# Matroids and quantum-secret-sharing schemes

Pradeep Sarvepalli* and Robert Raussendorf
*Department of Physics and Astronomy, University of British Columbia, Vancouver V6T 1Z1, Canada*
(Received 26 October 2009; published 24 May 2010)

A secret-sharing scheme is a cryptographic protocol to distribute a secret state in an encoded form among a group of players such that only authorized subsets of the players can reconstruct the secret. Classically, efficient secret-sharing schemes have been shown to be induced by matroids. Furthermore, access structures of such schemes can be characterized by an excluded minor relation. No such relations are known for quantum secret-sharing schemes. In this paper we take the first steps toward a matroidal characterization of quantum-secret-sharing schemes. In addition to providing a new perspective on quantum-secret-sharing schemes, this characterization has important benefits. While previous work has shown how to construct quantum-secret-sharing schemes for general access structures, these schemes are not claimed to be efficient. In this context the present results prove to be useful; they enable us to construct efficient quantum-secret-sharing schemes for many general access structures. More precisely, we show that an identically self-dual matroid that is representable over a finite field induces a pure-state quantum-secret-sharing scheme with information rate 1.

DOI: 10.1103/PhysRevA.81.052333 PACS number(s): 03.67.Dd, 03.67.Pp

## I. INTRODUCTION

Secret sharing is an important cryptographic primitive originally motivated by the need to distribute secure information among parties some of whom are untrustworthy [1,2]. Additionally, it finds applications in secure multiparty computation [3,4]. Secret-sharing schemes have a rich mathematical structure [5] and they have been shown to be closely associated with error-correcting codes [4,6,7] and matroids [4,8–10,12,32]. The interplay with these objects has enabled us to obtain new insights about not only secret-sharing schemes but also codes and matroids. Although relatively new, the field of quantum secret sharing [13] has made rapid progress both theoretically [14–20] and experimentally [21–24]. However, its connections with other mathematical disciplines have not been as well studied. In particular, no connections have been made with the theory of matroids, which is in sharp contrast to the classical scenario. These connections are of more than theoretical interest. Classically, optimal secret-sharing schemes, that is, those with information rate 1, are induced by matroids. Additionally, matroids provide alternate methods to prove bounds on the rates that can be achieved for certain access structures. For all these reasons it is useful to develop the theory of matroids and quantum-secret-sharing schemes.

In this paper it is our goal to bring to bear the theory of matroids to characterize quantum-secret-sharing schemes. While our results are only the first steps toward this characterization, they do indicate the usefulness of such associations. The paper is organized as follows. We begin with a brief review of the necessary background in secret sharing. In Sec. II we review some of the known results on classical secret-sharing schemes and matroids; these results are not well known in the quantum information community and also provide the backdrop for generalizing the connections between matroids and secret-sharing schemes. In Sec. III we prove the central result of this paper, namely, how representable identically self-dual matroids lead to efficient quantum-secret-sharing schemes. We assume that the reader is familiar with the basic results on quantum computing and stabilizer codes.

### A. Classical secret sharing

A secret-sharing scheme is a protocol to distribute a secret $s$ among a set of players $P$, by a dealer $D$, such that only authorized subsets of $P$ can reconstruct the secret. Subsets of $P$ which cannot reconstruct the secret are called unauthorized sets. The access structure $\Gamma$ consists of all subsets that can reconstruct the secret. The adversary structure $\mathcal{A}$ consists of all unauthorized subsets. Any access structure $\Gamma$ is required to satisfy the monotone property; that is, if $A \in \Gamma$, then any set $B \supseteq A$ is also in $\Gamma$. This is the only restriction on the access structures for classical secret-sharing schemes. Any access structure satisfying the monotone property can be realized by an appropriate secret-sharing scheme, albeit with great complexity (see, e.g., [12]). A secret-sharing scheme is said to be perfect if the unauthorized sets cannot extract any information about the secret. A precise information theoretic formulation can be given that quantifies this condition. We typically require the secret to be taken from a finite alphabet, $\mathcal{K}$. The shares distributed need not be in the same domain as the secret; in fact each share can be in a domain of different alphabet. Let the domain of the $i$th party be $\mathcal{S}_i$. An important metric of performance for secret-sharing schemes is the information rate $\rho$. This is defined as (see [12])

$$\rho = \min_i \frac{\log_2 |\mathcal{K}|}{\log_2 |\mathcal{S}_i|}. \tag{1}$$

Secret-sharing schemes with $\rho = 1$ are said to be ideal. The associated access structure is said to be ideal. More generally, if an access structure can be realized with information rate 1 for some secret-sharing scheme, then it is said to be ideal. Note that we do not restrict the dimension of the secret in this case. An important problem of secret sharing is to construct ideal secret-sharing schemes for any given (monotone) access structure. Not every access structure can be realized with an

*pradeep@phas.ubc.ca

information rate of 1 [25]; see [12] for examples of access structures which cannot be realized with information rate 1.

### B. Quantum secret sharing

A quantum-secret-sharing scheme generalizes the classical one in two possible ways. We use quantum states to share either a secret quantum state or a classical secret. We assume that the shares are distributed by means of a completely positive trace-preserving map.[1] Some authors refer to the first case as quantum state sharing, reserving the term "quantum secret sharing" for situations where the secret is shared in an adversarial setting. Although this might be preferable in some contexts, we will continue to use the traditional terminology. Quantum-secret-sharing schemes for classical secrets were introduced by Hillery *et al.* in [13]. They also proposed schemes for sharing quantum secrets, however, these are not perfect, that is, unauthorized sets can extract some information about the secret. Cleve *et al.* [14] proposed the first perfect quantum-secret-sharing schemes for quantum secrets. The theory of quantum secret sharing was developed further, making important connections with quantum coding theory in [14] and [15], with quantum information theory in [16] and [19], and, more recently, with graphs via labeled graph states in [18].

In this paper we are concerned with (perfect) sharing of quantum secrets. Unlike classical secret-sharing schemes, a quantum-secret-sharing scheme cannot realize every monotone access structure. An additional constraint due to the "no-cloning theorem" [26,27] has to be imposed on a realizable access structure. Recall that the no-cloning theorem states that an arbitrary quantum state cannot be copied. In any quantum-secret-sharing scheme we cannot have two disjoint authorized sets in the access structure, as this would violate the no-cloning theorem. This condition in conjunction with the monotonicity of the access structure determines the allowed access structures for all quantum-secret-sharing schemes [15, Theorem 8]. The same condition has been stated in different forms in the literature. We record this result in its various forms for future use. First, we need the notion of dual for a collection of sets. Let $P$ be a set, then we denote the powerset of $P$ as $2^P$. For any subset $A \subseteq 2^P$, we define the dual of $A$ as

$$A^* = \{x \subset P \mid \overline{x} \notin A\}. \tag{2}$$

*Lemma 1. Self-orthogonal access structures.* Let $\Gamma$ be the access structure and $\mathcal{A}$ the adversary structure of a secret-sharing scheme. Then the following statements are equivalent:

$$A \cap B \neq \emptyset \text{ for all } A, B \in \Gamma. \tag{3}$$

$$\Gamma \subseteq \Gamma^*. \tag{4}$$

$$\mathcal{A}^* \subseteq \mathcal{A}. \tag{5}$$

Further, every such $\Gamma$ can be realized by a quantum-secret-sharing scheme.

