necessary and that any subset of $V(G)$ satisfies exactly one of Propositions 2 and 3 was shown in [4, Lemma 2].

The access conditions for QQ secret-sharing schemes are the same as Propositions 2 and 3, except that they must hold both for G and for the so-called *conjugate graph* obtained by complementing G on the subgraph restricted to A.

III. GRAPH-STATE SCHEME FOR GENERAL ACCESS STRUCTURES

A. Classical secrets

In this section we make a connection between the CC protocol in the graph-state formalism and the standard error-correction model. We establish a correspondence between all graph-state schemes sharing one bit and $[[n,1]]$ binary quantum codes. This provides an alternative characterization of the access structure of the CC secret-sharing protocols. Further, Theorem 1 also generalizes the results of [12], which uses CSS codes derived from self-dual codes.

Theorem 1. Let Q be an $[[n,1]]$ quantum code with stabilizer matrix

$$S = \left[\begin{array}{ccc|ccc} I_r & A_1 & A_2 & B & 0 & C \\ 0 & 0 & 0 & D & I_{n-r-1} & E \end{array}\right] = [S_X|S_Z], \tag{10}$$

where $\operatorname{diag}(B + CA_2^t) = 0$. Then Q leads to the CC protocol (G, A), where the adjacency matrix of G is

$$A_{\mathsf{G}} = \begin{bmatrix} B + CA_2^t & A_1 & A_2 \\ A_1^t & 0 & 0 \\ A_2^t & 0 & 0 \end{bmatrix}, \tag{11}$$

and the encoding set $A = \operatorname{supp}([\,C^t \;\; E^t \;\; 1\,])$. A generating set for the access structure of (G, A) is given by

$$\Gamma_{\text{gen}} = \{\operatorname{supp}(g) | g \text{ is an encoded } Z \text{ operator.}\} \tag{12}$$

Proof. One choice of logical X and Z operators for Q is given by

$$\begin{bmatrix} \overline{X} \\ \overline{Z} \end{bmatrix} = \left[\begin{array}{ccc|ccc} 0 & E^t & 1 & C^t & 0 & 0 \\ 0 & 0 & 0 & A_2^t & 0 & 1 \end{array}\right]. \tag{13}$$

Note that the support of $\overline{X}$ is given by $A = \operatorname{supp}([\,C^t \;\; E^t \;\; 1\,])$. Let $|\overline{0}\rangle$ be the state stabilized by S and $\overline{Z}$. Let $|\overline{1}\rangle = \overline{X}|\overline{0}\rangle$. Both $|\overline{0}\rangle$ and $|\overline{1}\rangle$ are not graph states. The stabilizer matrix of $I^{\otimes r} H^{\otimes n-r}|\overline{0}\rangle$ is

$$\begin{bmatrix} S \\ \overline{Z} \end{bmatrix} = \left[\begin{array}{ccc|ccc} I_r & 0 & C & B & A_1 & A_2 \\ 0 & I_{n-r-1} & E & D & 0 & 0 \\ 0 & 0 & 1 & A_2^t & 0 & 0 \end{array}\right],$$

which through subsequent row transformations can be shown to be equivalent to $[I \mid A_{\mathsf{G}}]$. Therefore, $I^{\otimes r} H^{\otimes n-r}|\overline{0}\rangle = |\mathsf{G}\rangle$, as it is stabilized by $[I \mid A_{\mathsf{G}}]$. Further, we have $I^{\otimes r} H^{\otimes n-r}|\overline{1}\rangle = I^{\otimes r} H^{\otimes n-r}\overline{X}|\overline{0}\rangle = Z_A|\mathsf{G}\rangle$. Therefore, up to local Clifford gates, the basis states of the CC secret-sharing scheme induced by (G, A) and the basis states of Q are equivalent.

Furthermore, the secret can be recovered if we can distinguish between the states $|\overline{0}\rangle$ and $|\overline{1}\rangle$. We next show that these states can be distinguished. Let $|\psi_s\rangle = \overline{X}^s|\overline{0}\rangle$, where $s \in \{0,1\}$.

