Matroids and Quantum Secret Sharing Schemes

Pradeep Sarvepalli* and Robert Raussendorf
Department of Physics and Astronomy, University of British Columbia, Vancouver V6T 1Z1, Canada
(Dated: October 23, 2009)

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 one.

PACS numbers: 03.67.Dd; 03.67.Pp
Keywords: quantum secret sharing, matroids, self-dual matroids, quantum codes, quantum cryptography

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 [3, 25]. Additionally, it finds applications in secure multi-party distributed computation [2, 6]. Secret sharing schemes have a rich mathematical structure [19] and they have been shown to be closely associated to error correcting codes [6, 20, 26] and matroids [1, 4, 6, 10, 24, 28]. The interplay with these objects has enabled us to obtain new insights not only about secret sharing schemes but codes and matroids as well. Although relatively new, the field of quantum secret sharing [13] has made rapid progress both theoretically [5, 7, 11, 14, 15, 22, 31] and experimentally [9, 16, 17, 29]. 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 i.e. those with information rate one, 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 into bearing 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. This paper is organized as follows. We begin with a brief review of the necessary background in secret sharing. In Section 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 Section 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 Γ consists of all subsets that can reconstruct the secret. The adversary structure $\mathcal{A}$ consists of all unauthorized subsets. Any access structure Γ is required to satisfy the monotone property i.e. if $A \in \Gamma$, then any set $B \supseteq A$ is also in Γ. 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 large complexity, see for instance [28]. 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, $\mathbb{S}$. 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 ith party be $\mathbb{S}_i$. An important

*pradeep@phas.ubc.ca

metric of performance for secret sharing schemes is the information rate ρ which is defined as

$$\rho = \min_i \frac{\dim \mathbb{S}}{\dim \mathbb{S}_i}. \tag{1}$$

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 one 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 information rate of one.

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. Some authors refer to the first case as quantum state sharing, reserving the term "quantum secret sharing" to situations where the secret is shared in an adversarial setting. Though 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 i.e., unauthorized sets can extract some information about the secret. Cleve et al [5] proposed the first perfect quantum secret sharing schemes for quantum secrets. The theory of quantum secret sharing was developed further making important connections to quantum coding theory in [5, 11] and quantum information theory in [14, 22] and more recently to graphs via labelled graph states in [7].

In this paper we are concerned with the 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" [8, 30] 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 access structure determines the allowed access structures for all quantum secret sharing schemes [11, 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 of a set. 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 Γ be the access structure and $\mathcal{A}$ the adversary structure of a quantum secret sharing scheme. Then the following statements are equivalent.*

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

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

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

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 Γ^*, it follows that for any $A \in \Gamma$, we must have $\overline{A} \notin \Gamma$ i.e. $\overline{A} \in \mathcal{A}$. 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 $\overline{A} \in \mathcal{A}$ i.e. they are not in Γ 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. □

We often refer to an access structure that is realizable by a quantum secret sharing scheme as a quantum access structure. Smith [27, 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 a mixed state scheme if it encodes into a global mixed state. Self dual access structures can be realized by pure state schemes, where as non-self-dual access structures can be realized only as mixed state schemes. A theorem [11, 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 focussing 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 $\geq k$ and unauthorized sets are subsets of cardinality less than k. Smith [27] and independently Gottesman [11] 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 Γ_m of the access structure Γ as

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

If every party in P occurs in at least one minimal authorized set of Γ, 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 characterizing the associated access structures in terms of matroids if it is possible. We also address the construction of secret sharing schemes. Our constructions make use of CSS codes reminiscent of the constructions of Smith for general access structures.

II. MATROIDS AND SECRET SHARING

Matroids have been associated to secret sharing schemes [4, 6], also see [28] for a brief overview of some of the main results. Such 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, [1, 4]. Also, 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. By far we do same 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 to a matroid.

A. Matroids

First we recall a few facts about matroids, readers interested in a comprehensive introduction to matroids can refer to [21].

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 non-negative 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 (over $\mathbb{F}$) and the circuits with the minimal dependent columns of the matrix. 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 $\mathcal{B}^* = \{V \setminus B \mid B \in \mathcal{B}\}$ i.e. $\mathcal{M}(V, \mathcal{B})^* = \mathcal{M}(V, \mathcal{B}^*)$.

B. Secret sharing schemes from matroids

Given a matroid $\mathcal{M}$ we can associate a secret sharing scheme to $\mathcal{M}(V, \mathcal{C})$. 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 as

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

Consider the access structure given by

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

We can easily verify that Γ_i is a monotonic and that its minimal access structure is given by $\Gamma_{i,m}$. 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 [6].