*Proof.* We shall show that (3) $\Rightarrow$ (4). It follows that if $A \in \Gamma$, then $\overline{A} \notin \Gamma$ as $A \cap \overline{A} = \emptyset$. But $\Gamma^* = \{B \mid \overline{B} \notin \Gamma\}$. Since $\overline{A} \notin \Gamma$, it follows that $A \in \Gamma^*$ and $\Gamma \subseteq \Gamma^*$. Conversely, let $\Gamma \subseteq \Gamma^*$. Then from the definition of $\Gamma^*$, it follows that for any $A \in \Gamma$, we must have $\overline{A} \notin \Gamma$; that is, $\overline{A} \in \mathcal{A}$. Further, all subsets of $\overline{A}$ are also in $\mathcal{A}$. Now assume that there exists some $B \in \Gamma$ such that $A \cap B = \emptyset$. Then $B \subseteq \overline{A}$. But all subsets of $\overline{A} \in \mathcal{A}$; that is, they are not in $\Gamma$, which contradicts that $B \in \Gamma$. Therefore there exists no subset $B \in \Gamma$ such that $A \cap B = \emptyset$, proving that (4) $\Rightarrow$ (3).

Now we shall show that (4) $\Leftrightarrow$ (5). Assume that (4) holds. Then since $\Gamma \cap \mathcal{A} = \emptyset$ and $\Gamma \cup \mathcal{A} = 2^P = \Gamma^* \cup \mathcal{A}^*$, we have that $\mathcal{A} = (\Gamma^* \cup \mathcal{A}^*) \setminus \Gamma = (\Gamma^* \setminus \Gamma) \cup \mathcal{A}^*$, where we used the fact that $\Gamma^* \cap \mathcal{A}^* = \emptyset$ and $\Gamma \subseteq \Gamma^*$. It now follows that $\mathcal{A}^* \subseteq \mathcal{A}$, and (5) holds. Now assume that (5) holds, then again, we have $\Gamma \cup \mathcal{A} = \Gamma^* \cup \mathcal{A}^*$, and this time we can write $\Gamma^* = (\Gamma \cup \mathcal{A}) \setminus \mathcal{A}^* = (\Gamma^* \setminus \Gamma) \cup \mathcal{A}^*$, and therefore $\Gamma^* \supseteq \Gamma$ and (4) holds. This establishes the equivalence of these three conditions. That an access structure satisfying these conditions can be realized follows from [15, Theorem 8]. ∎

We often refer to an access structure that is realizable by a quantum-secret-sharing scheme as a quantum access structure. Smith [28, Theorem 1] characterized the adversary structure of quantum-secret-sharing schemes as in (5). Condition (4) is somewhat reminiscent of the requirement for self-orthogonal classical codes for quantum error correction. If $\Gamma = \Gamma^*$, then we say that the access structure is self-dual.

A quantum-secret-sharing scheme which encodes a pure-state secret into a global pure state is said to be a pure-state scheme, and one that encodes into a global mixed state is a mixed-state scheme. Self-dual access structures can be realized by pure-state schemes, whereas non-self-dual access structures can be realized only as mixed-state schemes. This is a consequence of Corollary 8 in Ref. [14], which states that in every pure-state scheme, the complement of any unauthorized set is an authorized set, and vice versa. Consequently, we must have $|\Gamma| = |\mathcal{A}|$, but $|\mathcal{A}| = |\Gamma^*|$, and since $\Gamma \subseteq \Gamma^*$, this is possible if and only if $\Gamma = \Gamma^*$. A theorem [15, Theorem 3] due to Gottesman shows that every mixed-state scheme can be derived from a pure-state scheme. So we do not lose any generality by focusing on the pure-state schemes. The simplest access structures are the $((k,n))$ threshold access structures—in this case, the authorized sets are any subset of size $\geqslant k$ and unauthorized sets are subsets of cardinality less than $k$. Smith [28] and, independently, Gottesman [15] showed how to construct quantum-secret-sharing schemes with general access structures.

In studying general access structures it is often convenient to work with the minimal access structures, which are the generating sets of the access structures. We define the minimal access structure $\Gamma_{\min}$ of the access structure $\Gamma$ as

$$\Gamma_{\min} = \{A \in \Gamma \mid B \not\subset A \text{ for any } B \in \Gamma\}. \tag{6}$$

If every party in $P$ occurs in at least one minimal authorized set of $\Gamma$, then we say that the access structure is connected. We restrict our attention to such access structures in this paper. Our primary goal in this paper is to explore connections of quantum-secret-sharing schemes with matroids and to characterize the associated access structures in terms of matroids if possible. We also address the construction of secret-sharing schemes. Our constructions make use of CSS

[1] We thank an anonymous referee for emphasizing this.

codes [29] reminiscent of the constructions of Smith for general access structures.

The efficiency of a quantum-secret-sharing scheme is quantified in terms of a metric called the quantum information rate, analogous to the information rate of classical schemes. This metric was first explicitly defined in [16] in terms of the von Neumann entropies of the secret and the shares; a notion of efficiency in terms of size of shares with respect to the secret was implicit in [15]. For our purposes it suffices to know that the quantum information rate, as in the classical case, is upper bounded by 1 [16, Corollary 7]. A quantum-secret-sharing scheme with rate 1 is said to be ideal. Alternatively, an ideal quantum-secret-sharing scheme is one in which the sizes of the secret and of each share are the same.

## II. MATROIDS AND SECRET SHARING

Matroids have been associated with secret-sharing schemes [4,9]; see [12] for a brief overview of some of the main results. Secret-sharing schemes which are induced by a matroid are called matroidal. Useful results with respect to characterization and performance of secret-sharing schemes can be derived by means of such an association, [8,9]. Such an association also implies an implicit correspondence between matroids and access structures. In fact, classically, most of the associations focus on this correspondence and tend to ignore the scheme realizing the access structure. To a large extent we take the same approach, however, since a given access structure might not be a quantum access structure, we do bear in mind that we cannot entirely ignore the fact that the access structure is being realized through a quantum scheme. It is important to note that not every secret-sharing scheme can be associated with a matroid.

### A. Matroids

First we recall a few facts about matroids; readers interested in a comprehensive introduction to matroids can refer to [30].

A set $V$ and $\mathcal{C} \subseteq 2^V$ form a matroid $\mathcal{M}(V,\mathcal{C})$ if and only if the following conditions hold. For any $A,B \in \mathcal{C}$ and $A \neq B$,

(M1) $A \not\subseteq B$.

(M2) If $x \in A \cap B$, then there exists a $C \in \mathcal{C}$ such that $C \subseteq (A \cup B) \setminus \{x\}$.