Suppose that $\omega \subseteq \{1, \ldots, n\}$. If ω contains the support of an encoded Z operator, i.e., $\omega \supseteq \operatorname{supp}(\overline{Z})$, then by measuring the logical Z operator we can recover the secret because $\overline{Z}|\psi_s\rangle = \overline{Z}\overline{X}^s|\overline{0}\rangle = (-1)^s\overline{X}^s|\overline{0}\rangle$. Thus ω is an authorized set.

If ω does not contain the support of a logical Z operator, then it is an unauthorized set. Let F be a (Pauli) operator such that $\omega \supseteq \operatorname{supp}(F) \not\supseteq \operatorname{supp}(\overline{Z}M)$, for any $M \in S$. Let $C(S)$ be the centralizer of S. If $F \notin C(S)$, then F is detectable; therefore $\langle\psi_s|F|\psi_s\rangle = 0$. If $F \in \langle i, S\rangle$, then $\langle\psi_s|F|\psi_s\rangle = \alpha$ for some $\alpha \in \{\pm i, \pm 1\}$, independent of s. If $F \in C(S) \setminus \langle i, S\rangle$ and does not contain the support of an encoded Z operator, then it must be an encoded X or Y operator. Since $|\psi_s\rangle = \overline{X}^s|\overline{0}\rangle$, we have $\langle\psi_s|F|\psi_s\rangle = \langle\overline{0}|\overline{X}^s F \overline{X}^s|\overline{0}\rangle = 0$, where we used the fact that $F|\overline{0}\rangle = \alpha|\overline{1}\rangle$ for some nonzero $\alpha \in \mathbb{C}$ when F is an encoded X or Y operator. Therefore, $\langle\psi_s|F|\psi_s\rangle = c(F)$ independent of s for all operators in the support of ω; thus by Proposition 1, ω is unauthorized. (We need to restrict our attention only to Pauli operators [F in Eq. (1)] of Proposition 3) This shows that Γ_{gen} generates the access structure for the secret-sharing scheme.

Since the capacity to distinguish $|\overline{0}\rangle$ and $|\overline{1}\rangle$ enables the recovery of s, the access structure generated by Γ_{gen} must coincide with the access structure as defined by Propositions 2 and 3. Thus the stabilizer code induces the graph-state secret-sharing scheme (G, A). ■

A few remarks are in order with respect to the above theorem.

Remark 1. The requirements on $\operatorname{diag}(B + CA_2^t)$ and the form of the stabilizer matrix are not restrictions because any stabilizer code can be transformed through local Clifford unitaries to a code which satisfies these conditions. These two codes will lead to the same access structure.

Remark 2. Since the standard form of the stabilizer matrix, i.e., Eq. (10), is not unique, the graph-state scheme that can be associated with the quantum code is not unique either. Therefore the same $[[n,1]]$ code can lead to different secret-sharing schemes.

We also note that if $B + CA_2^t = 0$, then G is bipartite. This is the case, for instance, for an $[[n,1]]$ CSS code, for which both B and C are all zero. If A_1 is empty, i.e., $r = n - 1$ in Eq. (10), then in effect we are covering all possible graphs. If $A_2 = 0$, then the access structure is trivial; the minimal access structure contains a singleton set.

Theorem 1 gives a succinct characterization of the access structure; we just need to specify the stabilizer generators and the encoded Z operator. All the authorized sets can then be enumerated. Note that our characterization does not give the minimal access structure but rather a generating set for the access structure. If we want to obtain the minimal access structure, then we need to look only at those encoded Z operators which are also minimal in the sense that they do not properly contain any other encoded Z operator within their support. We make the following observation regarding the size of the authorized sets for secret-sharing schemes coming from CSS codes.

Corollary 2. For the CC secret-sharing scheme in Theorem 1, if Q is a CSS code, then every set $\omega \subseteq \{1, \ldots, n\}$ of size $|\omega| \geqslant r + 1$, is an authorized set. If $|\omega| \leqslant r$ and $n \geqslant 2r + 1$, then $\overline{\omega}$ is authorized.