We say that $V$ is the ground set and $\mathcal{C}$ the set of circuits of the matroid. A proper subset of any circuit is said to be independent, while a set containing any circuit is said to be dependent. With every matroid we define a nonnegative integer-valued function called the rank function, $\mathrm{rk} : V \to \mathbb{N}$ as

$$\mathrm{rk}(X) = |I|, \tag{7}$$

where $I \subseteq X \subseteq V$ is a maximal independent subset of $X$. A matroid is said to be (linearly) representable over a field $\mathbb{F}$ if the ground set can be identified with the columns of a matrix $M$ (over $\mathbb{F}$) and the circuits with the minimal dependent columns of the matrix. We say that $M$ is a representation of the matroid. In this paper we are only interested in finite fields. We can also define matroids in terms of their bases, which are maximal independent sets of $V$. A set $V$ and $\mathcal{B} \subseteq 2^V$ form a matroid $\mathcal{M}(V,\mathcal{B})$ if and only if the following conditions hold.

(B1) $\mathcal{B} \neq \emptyset$.

(B2) If $B_1, B_2 \in \mathcal{B}$ such that $x \in B_1 \setminus B_2$, then there exists a $y \in B_2 \setminus B_1$ such that $(B_1 \setminus x) \cup \{y\} \in \mathcal{B}$.

Given a matroid $\mathcal{M}(V,\mathcal{B})$ we define its dual matroid $\mathcal{M}(V,\mathcal{B})^*$ as the matroid with ground set $V$ and bases $\mathcal{B}^* = \{V \setminus B \mid B \in \mathcal{B}\}$; that is, $\mathcal{M}(V,\mathcal{B})^* = \mathcal{M}(V,\mathcal{B}^*)$.

### B. Secret-sharing schemes from matroids

We can associate a secret-sharing scheme with a given matroid $\mathcal{M}(V,\mathcal{C})$; strictly speaking, it is the access structure which is associated with the matroid. We assume that the ground set of the matroid is given by $V = \{0,1,\ldots,n-1,n\}$. We identify one of the elements of the ground set, say $i \in V$, as the dealer and then list all the circuits of $\mathcal{M}$ that contain $i$. Let this be denoted

$$\Gamma_{i,\min} = \{C \mid C \cup \{i\} \in \mathcal{C}\}. \tag{8}$$

We note that $\Gamma_{i,\min}$ is minimal in the sense that there exist no sets $A,B \in \Gamma_{i,\min}$ such that $A \subsetneq B$, as that would imply that the circuit $A \cup \{i\} \subsetneq B \cup \{i\}$, which is not possible for two circuits by M1. Consider the access structure given by

$$\Gamma_i = \{A \mid V \setminus \{i\} \supseteq A \supseteq C \ \text{ for some } \ C \in \Gamma_{i,\min}\}. \tag{9}$$

We can easily verify that $\Gamma_i$ is a monotonic and that its minimal access structure is given by $\Gamma_{i,\min}$. Since any monotonic access structure can be realized as a secret-sharing scheme, every matroid defines an access structure. This result is stated in the following fact (see [4]).

*Fact 1*. Every matroid $\mathcal{M}(V,\mathcal{C})$ induces an access structure $\Gamma_i$ as defined in Eq. (9).

Please note that the preceding association is, in a sense, nonconstructive: it does not specify how to derive the associated secret-sharing scheme; it merely states that there exists a secret-sharing scheme that can realize the induced access structure $\Gamma_i$. Further, depending on which element of the ground set of the matroid is identified as the dealer, we may obtain many schemes with possibly different access structures from the same matroid.

A natural question that we are faced with is how to make this association constructive and determine the bounds on the information rate of the resulting access structure. Brickell and Davenport [9] showed that if the matroid is representable over a finite field,[2] then the matroid induces ideal secret-sharing schemes and access structures.

However, if the matroid is not representable, then we can no longer be certain whether the matroid induces an ideal secret-sharing scheme. Seymour proved that there exist nonrepresentable matroids which cannot induce an ideal secret-sharing scheme [32], while Simonis and Ashikhmin [7] showed that there exist nonrepresentable matroids, such as the non-Pappus matroid, which induce ideal schemes. However, the latter matroids—while not affording a linear representation—can be multilinearly represented. Matroids which induce ideal access structures are called secret-sharing-representable matroids [31]. They may not be linearly representable.

[2]Strictly, Theorem 2 in Ref. [9] only requires the matroid to be representable over a near field.

### C. Matroids from secret-sharing schemes

Given that we can obtain secret-sharing schemes from matroids, we could ask if the converse is possible. As we mentioned earlier, such a correspondence does not exist for all secret-sharing schemes. We review some of the related work in this context. The correspondence between the matroids and secret-sharing schemes naturally implies that the access structure is associated with the circuits of the matroid. This association could involve the scheme explicitly. However, a result due to Martin [5] (see also [12]) shows that we can associate the access structure with a matroid independently of the scheme used to realize that structure. This involves a function, say $f$, defined on the space of access structures; $f$ maps an access structure to an ordered pair, which may or may not be a matroid. If $f(\Gamma)$ is a matroid, then we say that $\Gamma$ is matroid related. The minimal access structure will play a more important role in this regard. As usual we denote the set of participants $P$ and the dealer $D$. Define the extended structure $\Gamma_{\text{ext}} = \{A \cup \{D\} \mid \text{ for all } A \in \Gamma_{\min}\}$. Further, let

$$\mathbb{J}(A,B) = A \cup B \setminus \left( \bigcap_{\substack{C \in \Gamma_{\text{ext}} \\ C \subseteq A \cup B}} C \right) \tag{10}$$

$$\mathcal{C}_\Gamma = \left\{ \begin{matrix} \text{minimal sets of } \mathbb{J}(A,B) \text{ for} \\ \text{all } A,B \in \Gamma_{\min} \text{ and } A \neq B \end{matrix} \right\}. \tag{11}$$

We let $f(\Gamma) = (P \cup \{D\}, \mathcal{C}_\Gamma)$. If $\mathcal{C}_\Gamma$ satisfies the axioms M1 and M2, then we associate $\Gamma$ with the matroid $\mathcal{M}_\Gamma$, whose ground set is $P \cup \{D\}$, and the set of circuits is given by $\mathcal{C}_\Gamma$; that is,

$$\mathcal{M}_\Gamma = \mathcal{M}(P \cup \{D\}, \mathcal{C}_\Gamma). \tag{12}$$

This definition of the matroid is in terms of the circuits that can be formed from the ground set. *We could always define a structure from the secret-sharing scheme, or, equivalently, its access structure, as in Eq. (12), but the resulting structure* is not necessarily a matroid. It is a matroid only under certain conditions. Only when $(P \cup \{D\}, \mathcal{C}_\Gamma)$ induce a matroid do we say that $\Gamma$ is matroidal or matroid related.

Classically an access structure induces a matroid only when it satisfies certain conditions. Before we can state this condition precisely we need the notion of minors. Let $\Gamma$ be an access structure; then we define two operations of deletion and contraction, which we denote $\setminus$ and $/$, respectively. Given a set $Z \subseteq P$, we define

$$\Gamma \setminus Z = \{A \subseteq P \setminus Z \mid A \in \Gamma\}, \tag{13}$$

$$\Gamma / Z = \{A \subseteq P \setminus Z \mid A \cup Z \in \Gamma\}. \tag{14}$$

An access structure $\Gamma'$ derived from $\Gamma$ through a sequence of deletions and contractions is called a minor of $\Gamma$. A result of Seymour's [11] shows that an access structure is matroid related if it satisfies a forbidden minor relation.

*Lemma 2 [11].* An access structure $\Gamma \subseteq 2^P$ is matroid related if and only if it does not have the following minors.

(a) $\Gamma_a = \{\{1,2\},\{2,3\},\{3,4\}\}$.

(b) $\Gamma_b = \{1,2\},\{1,3\},\{1,4\},\{2,3\}\}$.

(c) $\Gamma_c = \{\{1,2\},\{1,3\},\{2,3,4\}\}$.

(d) $\Gamma_d = \{\{1,\ldots,s\},\{1,s+1\},\ldots,\{s,s+1\}\}$, where $P = \{1,\ldots,4\}$ except in $d$, where $P = \{1,\ldots s,s+1\}$ and $s \geqslant 3$.

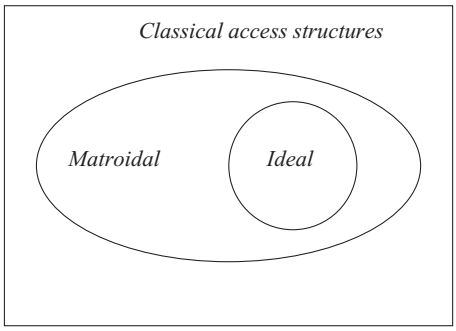



FIG. 1. Relation among ideal, matroidal, and general classical access structures.

Please note that in the preceding result, the minimal access structures are given rather than the complete access structure. Seymour originally stated this result in terms of matroid ports. The reformulation we have given here in terms of the access structures is due to Martí-Farré and Padró [31]. This result together with Lemma 1 immediately provides us with a criterion as to which quantum access structures can be induced by matroids.

Self-orthogonality, however, is not a property inherited by minors of access structures. For instance, contraction does not always preserve the self-orthogonality of the access structures. Consider the following (minimal) access structure: $\Gamma = \{\{1,2,3\},\{2,3,4\},\{3,4,5\}\}$. Then $\Gamma/3 = \{\{1,2\},\{2,4\},\{4,5\}\}$. In this case we have two disjoint authorized sets; such an access structure cannot be realized by a quantum-secret-sharing scheme, as it would lead to a violation of the no-cloning theorem. Therefore, it is not possible to determine a result similar to Lemma 2 for self-orthogonal access structures, that is, a finite list of forbidden minors for access structures that are self-orthogonal.

Brickell and Davenport [9, Theorem 1] showed that every classical ideal access structure induces a matroid. In Figs. 1 and 2 we summarize the relation among permissible access structures, matroidal access structures, and ideal access structures for classical schemes and quantum schemes. We do not know if every access structure that is realized by an ideal quantum-secret-sharing scheme induces a matroid. For this reason, in Fig. 2, the set of ideal quantum access structures is depicted as not being entirely in the set of

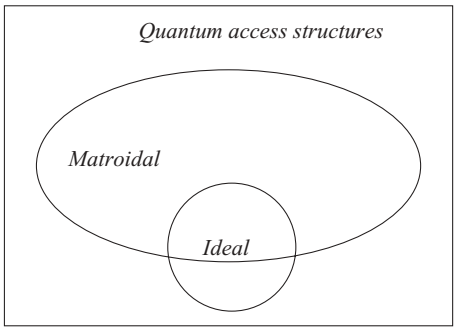



FIG. 2. Relation among ideal, matroidal, and general quantum access structures. It is possible that all ideal quantum access structures are also matroidal.

matroidal access structures, although we caution that it is possible that all ideal quantum access structures are also matrodial.

## III. RELATING MATROIDS AND QUANTUM SECRET SHARING

### A. Matroidal quantum-secret-sharing schemes

In this section we present the central result of our paper, Theorem 4. It shows that a class of matroids induces ideal pure-state quantum-secret-sharing schemes. First, we need the following preliminaries. We say a matroid is self-dual if it is isomorphic to its dual matroid. If it is equal to its dual matroid, then we say it is an identically self-dual (ISD) matroid.

*Fact 2*. Let $\Gamma_i$ and $\Gamma_i^d$ be the access structures induced by a matroid $\mathcal{M}(V,\mathcal{C})$ and its dual matroid $\mathcal{M}^*$ by treating the $i$th element as the dealer. Then we have

$$\Gamma_i^d = \Gamma_i^*. \tag{15}$$

Fact 2 was stated in [4]. For an identically self-dual matroid, we have $\Gamma_i = \Gamma_i^d$; therefore, together with Lemma 1, and the fact that every self-dual access structure can be realized as a pure-state scheme [15, Theorem 8], we have the following result, stated explicitly due to its relevance for us.

*Corollary 3*. An identically self-dual matroid $\mathcal{M}$ induces a pure-state quantum-secret-sharing scheme.

However, the preceding result does not give us a method to construct a quantum-secret-sharing scheme from the matroid, nor does it tell us if the scheme is ideal. The following theorem gives the general procedure to transform a representable identically self-dual matroid into a quantum-secret-sharing scheme. We denote a finite field with $q$ elements as $\mathbb{F}_q$. Following standard notation, we use $[n,k,d]_q$ to denote a classical code over $\mathbb{F}_q$ and $[[n,k,d]]_q$ to denote a quantum code over $\mathbb{F}_q$. If $C$ is a code, we denote a generator matrix of $C$ by $G_C$. The code obtained by deleting the $i$th coordinate of $C$ is called a punctured code of $C$ and denoted $\rho_i(C)$. Suppose we consider the subcode of $C$ with the $i$th coordinate 0; then the code obtained by puncturing the $i$th coordinate of the subcode is called a shortening of $C$ and denoted $\sigma_i(C)$. If $C$ is an $[n,k,d]_q$ code, then $\sigma_i(C)$ is an $[n-1,k-1,d]_q$ code, while $\rho_i(C)$ is an $[n-1,k,d-1]_q$ code. We have the following useful relations between the punctured and shortened codes and their duals [33, Theorem 1.5.7]:

$$\sigma_i(C) \subset \rho_i(C) \quad \text{and} \quad \sigma_i(C)^\perp = \rho_i(C^\perp). \tag{16}$$

We also have $\rho_i(C)^\perp \subset \sigma_i(C)^\perp$.

If $x \in \mathbb{F}_q^n$, then we denote the support of $x$ as $\mathrm{supp}(x) = \{i \mid x_i \neq 0\}$. A codeword $x$ in $C$ is said to be a minimal support element if there exists no nonzero codeword $y$ in $C$ such that $\mathrm{supp}(y) \subsetneq \mathrm{supp}(x)$. If, in addition, its leftmost nonzero component is 1, then it is said to be a minimal codeword. Minimal codewords were introduced by Massey [6]. They facilitate the study of classical secret-sharing schemes, especially in characterizing the access structures. We now give the quantum-secret-sharing schemes that realize the access structures induced by matroids. These schemes assume that the domain of the secret is $\mathbb{F}_q$ where $q = p^m$ and $p$ is the characteristic of the finite field. In other words, we are sharing a qudit whose state space is the $q$-dimensional complex vector space $\mathbb{C}^q$. Let $\mathcal{B} = \{|x\rangle \mid x \in \mathbb{F}_q\}$ be an orthonormal basis of $\mathbb{C}^q$. The generalized Pauli operators on a qudit are given by