Proof. Let $(a|b) = (a_1, \ldots, a_n | b_1, \ldots, b_n) \in \mathbb{F}_2^{2n}$ be an encoded operator of Q. Then it must satisfy $S_X b^t + S_Z a^t = 0$, where S_X and S_Z are as defined in Eq. (10). If Q is a CSS code, then B and C in Eq. (10) are both zero; further for the encoded Z operator $a = 0$ and b is simply any combination of linearly dependent columns of the matrix $S_X = [\begin{smallmatrix} I_r & A_1 & A_2 \\ 0 & 0 & 0 \end{smallmatrix}]$. Since the rank of S_X is r, any collection of $|\omega| \geqslant r + 1$ columns will be dependent and they must contain the support of an encoded operator. If $|\omega| < r + 1$, then $|\overline{\omega}| \geqslant n - |\omega| \geqslant n - r \geqslant 2r + 1 - r \geqslant r + 1$; thus $\overline{\omega}$ must contain an encoded Z operator and $\overline{\omega}$ must be authorized. ■

Theorem 1 shows that any $[[n,1]]$ code can be used to realize a graph-state quantum secret-sharing scheme. The converse, namely, that every graph-state secret-sharing scheme leads to an $[[n,1]]$ code, is straightforward, but we include it for completeness.

Corollary 3. Every (G, A) CC secret-sharing scheme corresponds to a $[[|V(\mathsf{G})|,1]]$ stabilizer code and vice versa. If G is bipartite and A is a subset of one of the bipartitions, then (G, A) corresponds to a $[[|V(G)|,1]]$ CSS code up to local Clifford gates.

Proof. We only sketch the proof. Suppose we have a (G, A) graph-state secret-sharing scheme. Then the two states $|\mathsf{G}\rangle$ and $Z_A|\mathsf{G}\rangle$ are both stabilized by a subgroup of $S(|\mathsf{G}\rangle)$. The stabilizer of $|\mathsf{G}\rangle$ is given in Eq. (3). Pick an arbitrary element

a in A and form the following group:

$$S = \left\langle K_v' \middle| \begin{array}{ll} K_v' = K_v & v \in \overline{A} \\ K_v' = K_v K_a & v \in A \end{array} \right\rangle .$$

As S is subgroup of $S(|\mathsf{G}\rangle)$, it obviously stabilizes $|\mathsf{G}\rangle$. The operator Z_A anticommutes with K_v, if and only if $v \in A$. Because $\{Z_A, K_a\} = 0$, S also stabilizes $Z_A|\mathsf{G}\rangle$. Since S has $|V(\mathsf{G})| - 1$ generators it defines a $[[|V(\mathsf{G})|,1]]$ code. We can choose Z_A and K_a to be the logical X and Z operators for this code, respectively.

(Although S is sufficient to characterize the code, we can actually show that the authorized sets of (G, A) are also related to the code. If B is an authorized set, then by Proposition 2, B contains a set D satisfying Eqs. (7) and (8). It can be easily verified that for such a set, $\{K_D, Z_A\} = 0$ and $\text{supp}(K_D) = D \cup \text{Odd}(D)$. Clearly, $[K_a, K_D] = 0$; thus K_D is an encoded Z operator and every authorized set contains the support of an encoded Z operator.) The preceding discussion together with Theorem 1 proves the first part of the corollary.

For the second part let V_l, V_r be the bipartition of $V(\mathsf{G})$, with $A \subseteq V_r$. Then observe that conjugation of S by $I^{\otimes |V_l|} H^{\otimes |V_r|}$ gives a stabilizer generated by X-only and Z-only generators, i.e., a CSS code. ■

A subtle point must be kept in mind when dealing with the correspondence in Corollary 3, namely, it is not a one-to-one correspondence between an $[[n,1]]$ code and a CC secret-sharing scheme. Many $[[n,1]]$ codes could lead to the same CC secret-sharing scheme. Further, given an $[[n,1]]$ code, different choices of the logical operators could also lead to different secret-sharing schemes.

Recall that a pure-state scheme is one in which a pure state is encoded into a pure state. In a mixed-state scheme a pure state could be encoded into a mixed state. Such schemes could be more efficient than the pure-state schemes. The framework of quantum codes makes it possible to use mixed states for sharing classical secrets with higher efficiency than a purely classical scheme, [8, Theorem 11]. At the present it is not clear how to include those schemes in the graph-state formalism.

B. Quantum secrets

Every graph leads to a CC secret-sharing scheme, but it appears that every graph does not lead to a perfect QQ secret-sharing scheme. In this section, we show that a large class of bipartite graphs lead to QQ secret-sharing schemes for nonthreshold access structures.