$$X(a)|x\rangle = |x+a\rangle \quad \text{and} \quad Z(b)|x\rangle = e^{j2\pi/p \mathrm{tr}(bx)}|x\rangle,$$

where $\mathrm{tr}(x) = \sum_{i=0}^{m-1} x^{p^i}$. A generalized Pauli operator on $n$ qudits is of the form

$$e^{j2\pi l/p} X(a_1)Z(b_1) \otimes X(a_2)Z(b_2) \otimes \cdots \otimes X(a_n)Z(b_n),$$

where $l \in \mathbb{F}_p$. We denote this compactly as $e^{j2\pi l/p} X(a)Z(b)$ and its representation over $\mathbb{F}_q^{2n}$ is given by $(a_1,\ldots,a_n \mid b_1,\ldots,b_n) = (a \mid b)$. It suffices for now to recall that an $[[n,k]]_q$ CSS code encoding $k$ qudits into $n$ qudits can be defined by a classical code over $\mathbb{F}_q^{2n}$ which has a generator matrix of the form

$$G = \left[\begin{array}{c|c} G_1 & 0 \\ 0 & G_2 \end{array}\right],$$

where $G_1 G_2^t = 0$, $G_1 \in \mathbb{F}_q^{s\times n}$, and $G_2 \in \mathbb{F}_q^{(n-k-s)\times n}$. We call $G$ the stabilizer matrix of the quantum code or, simply, the stabilizer. For the case where $k=1$, we call a pair of elements $\overline{X} = X(a)Z(b)$ and $\overline{Z} = X(c)Z(d)$, or, equivalently, their representations $(a \mid b)$ and $(c \mid d)$, the encoded or logical operators of the code if $a\cdot d - b\cdot c = 1$ and $G_1 b^t = G_1 d^t = 0$ and $G_2 a^t = G_2 c^t = 0$. We note that other choices are possible for the encoded operators. For further details on nonbinary stabilizer codes we refer the reader to [34] and [35]; for quantum circuits over a nonbinary alphabet, to [36].

*Theorem 4*. Let $\mathcal{M}(V,\mathcal{C})$ be an identically self-dual matroid representable over a finite field $\mathbb{F}_q$, where $V = \{0,1,\ldots,n-1,n\}$. Suppose that $C \subseteq \mathbb{F}_q^{n+1}$ such that the generator matrix of $C$ is a representation of $\mathcal{M}$. Let

$$G_C = \left[\begin{array}{c|c} 1 & g \\ \mathbf{0} & G_{\sigma_0(C)} \end{array}\right] \quad \text{and} \quad G_{\rho_0(C)} = \left[\begin{array}{c} g \\ G_{\sigma_0(C)} \end{array}\right]. \tag{17}$$

Then there exists an ideal pure-state quantum-secret-sharing scheme $\Sigma$ on $P = \{1,\ldots,n\}$ whose access structure $\Gamma_0$ and minimal access structure $\Gamma_{0,\min}$ are defined by Eqs. (9) and (8), respectively. The encoding for $\Sigma$ is determined by the stabilizer code, with the stabilizer matrix given by

$$S = \left[\begin{array}{c|c} G_{\sigma_0(C)} & \mathbf{0} \\ \mathbf{0} & G_{\rho_0(C)^\perp} \end{array}\right]. \tag{18}$$

Given an authorized set $A$, the reconstruction procedure (involving a possible renumbering of the shares so that shares in $A$ correspond to the first $|A|$ parties) is the transformation on $S$ such that the encoded operators for the transformed stabilizer code are $\overline{X}' = X(1)\otimes I^{\otimes n-1}$ and $\overline{Z}' = Z(1)\otimes I^{\otimes n-1}$.

*Proof*. The proof of Theorem 4 is structured as follows. Since $\Sigma$ relies on the encoding of the stabilizer code derived from $S$, we first show that $S$ defines a stabilizer code and identify certain properties of the codes $C$ and $C^\perp$ essential to recovering the secret. Then we show that if the secrets are encoded using the stabilizer encoding, then an element $A \in \Gamma_{0,\min}$ does correspond to a minimal authorized set by explicitly reconstructing the secret with the shares in $A$ and proving that no proper subset of $A$ can reconstruct the secret.

Encoding the secret: We can easily check that the matrix given in Eq. (18) does define a stabilizer code. Assuming that $C$ is an $[n+1,k,d]_q$ code, we see that $\sigma_0(C)$ is an $[n,k-1,d]_q$ code, while $\rho_0(C)$ is an $[n,k,d-1]_q$ code with $\sigma_0(C) \subset \rho_0(C)$. Therefore we have $\rho_0(C)^\perp \subset \sigma_0(C)^\perp$, ensuring the orthogonality of $\sigma_0(C)$ and $\rho_0(C)^\perp$ in Eq. (18). The dimension of $S$ is given by $k-1+n-k=n-1$. Thus $S$ defines an $[[n,1]]_q$ quantum code, $Q$.

Since $\mathcal{M}(V,\mathcal{C})$ is an identically self-dual matroid, both $C$ and $C^\perp$ represent $\mathcal{M}(V,\mathcal{C})$. Therefore, $g \neq 0$; otherwise the zeroth column would be all zero in $C^\perp$, which would mean that $\{0\}$ is a circuit, while from $C$, we would conclude that $\{0\}$ is independent and not a circuit: a contradiction. Furthermore, without loss of generality we can choose $(1 \mid g)$ to be a minimal codeword $c$ in $C$.[3]

The mapping for the secret-sharing scheme is given as follows up to a normalization factor:

$$|s\rangle \mapsto \sum_{x \in \sigma_0(C)} |sg + x\rangle, \quad \text{where} \quad s \in \mathbb{F}_q. \tag{19}$$

Encoding of an arbitrary secret state follows by linearity of the encoding map. The encoded $X$ operator for the quantum code is given by $\overline{X} = \otimes_{i=1}^n X(g_i)$ or, equivalently $(g \mid 0)$, its representation over $\mathbb{F}_q^{2n}$.

Recovering the secret: Let $A \in \Gamma_{0,\min}$; then $A \cup \{0\} \in \mathcal{C}$ and there exists a minimal codeword $c' \in C^\perp$ such that $\mathrm{supp}(c') = A \cup \{0\}$ and $c'_0 = 1$. Because $\mathcal{M}(V,\mathcal{C})$ is an identically self-dual matroid, we know that there exists a codeword $c \in C$ such that $\mathrm{supp}(c) = \mathrm{supp}(c')$. We can choose $c_0 = 1$ since $C$ is a linear code. Then we have $\rho_0(c) \notin \sigma_0(C)$. Further, both $\rho_0(c)$ and $g$ are in the same coset of $\sigma_0(C)$ in $\rho_0(C)$. This holds because the cosets of $\sigma_0(C)$ in $\rho_0(C)$ are in one-to-one correspondence with the cosets of $[\mathbf{0} \mid \sigma_0(C)]$ in $C$. The various coset representatives are given by $(\alpha \mid \alpha g)$, $\alpha \in \mathbb{F}_q$. Two coset representatives $r,r'$ represent the same coset if and only if $r_0 = r'_0$. Therefore all the codewords $c$, with $c_0 = 1$ are in the same coset as $(1 \mid g)$. From this it follows that $\rho_0(c)$ is in the same coset as $(g)$. Therefore, the state $|s\rangle$ might as well be given by

$$|s\rangle \mapsto \sum_{x \in \sigma_0(C)} |\, s \cdot \rho_0(c) + x\rangle. \tag{20}$$