Recall that every QQ secret-sharing scheme includes a step where the dealer encrypts the secret before distributing the shares. In Refs. [3,7], this was broken down into the following steps: (i) The dealer prepares a graph state over the dealer's qubit and the players' qubits. (ii) An ancilla qubit prepared in the secret state is entangled with the dealer's qubit. (iii) The ancilla and dealer's qubits are measured in the Bell basis leading to an encoded teleporation onto the players' qubits. In this paper we simplify these steps by involving only one additional qubit, namely, the dealer's qubit. We make use of the teleportation scheme to encode into a quantum code using graph states; see [13,14].

Before we give our construction (Theorem 4), we illustrate it through an example. Consider the graph shown in Fig. 1.

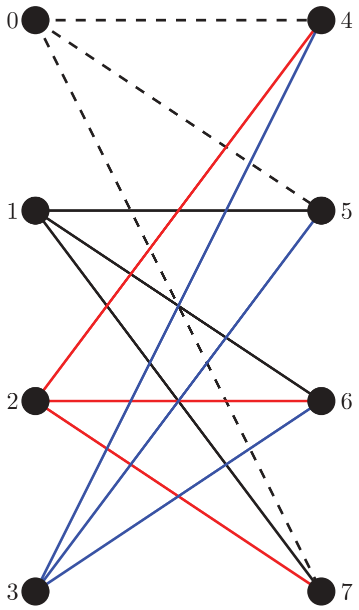

FIG. 1. (Color online) A general QQ secret-sharing scheme from a bipartite graph. All qubits except the dealer's qubit are prepared in the $|+\rangle$ state, while the dealer's qubit (0) is prepared in the secret state. Then we apply CZ gates along the edges of G. The dealer's qubit is then measured in the σ_x basis. A correction operator $K_j' = X_j \prod_{k \in N_j \setminus 0} Z_k$, where $j \in N_0$ is applied if we measure 1.

Pick any vertex of the graph; say we pick 0. The dealer prepares this qubit in the secret state to be shared. Then this qubit is entangled with the qubits in N_0 using CONTROLLED-Z gates. Then we measure the dealer's qubit in the σ_x basis. If we measure 0, then the secret has been encoded as desired, otherwise, we need to apply a correction of the encoded Z on the state. The qubits are then distributed to the players.

Consider the secret being encoded into $Z_A^s|\mathsf{G} \setminus 0\rangle$, where $A = \{4,5,7\}$. Then it can be verified that all the minimal authorized sets given in $\Gamma_{0,\,\min}$ satisfy both Eqs. (7) and (8) for both $\mathsf{G} \setminus 0$ and the conjugate graph with respect to A (which is obtained by taking the complement of $\mathsf{G} \setminus 0$ on A):

$$\Gamma_{0,\,\min} = \left\{ \begin{array}{c} \{1,2,7\}; \{1,3,5\}; \{1,4,6\}; \{2,3,4\}; \\ \{2,5,6\}; \{3,6,7\}; \{4,5,7\} \end{array} \right\}. \qquad (14)$$

We now give the construction for QQ secret-sharing schemes with arbitrary access structures.

Theorem 4. Let G be a bipartite graph whose adjacency matrix A_{G} is given by

$$A_{\mathsf{G}} = \begin{bmatrix} 0 & P \\ P^t & 0 \end{bmatrix}, \quad \text{where } PP^t = I. \qquad (15)$$

Then for every vertex i we can define a perfect QQ quantum secret-sharing scheme from G. The encoding for the quantum secret-sharing scheme is given by

$$\mathcal{E} : a|0\rangle + b|1\rangle \mapsto a|\mathsf{G} \setminus i\rangle + bZ_{N_i}|\mathsf{G} \setminus i\rangle. \qquad (16)$$

A generating set for the access structure Γ_i is given by the following:

$$\Gamma_{i,\text{gen}} = \left\{ D \cup \text{Odd}(D) \setminus i \middle| \begin{array}{c} D \subseteq V_r \\ |D \cap N_i| = 1 \bmod 2 \end{array} \right\}, \qquad (17)$$

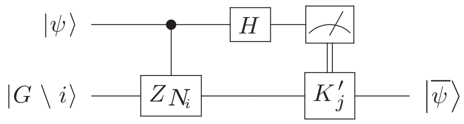

FIG. 2. Encrypting the secret state $|\psi\rangle$ for QQ secret sharing using teleportation. The operator $K'_j = X_j\prod_{k\in N_j\setminus i} Z_k$ is such that $j\in N_i$. It is applied only if the measurement outcome is 1.

where V_r is the bipartition of vertices of G that does not contain i. The encryption and recovery of the secret are as shown in Figs. 2 and 3, respectively.