Denote the columns of $G_{\sigma_0(C)}$ by $s_i$, where $1 \leqslant i \leqslant n$. Since $c' \in C^\perp$, we have

$$G_C (c')^t = \begin{bmatrix} 1 & c_1 & c_2 \ldots & c_n \\ \mathbf{0} & s_1 & \ldots & s_n \end{bmatrix} \begin{bmatrix} 1 \\ c'_1 \\ \vdots \\ c'_n \end{bmatrix} = \mathbf{0}.$$

This equation can also be written as

$$\begin{bmatrix} c_1 & c_2 \ldots & c_n \\ s_1 & \ldots & s_n \end{bmatrix} \begin{bmatrix} -c'_1 \\ \vdots \\ -c'_n \end{bmatrix} = \begin{bmatrix} 1 \\ \mathbf{0} \end{bmatrix}.$$

In other words, there exists a linear combination of the columns in $G_{\sigma_0(C)}$ such that

$$\sum_{i \in \mathrm{supp}[\rho_0(c')]} c_i c'_i = -1 \quad \text{and} \quad \sum_{i \in \mathrm{supp}[\rho_0(c')]} c'_i s_i = 0. \tag{21}$$

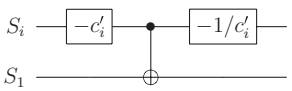
Now let us rewrite the stabilizer and the encoded $X$ operator as follows:

$$\left[\begin{array}{c} \overline{X} \\ \hline S \end{array}\right] = \left[\begin{array}{c|c} \rho_0(c) & \mathbf{0} \\ \hline G_{\sigma_0(C)} & \mathbf{0} \\ \mathbf{0} & G_{\rho_0(C)^\perp} \end{array}\right],$$

$$= \left[\begin{array}{ccccc|c} c_1 & \cdots & c_l & 0 \cdots & 0 & \mathbf{0} \\ \hline s_1 & \cdots & & s_n & & \mathbf{0} \\ & & \mathbf{0} & & & r_1 \cdots r_n \end{array}\right],$$

where, without loss of generality, we can assume that $\rho_0(c')$ and therefore $\rho_0(c)$ have support in the first $l$ columns only (that is, $c_i \neq 0$ for $1 \leqslant i \leqslant l$) and that $c_i = 0$ for $i > l$, where $1 \leqslant l \leqslant n$. This amounts to a renumbering of the shares so that the shares in $A$ are the first $|A|$ shares. Note that $l \geqslant 1$ because we must have $c \cdot c' = 0$ and $l = 0$ implies that $(1 \mid 0) \cdot (1 \mid 0) = 0$, which is clearly not possible.

Let us transform the first column of $S$ per Eq. (21); that is, $s_1 \mapsto -\sum_{i \in \mathrm{supp}[\rho_0(c')]} c'_i s_i$. For binary schemes this involves applying controlled-NOT (CNOT) gates from $\mathrm{supp}[\rho_0(c')] \setminus \{1\}$ to the qudit $\{1\}$ (as the target qudit). For nonbinary schemes, we have to use the generalized CNOT gates (called ADD gates in [36]) along with appropriately scaling by $c'_i$.[4] More concretely, after scaling the first qudit by $c'_1$, we implement a circuit of the form




for each $i \in \mathrm{supp}[\rho_0(c')] \setminus \{1\}$, where $S_i$ is the $i$th qudit. Then $S$ and $\overline{X}$ are transformed as

$$\left[\begin{array}{ccccc|c} 1 & c_2 & \cdots & c_l & 0 \cdots 0 & \mathbf{0} \\ \hline \mathbf{0} & s_2 & \cdots & & s_n & \mathbf{0} \\ & & \mathbf{0} & & & r_1\ \tilde{r}_2 \cdots \tilde{r}_l\ r_{l+1} \cdots r_n \end{array}\right].$$

Therein, the columns $r_2$ to $r_l$ are transformed in the $Z$ part, while only the first column is transformed in the $X$ part (see Lemma 2 in [36]). Now let us transform the encoded $X$ operator to the operator given by $\overline{X}' = X(1) \otimes I^{\otimes n-1}$, which acts only on the first qudit. This can be achieved by (generalized) CNOT gates applied from qudit $\{1\}$ to each of the

[3] If $(1 \mid g)$ is not minimal, then there exists some codeword $(1 \mid g')$ or $(0 \mid a)$ such that its support is strictly contained in $\mathrm{supp}(1 \mid g)$. If $\mathrm{supp}(0 \mid a) \subset \mathrm{supp}(1 \mid g)$, then we can find a codeword $(1 \mid g')$, from a linear combination of $(1 \mid g)$ and $(0 \mid a)$, such that $\mathrm{supp}(1 \mid g') \subset \mathrm{supp}(1 \mid g)$ and $\mathrm{supp}(0 \mid a) \not\subset \mathrm{supp}(1 \mid g')$. In either case there is a codeword of the form $(1 \mid g')$ whose support is strictly smaller than $\mathrm{supp}(1 \mid g)$. If $(1 \mid g')$ is minimal, we are done, or we can repeat this process until we find one; the process will terminate in a finite number of steps, as $n$ is finite.

[4] The ADD gate generalizes the CNOT gate and is defined as $\mathrm{ADD}^{i,j} = \sum_{x,y \in \mathbb{F}_q} |x\rangle_i |x+y\rangle_j \langle y|_j \langle x|_i$. Scaling is implemented via the multiplier gate, which is defined as $M_\gamma = \sum_{x \in \mathbb{F}_q} |\gamma x\rangle\langle x|$ for $\gamma \in \mathbb{F}_q^\times$; see [36] for additional details.

qudits in supp$[\rho_0(c')] \setminus \{1\}$. This time qudit $\{1\}$ is the control qudit. This gives us

$$\left[\begin{array}{c|c} 1 \quad \mathbf{0} & \mathbf{0} \\ \hline \mathbf{0}\ \tilde{s}_2 \cdots \tilde{s}_l\ s_{l+1} \cdots s_n & \mathbf{0} \\ \mathbf{0} & \mathbf{0}\ \tilde{r}_2 \cdots \tilde{r}_l\ r_{l+1} \cdots r_n \end{array}\right],$$

which is in the form

$$\left[\begin{array}{cc|c} 1 & \mathbf{0} & \mathbf{0} \\ \hline \mathbf{0} & \tilde{S}_X & \mathbf{0} \\ \mathbf{0} & & \tilde{S}_Z \end{array}\right].$$

The column $\tilde{r}_1$ has to become $\mathbf{0}$ because the stabilizer must commute with the encoded $X$ operator, now given by $\overline{X}' = X(1) \otimes I^{\otimes n-1}$. [The encoded $Z$ operator is now given by $\overline{Z}' = Z(1) \otimes I^{\otimes n-1}$, since it clearly commutes with the elements of the transformed stabilizer but not with $\overline{X}'$.] Further, the encoded secret has now been transformed as

$$\sum_{x \in \tilde{S}_X} |s\rangle|x\rangle = |s\rangle \sum_{x \in \tilde{S}_X} |x\rangle.$$

As can be seen, the secret is completely disentangled from the rest of the qubits. Furthermore, in all these transformations we operated only on the qudits in the support of the minimal codeword. Thus the elements of $\Gamma_{0,\min}$ are authorized sets.