Proof. We shall prove this theorem in parts. For convenience, we shall ignore the normalization factors for quantum states.

(i) Encryption of the secret: Assume that the secret to be encoded is $|\psi\rangle = a|0\rangle + b|1\rangle$. Then it can be easily verified that in Fig. 2 the state $|\psi\rangle|\mathsf{G}\setminus i\rangle$ is transformed to the following state prior to measurement (up to normalization):

$$|0\rangle(a|\mathsf{G}\setminus i\rangle + bZ_{N_i}|\mathsf{G}\setminus i\rangle) + |1\rangle(a|\mathsf{G}\setminus i\rangle - bZ_{N_i}|\mathsf{G}\setminus i\rangle).$$

If we measure zero, then we get the desired state but if we measure 1, then we have to apply the correction operator

$$K'_j = X_j \prod_{k\in N_j\setminus i} Z_k \tag{18}$$

for any $j\in N_i$. Observe that $[K_i,K_j] = [X_iZ_{N_i}, Z_iK'_j] = 0$; therefore, $\{Z_{N_i}, K'_j\} = 0$. Thus K'_j anticommutes with the Z_{N_i}. It can also be verified that K'_j stabilizes $|\mathsf{G}\setminus i\rangle$; therefore it acts as a correction operator to give the state in Eq. (16).

(ii) Recovery: Before we show that $D\cup \mathrm{Odd}(D)\setminus i$ is authorized, we need the following operators. Let $K_D = \prod_{j\in D} K_j$; because G is bipartite, $\mathrm{supp}(K_D) = D\cup\mathrm{Odd}(D)$. By assumption $|D\cap N_i| = 1 \bmod 2$; therefore, $i\in\mathrm{Odd}(D)\subseteq \mathrm{supp}(K_D)$. Define now K'_D as

$$K'_D = Z_iK_D = \prod_{j\in D} X_j \prod_{k\in\mathrm{Odd}(D)\setminus i} Z_k. \tag{19}$$

Note that K'_D stabilizes $|\mathsf{G}\setminus i\rangle$. Further, $[K_i,K_D] = [X_iZ_{N_i}, Z_iK'_D] = 0$; therefore, $\{Z_{N_i},K'_D\} = 0$.

Consider the operator $K_{\mathrm{Odd}(D)}$. Define $K'_{\mathrm{Odd}(D)}$

$$K'_{\mathrm{Odd}(D)} = X_iK_{\mathrm{Odd}(D)} = \prod_{j\in\mathrm{Odd}(D)\setminus i} X_j \prod_{k\in D} Z_k. \tag{20}$$

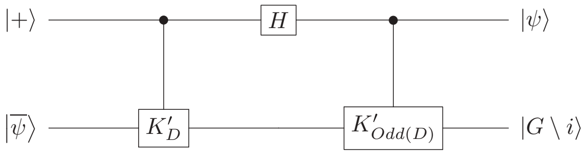

FIG. 3. Reconstructing the secret state $|\psi\rangle$ for QQ secret sharing given an authorized set D as in Eq. (17). The operator $K'_D = Z_i\prod_{j\in D}K_j = \prod_{j\in D}X_j\prod_{k\in\mathrm{Odd}(D)\setminus i}Z_k$ and $K'_{\mathrm{Odd}(D)} = \prod_{j\in D}Z_j\prod_{k\in\mathrm{Odd}(D)\setminus i}X_k$.

Because $K_{\mathrm{Odd}(D)}$ is also in $S(|\mathsf{G}\rangle)$ we have

$$\begin{aligned}|\mathsf{G}\rangle &= |0\rangle|\mathsf{G}\setminus i\rangle + |1\rangle Z_{N_i}|\mathsf{G}\setminus i\rangle,\\ &= K_{\mathrm{Odd}(D)}|\mathsf{G}\rangle = X_iK'_{\mathrm{Odd}(D)}|\mathsf{G}\rangle,\\ &= |1\rangle K'_{\mathrm{Odd}(D)}|\mathsf{G}\setminus i\rangle + |0\rangle K'_{\mathrm{Odd}(D)}Z_{N_i}|\mathsf{G}\setminus i\rangle.\end{aligned}$$

Hence, $K'_{\mathrm{Odd}(D)}Z_{N_i}$ stabilizes $|\mathsf{G}\setminus i\rangle$.

We now show that the set $D\cup\mathrm{Odd}(D)\setminus i$ as in Eq. (17) is authorized; note that it satisfies the requirements of Proposition 2 If we trace through the circuit given in Fig. 3, the state transforms as follows:

$$\begin{aligned}|+\rangle|\overline{\psi}\rangle &= (|0\rangle+|1\rangle)(a|\mathsf{G}\setminus i\rangle + bZ_{N_i}|\mathsf{G}\setminus i\rangle)\\ &\xrightarrow{c-K'_D} |0\rangle(a|\mathsf{G}\setminus i\rangle + bZ_{N_i}|\mathsf{G}\setminus i\rangle)\\ &\quad +|1\rangle(aK'_D|\mathsf{G}\setminus i\rangle + bK'_DZ_{N_i}|\mathsf{G}\setminus i\rangle)\\ &\xrightarrow{H} a|0\rangle|\mathsf{G}\setminus i\rangle + b|1\rangle Z_{N_i}|\mathsf{G}\setminus i\rangle\\ &\xrightarrow{c-K'_{\mathrm{Odd}(D)}} a|0\rangle|\mathsf{G}\setminus i\rangle + b|1\rangle|\mathsf{G}\setminus i\rangle\\ &= (a|0\rangle + b|1\rangle)|\mathsf{G}\setminus i\rangle,\end{aligned}$$

where we used the fact that $K'_{\mathrm{Odd}(D)}Z_{N_i}$ stabilizes $|\mathsf{G}\setminus i\rangle$. Thus $D\cup\mathrm{Odd}(D)\setminus i$ is able to reconstruct the quantum secret $|\psi\rangle$. The no-cloning theorem now implies that the complement of this set is unauthorized.

(iii) Completeness of $\Gamma_{i,\mathrm{gen}}$: Now we show that the access structure as defined in Eq. (17) is complete in the sense that every authorized set contains some element of $\Gamma_{i,\mathrm{gen}}$. Assume that there exists some set A which is authorized but not generated by $\Gamma_{i,\mathrm{gen}}$. The encoding in Eq. (16) can also be used to realize a CC secret-sharing scheme, namely, $(\mathsf{G}\setminus i, N_i)$. For this CC protocol A is an authorized set. But then by Proposition 2, A contains some set D such that $D\cup\mathrm{Odd}(D)\subseteq A$ and $|D\cap N_i| = 1 \bmod 2$, where the odd neighborhood of D is being considered with respect to $\mathsf{G}\setminus i$. Because $\mathsf{G}\setminus i$ is bipartite, this can happen only if $D\subseteq V_r$. Because $|D\cap N_i| = 1 \bmod 2$, $\mathrm{Odd}(D)$ must also contain i with respect to G. But then $D\cup\mathrm{Odd}(D)\setminus i$ is in $\Gamma_{i,\mathrm{gen}}$. This shows that every authorized set is generated by $\Gamma_{i,\mathrm{gen}}$.

(iv) Perfectness of $\Gamma_{i,\mathrm{gen}}$: To show that the scheme is perfect, we must show that every set is either authorized or unauthorized. Alternatively, the complement of every unauthorized set is authorized, [1, Corollary 8]. Assume that the set $B\subseteq V(\mathsf{G}\setminus i)$ is unauthorized. Then for the CC protocol $(\mathsf{G}\setminus i, N_i)$, B is either authorized or unauthorized by [4, Lemma 2]. If it is authorized for $(\mathsf{G}\setminus i, N_i)$, then by proceeding as in (iii), we can show that it can also recover the quantum secret contradicting that B is unauthorized. Therefore, B must be unauthorized for $(\mathsf{G}\setminus i, N_i)$. By Corollary 3, it is equivalent to a $[[|V(G)|-1,1]]$ quantum code. In particular, the stabilizer matrix of the associated quantum code, written in standard form as in Eq. (10), has $r = |V(G)|/2 - 1$. By Corollary 2, B can be unauthorized only if $|B|\leqslant r$. But then $|\overline{B}| \geqslant |V(G)| - 1 - |V(G)|/2 + 1 \geqslant r+1$. Thus $\overline{B}$ is authorized for $(\mathsf{G}\setminus i, N_i)$. Once again using arguments similar to (iii), we conclude that $\overline{B}$ is authorized. This shows that the proposed protocol is perfect.