Completeness of $\Gamma_0$: By Fact 2, the access structure $\Gamma_0$ is self-dual, therefore $|\Gamma_0| = 2^{n-1}$. But the complement of every one of these authorized sets is an unauthorized set; otherwise we would violate the no-cloning theorem. Together these sets exhaust all the possible subsets of $\{1, \ldots, n\}$. Thus there are no more authorized sets outside the ones given in $\Gamma_0$ and the quantum access structure is completely defined by $\Gamma_0$.

Minimality of $\Gamma_{0,\min}$: We now claim that $\Gamma_{0,\min}$ does define the minimal access structure of the quantum-secret-sharing scheme. Suppose $A \in \Gamma_{0,\min}$ is not a minimal authorized set for $\Sigma$. Then there exists a $B \subsetneq A$ that is authorized. Since $\Gamma_0$ contains all the authorized sets of $\Sigma$, it follows that $B \in \Gamma_0$. From Eqs. (8) and (9) , we see that $\Gamma_{0,\min}$ is the minimal access structure of $\Gamma_0$, therefore there exists some element $D \in \Gamma_{0,\min}$ such that $D \subseteq B \subsetneq A$. But $\Gamma_{0,\min}$ cannot contain sets $D, A$ such that $D \subsetneq A$. Hence all the sets in $\Gamma_{0,\min}$ are minimal authorized sets of $\Sigma$.

Finally, the purity of $\Sigma$ follows from the explicit encoding procedure given. That $\Sigma$ is ideal follows from the fact that each share has the same dimension as the secret.

We note that the choice of which element in the matroid is identified with the dealer is arbitrary. In Theorem 4, for simplicity we have assumed that the first element is the dealer. Further, we need the representation of the matroid before we can use it to construct the scheme. It is still open if every identically self-dual matroid can be realized as a self-dual code [4]. However, every self-dual code induces a identically self-dual matroid. Consequently, we have the following corollary, which gives us many efficient pure-state quantum-secret-sharing schemes.

*Corollary 5.* Let $C \subseteq \mathbb{F}_q^n$ be an $[n+1, k, d]_q$ code such that $C^\perp = C$, with generator matrix $G_C$ given as

$$G_C = \left[\begin{array}{c|c} 1 & g \\ \mathbf{0} & G_{\sigma_0(C)} \end{array}\right] \quad \text{and} \quad G_{\rho_0(C)} = \left[\begin{array}{c} g \\ G_{\sigma_0(C)} \end{array}\right]. \tag{22}$$

Then there exists an ideal pure-state quantum-secret-sharing scheme $\Sigma$ on $n$ parties, whose minimal access structure is

$$\Gamma_{0,\min} = \left\{ \text{supp}(c) \setminus \{0\} \,\middle|\, \begin{array}{l} c \text{ is a minimal codeword} \\ \text{of } C \text{ with } c_0 = 1 \end{array} \right\}.$$

The encoding for $\Sigma$ is determined by the stabilizer code, with the stabilizer matrix given by

$$S = \left[\begin{array}{c|c} G_{\sigma_0(C)} & \mathbf{0} \\ \mathbf{0} & G_{\rho_0(C)^\perp} \end{array}\right]. \tag{23}$$

The encoding for a state $|s\rangle$, where $s \in \mathbb{F}_q$, is given as

$$|s\rangle \mapsto \sum_{x \in \sigma_0(C)} |s \cdot g + x\rangle. \tag{24}$$

The reconstruction procedure for an authorized set $A$ of $\Sigma$ (involving a possible renumbering of the shares so that shares in $A$ correspond to the first $|A|$ parties) is the transformation on $S$ such that the encoded operators for the transformed stabilizer are $\overline{X}' = X(1) \otimes I^{\otimes n-1}$ and $\overline{Z}' = Z(1) \otimes I^{\otimes n-1}$.

### B. An example

We now give an example to illustrate the construction. Let us consider the extended Hamming code given by the following generator matrix.

$$G_C = \left[\begin{array}{c|cccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}\right].$$

We can check that $C$ is self-dual. The punctured code $\rho_0(C)$ and the shortened code $\sigma_0(C)$ are given by the following generator matrices.

$$G_{\rho_0(C)} = \left[\begin{array}{ccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}\right].$$

$$G_{\sigma_0(C)} = \left[\begin{array}{ccccccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}\right].$$

Now let us form a (CSS) stabilizer code with a stabilizer matrix as follows.

$$S = \left[\begin{array}{c|c} G_{\sigma_0(C)} & \mathbf{0} \\ \hline \mathbf{0} & \rho_{0(C)^\perp} \end{array}\right].$$

$$= \left[\begin{array}{ccccccc|ccccccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 & & & & & & & \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & & & & \mathbf{0} & & & \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & & & & & & & \\ \hline & & & & & & & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ & & & & \mathbf{0} & & & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ & & & & & & & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}\right].$$

For this stabilizer code the encoding for $|0\rangle$ and $|1\rangle$ is given as follows:

$$|0\rangle \mapsto |0000000\rangle + |1000111\rangle + |0101011\rangle + |0011110\rangle + |1101100\rangle + |1011001\rangle + |0110101\rangle + |1110010\rangle,$$

$$|1\rangle \mapsto |1111111\rangle + |0111000\rangle + |1010100\rangle + |1100001\rangle + |0010011\rangle + |0100110\rangle + |1001010\rangle + |0001101\rangle.$$

Observe that $|s\rangle \mapsto \sum_{c\in\sigma_0(C)} |s\cdot\overline{X}+c\rangle$, where $\overline{X}$ is in $\sigma_0(C)^\perp \setminus \sigma_0(C)$. Now consider a minimal codeword $c$ in $C^\perp$ such that $c_0 = 1$. One such codeword is $c = (1,1,1,0,0,0,0,1)$. Observe that $(1,1,0,0,0,0,1\,|\,\mathbf{0})$, that is, $X_1X_2X_7$ is an encoded operator for the stabilizer code. The support of $c$ is given by $\{0,1,2,7\}$. The linear combination of the columns in the support of $\rho_0(c)$ gives us $(1,0,0,0)^t$. Let us now transform $S$, so that columns 2 and 7 are added to the first column in $S$. We can achieve this if we apply a CNOT gate from qubit 2 to 1 (i.e., the target qubit is 1), followed by a CNOT gate from qubit 7 to qubit 1. This transforms the stabilizer as

$$S \mapsto \left[\begin{array}{ccccccc|ccccccc} 0&0&0&0&1&1&1&&&&&&&\\ 0&1&0&1&0&1&1&&&\mathbf{0}&&&&\\ 0&0&1&1&1&1&0&&&&&&&\\ \hline &&&&&&&1&1&0&0&1&1&0\\ &&&\mathbf{0}&&&&0&1&0&1&0&1&1\\ &&&&&&&0&0&1&1&1&1&0 \end{array}\right].$$