This completes the proof that the proposed scheme realizes a perfect QQ protocol. ■

The access structure realized by the scheme in Theorem 4 is the same as the access structure realized by the quantum secret-sharing scheme using the approach of quantum error-correcting codes as the following result shows.

Corollary 5. Let Q be an $[[n,0]]$ CSS code, with the stabilizer matrix

$$S = \left[\begin{array}{cc|cc} I & P & 0 & 0 \\ 0 & 0 & I & P \end{array}\right], \tag{21}$$

where $PP^t = I$. Then the $[[n-1,1]]$ quantum code obtained by puncturing the ith qubit realizes the QQ secret-sharing protocol of Theorem 4.

Proof. It suffices to show that the quantum states in Eq. (16) form a basis for the quantum code obtained by puncturing the ith qubit. Without loss of generality we can assume that we puncture the 0th qubit. Let $P = [\begin{smallmatrix} g \\ Q \end{smallmatrix}]$, where $(0|g) \in \mathbb{F}_2^n$ and $\operatorname{supp}(0|g) = N_i$. Note that $g \neq 0$ because of the requirement $PP^t = I$. Then puncturing the ith qubit results in an $[[n-1,1]]$ quantum code. The stabilizer matrix for this code is

$$\left[\begin{array}{cc|cc} I & Q & 0 & 0 \\ 0 & 0 & I & Q \end{array}\right],$$

while the encoded operators are given by

$$\begin{bmatrix} \overline{X} \\ \overline{Z} \end{bmatrix} = \left[\begin{array}{cc|cc} 0 & g & 0 & 0 \\ 0 & 0 & 0 & g \end{array}\right].$$

Consider the state $|\overline{0}\rangle$ stabilized by S and $\overline{Z}$. Its stabilizer matrix is

$$\left[\begin{array}{cc|cc} I & Q & 0 & 0 \\ 0 & 0 & 0 & g \\ 0 & 0 & I & Q \end{array}\right].$$

This matrix, using $PP^t = I$, can be transformed to

$$\left[\begin{array}{cc|cc} I & Q & 0 & 0 \\ 0 & 0 & Q^t & I \end{array}\right].$$

This is precisely the stabilizer of the state $I^{\otimes n/2-1}H^{\otimes n/2}|\mathsf{G}\setminus i\rangle$. Thus $I^{\otimes n/2-1}H^{\otimes n/2}|\overline{0}\rangle = |\mathsf{G}\setminus i\rangle$ and $I^{\otimes n/2-1}H^{\otimes n/2}\overline{X}|\overline{0}\rangle = Z_{N_i}|\mathsf{G}\setminus i\rangle$. ■

With respect to the sharing of quantum secrets we have considered only those schemes arising from bipartite graphs; in terms of quantum codes they correspond to CSS codes. As such they do not exhaust all possible access structures. For instance, the ((3,5)) threshold scheme can be realized using a [[5,1,3]] code, which is not a CSS code. It is possible to extend the ideas presented in this paper to the more general case when the graph is not bipartite, but we do not have a simple classification of graphs which lead to perfect QQ secret-sharing schemes. Although given a graph and an encoding set we can check if it leads to a QQ secret-sharing scheme (see [5] and [4, Corollary 3]), this is not efficient, in that we must check for all possible encoding sets. In contrast, the present result gives a class of graphs which are guaranteed to lead to perfect QQ schemes; additionally, the encoding sets are also defined based on the graph. (Please note that a similar problem exists even when the question is formulated in terms of quantum codes. Although the results in Ref. [1] (see Theorem 7 therein) can be used to find out if a given quantum code can be viewed as a secret-sharing scheme but it also involves exhaustive checking.)

Before we conclude this section, we demonstrate the usefulness of our results by showing how they can help in answering some questions related to the graph-state formalism. Just as every CC scheme is a quantum code, every QQ scheme is also a quantum code by Ref. [1, Proposition 6].

Theorem 6. There do not exist any graph-state $((k,2k-1))$ QQ secret-sharing protocols if $k \geqslant 4$.

Proof. In Ref. [15], it was shown that every $((k,2k-1))$ quantum threshold secret-sharing scheme is a $[[2t-1,1,t]]$ quantum maximum distance separable (MDS) code. In Ref. [10], it was shown that there do not exist any $[[n,1]]$ binary quantum MDS codes of length greater than 5. It follows, therefore, that there are no (pure-state) QQ quantum threshold schemes of length $2k-1$ greater than 5; equivalently $k \geqslant 4$. ■

Please note that Theorem 6 refers only to perfect QQ protocols using qubits. If we use qudits, then it is possible to realize a $((k,2k-1))$ quantum threshold secret-sharing scheme for any k; see [1, Theorem 5]. Such schemes can share a qudit of higher dimension, thus using them to share only a qubit would mean lower efficiency. The existence of quantum threshold schemes was studied at great length in Ref. [4]. Through the connection to quantum codes we are able to shed light on this issue, immediately improving upon the bound in Ref. [4, Corollary 4].

IV. CONCLUSION

In this paper we have elucidated the connection between graph-state secret-sharing schemes [3] and those based on quantum error-correcting codes [1,8]. In particular, we have shown that CC secret-sharing protocols arise from $[[n,1]]$ quantum codes. We also characterized the access structure of these schemes in terms of the encoded operators of the associated quantum code. Further, we bounded the maximal size of an unauthorized set when the schemes are based on CSS codes.

We also showed that a class of $[[n,1]]$ CSS codes are in correspondence with QQ protocols for sharing a qubit. As a consequence we were able to construct quantum secret-sharing schemes with arbitrary access structures in the graph-state formalism. Although these access structures can be realized by secret-sharing schemes based on quantum codes, our results close some gaps in our understanding of graph-state protocols for nonthreshold access structures. They also lead to a partial classification of graphs which lead to perfect QQ protocols.

Our results also lead to a better understanding of the graph-state protocols. We showed, in particular, how they can address questions related to graph-state secret sharing. Many of the ideas presented here, with respect to the encoding, recovery, and characterization of the access structure could be useful even when the QQ protocol is based on nonbipartite graphs.

ACKNOWLEDGMENTS

I would like to thank Ben Fortescue for helpful discussions and Ken Brown for supporting this research. I also thank an anonymous referee for making helpful comments to improve the paper.

[1] R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999).

[2] M. Hillery, V. Buzek, and A. Berthaume, Phys. Rev. A **59**, 1829 (1999).

[3] D. Markham and B. C. Sanders, Phys. Rev. A **78**, 042309 (2008).

[4] J. Javelle, M. Mhalla, and S. Perdrix, arXiv:1109.1487.

[5] E. Kashefi, D. Markham, M. Mhalla, and S. Perdrix, Electronic Proceedings of Theoretical Computer Science **9**, 87 (2009).

[6] S. Gravier, J. Javelle, M. Mhalla, and S. Perdrix, arXiv:1112.2495.

[7] A. Keet, B. Fortescue, D. Markham, and B. C. Sanders, Phys. Rev. A **82**, 062315 (2010).

[8] D. Gottesman, Phys. Rev. A **61**, 042311 (2000).

[9] A. Smith, arXiv:quant-ph/0001087.

[10] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, IEEE Trans. Inf. Theory **44**, 1369 (1998).

[11] D. Gottesman, Ph.D. thesis, Caltech, arXiv:quant-ph/9705052.

[12] P. K. Sarvepalli and A. Klappenecker, Phys. Rev. A **80**, 022321 (2009).

[13] M. Grassl, in *Proceedings of the Third International Workshop Coding and Cryptology*, Lecture Notes in Computer Science, edited by Y. M. Chee *et al.* (Springer, Berlin, 2011), p. 142.

[14] M. Hein, J. Eisert, and H. J. Briegel, Phys. Rev. A **69**, 062311 (2004).

[15] K. Rietjens, B. Schoenmakers, and P. Tuyls, in *Proceedings of the 2005 IEEE International Symposium on Information Theory, Adelaide, Australia* (IEEE, Piscataway, NJ, 2005), pp. 1598–1302.