The encoded operator $(1,1,0,0,0,0,1\,|\,\mathbf{0})$ maps to $(1,1,0,0,0,0,1\,|\,\mathbf{0})$. We now transform the encoded $X$ operator to $(1,0,0,0,0,0,0\,|\,\mathbf{0})$. This can be achieved by a CNOT gate from qubit 1 to qubit 2, followed by a CNOT gate from qubit 1 to qubit 7. Then the stabilizer gets further transformed as

$$S \mapsto \left[\begin{array}{ccccccc|ccccccc} 0&0&0&0&1&1&1&&&&&&&\\ 0&1&0&1&0&1&1&&&\mathbf{0}&&&&\\ 0&0&1&1&1&1&0&&&&&&&\\ \hline &&&&&&&0&1&0&0&1&1&0\\ &&&\mathbf{0}&&&&0&1&0&1&0&1&1\\ &&&&&&&0&0&1&1&1&1&0 \end{array}\right].$$

Observe that, this time, only the $Z$ part of the stabilizer is transformed. Now the encoded secret is in the state

$$|s\rangle(|000000\rangle + |000111\rangle + |101011\rangle + |011110\rangle + |101100\rangle + |011001\rangle + |110101\rangle + |110010\rangle).$$

The secret is completely disentangled from the rest of the shares. Therefore, $\mathrm{supp}(c)\setminus\{0\}$ forms an authorized set. The rest of the shares cannot reconstruct or extract any information from their shares because of the no-cloning theorem. Similarly, any minimal code word in $C^\perp$ with $c_0 = 1$ defines an authorized set for the scheme. Suppose that $c$ is a minimal code word with $c_0 = 0$, then it must be in $\sigma_0(C)$, and any other vector whose support is the same must be in $S$ or outside $C(S)$, the centralizer of $S$. No such operator can reveal any information about the encoded secret since they are detectable errors of the stabilizer code, and by definition detectable errors reveal nothing about the encoded information.

### C. Discussion

The results in this section have important benefits. Quantum-secret-sharing schemes for general access structures were proposed by Gottesman [15] and Smith [28], based on monotone span programs. These constructions are not optimal in general. Our method gives optimal schemes with information rate 1. However, not every ideal quantum-secret-sharing scheme can be derived by Theorem 4. For instance, the ((3,5)) threshold scheme can be realized using the [[5,1,3]] quantum code, but it cannot be realized by the method proposed. Furthermore, the access structure of the ((3,5)) scheme induces a matroid. It would be worth investigating to find out how such quantum schemes can be derived from matroids. Another interesting question would be to derive ideal quantum-secret-sharing schemes from nonrepresentable identically self-dual matroids.

## ACKNOWLEDGMENTS

We thank Hoi-Kwong Lo for pointing out an inaccuracy in a previous version of the paper. We thank an anonymous reviewer for making very helpful and insightful comments to improve the paper. Part of this work was presented at the Workshop on Applications of Matroid Theory and Combinatorial Optimization to Information and Coding Theory, Banff International Research Station, Banff, Canada, 2009. This research was supported by NSERC, CIFAR, and MITACS.

[1] G. R. Blakley, in *Proceedings of the National Computer Conference, 1979* (AFIPS, 1979), pp. 313–317.
[2] A. Shamir, Commun. ACM **22**(11), 612 (1979).
[3] M. Ben-Or, C. Crepeau, D. Gottesman, A. Hassidim, and A. Smith, in *47th IEEE Symposium on the Foundations of Computer Science* (2006), pp. 249–260.
[4] R. Cramer, V. Daza, I. Gracia, J. J. Urroz, G. Leander, J. Martí-Farré, and C. Padró, IEEE Trans. Inf. Theory **54**(6), 2644 (2008).
[5] K. M. Martin, Ph.D. thesis, Royal Holloway and Bedford New College, University of London, 1991.
[6] J. L. Massey, in *Proceedings of the 6th Joint Swedish-Russian Workshop on Information Theory, Mölle, Sweden* (1993), pp. 276–279.
[7] J. Simonis and A. Ashikhmin, Designs Codes Cryptogr. **14**, 179 (1998).
[8] A. Beimel and N. Livne, IEEE Trans. Inf. Theory **54**, 2626 (2008).
[9] E. F. Brickell and D. M. Davenport, J. Cryptol. **4**, 123 (1991).
[10] J. Dj. Golić, J. Cryptol. **11**, 75 (1998).
[11] P. D. Seymour, Q. J. Math. Oxford Ser. **27**, 407 (1976).
[12] D. E. Stinson, Designs Codes Cryptogr. **2**, 357 (1992).

[13] M. Hillery, V. Buzek, and A. Berthaume, Phys. Rev. A **59**(3), 1829 (1999).
[14] R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**(3), 648 (1999).
[15] D. Gottesman, Phys. Rev. A **61**, 042311 (2000).
[16] H. Imai, J. Müller-Quade, A. Nascimento, P. Tuyls, and A. Winter, Quantum Inf. Comput. **5**(1), 068 (2004).
[17] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**(1), 162 (1999).
[18] D. Markham and B. C. Sanders, Phys. Rev. A **78**, 042309 (2008).
[19] K. Rietjens, B. Schoenmakers, and P. Tuyls, in *Proceedings of the 2005 IEEE International Symposium on Information Theory, Adelaide, Australia* (2005), pp. 1598–1602.
[20] L. Xiao, G. L. Long, F.-G. Deng, and J.-W. Pan, Phys. Rev. A **69**, 052307 (2004).
[21] S. Gaertner, C. Kurtsiefer, M. Bourennane, and H. Weinfurter, Phys. Rev. Lett. **98**, 020503 (2002).
[22] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, and P. K. Lam, Proc. SPIE **5468**, 100 (2004).
[23] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, and P. K. Lam, Phys. Rev. Lett. **92**, 177903 (2004).
[24] W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A **63**, 042301 (2001).
[25] J. Benaloh and J. Leichter, in *Advances in Cryptology (Proceedings of CRYPTO '88. Santa Barbara, CA, August 1988*, edited by S. Goldwasser). *Lecture Notes in Computer Science*, Vol. 403, edited by G. Goos and J. Hartmanis (Springer-Verlag, New York, 1990), pp. 27–35.
[26] D. Dieks, Phys. Lett. A **92**, 271 (1982).
[27] W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).
[28] A. Smith, e-print arXiv:quant-ph/0001087.
[29] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, IEEE Trans. Inf. Theory **44**, 1369 (1998).
[30] J. Oxley, [http://www.math.lsu.edu/∼oxley/survey4.pdf] (2004).
[31] J. Martí-Farré and C. Padró, in *Fourth IACR Theory of Cryptography Conference, TCC 2007, Lecture Notes in Computer Science*, Vol. 4392 (2007), pp. 273–290.
[32] P. D. Seymour, J. Comb. Theory B **56**, 69 (1992).
[33] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes* (Cambridge University Press, Cambridge, 2003).
[34] A. Ashikhmin and E. Knill, IEEE Trans. Inf. Theory **47**(7), 3065 (2001).
[35] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, IEEE Trans. Inf. Theory **52**(11), 4892 (2006).
[36] M. Grassl, M. Rötteler, and T. Beth, Internat. J. Found. Comput. Sci. **14**(5), 757 (2003).