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

Please note that the above 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 Γ_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 [4] showed that if the matroid is representable over a finite field [32], then we obtain ideal secret sharing schemes and access structures.

However, if the matroid is not representable, then we can no longer be certain if the matroid induces an ideal secret sharing scheme. Seymour proved that there exist non-representable matroids which cannot induce an ideal secret sharing scheme [24], while Simonis and Ashikhmin [26] showed that there exist non-representable matroids, such as the non-Pappus matroid, which induce ideal schemes. However, these latter matroids—while not affording a linear representation—can be multilinearly represented. Matroids which induce ideal access structures are called ss-representable matroids [18]. They may not be linearly representable.

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 to the circuits of the matroid. This association could involve the scheme explicitly. However a result due to Martin [19], see also [28], shows that we can associate the access structure to 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 Γ is matroid-related. The minimal access structure will play a more important role in this regard. As usual we denote by P the set of participants and by D the dealer. Define the extended access structure $\Gamma_e = \{A \cup D \mid \text{ for all } A \in \Gamma_m\}$. Further let

$$\mathbb{J}(A,B) \;=\; A \cup B \setminus \Big(\bigcap\nolimits_{C \in \Gamma_e : C \subseteq A \cup B} C\Big) \tag{10}$$

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

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

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

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, equivalently its access structure, as above 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 we say that Γ is 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 Γ be an access structure, then we define two operations of deletion and contraction, which we denote by "\" 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 Γ' derived from Γ through a sequence of deletions and contractions is called a minor of Γ. A result by Seymour [23] shows that the access structures are matroid related if the access structure satisfies a forbidden minor relation.

Lemma 2 (Seymour)**.** *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 $s \geq 3$.

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 [18]. 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 i.e. the forbidden minors for access structures that are self-orthogonal. Incidentally, there exist other important classes of matroids such as transversal matroids which are not minor closed.

Brickell and Davenport [4, Theorem 1] showed that every classical ideal access structure induces a matroid. In figures 1 and 2 we summarize the relation between 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. Therefore we show that the set of ideal quantum access structures does not lie entirely in the set of matroidal access structures in figure 2.

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 induce 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.

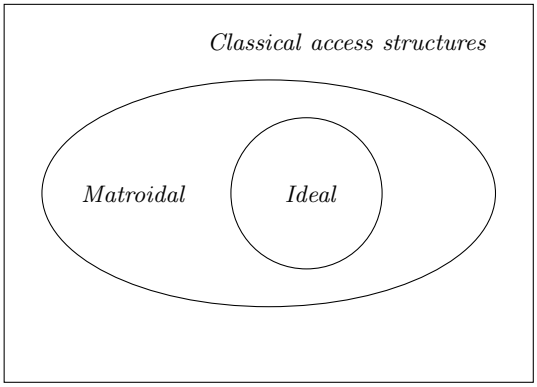

FIG. 1: Relation between ideal, matroidal and general classical access structures

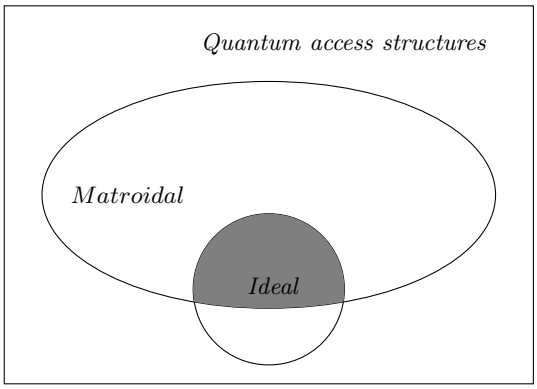

FIG. 2: Relation between ideal, matroidal and general quantum access structures. It is possible that all ideal quantum access structures are also matroidal.

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

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

Fact 2 was stated in [6]. Together with Lemma 1, and the fact that every self-dual access structure can be realized as a pure state scheme [11, Theorem 8], it implies 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, neither 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 ith coordinate of C is called a punctured code of C and denoted as $\rho_i(C)$. Suppose we consider the subcode of C with the ith coordinate zero, then the code obtained by puncturing the ith coordinate of the subcode is called a shortening of C and denoted as $\sigma_i(C)$. We have the following useful relations between the punctured and shortened codes and their duals.

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

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 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 [20]. They facilitate the study of classical secret sharing schemes, especially in characterizing the access structures.

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*

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

Then there exists an ideal pure state quantum secret sharing scheme Σ on $P = \{1,\ldots,n\}$ whose access structure Γ_0 and minimal access structure $\Gamma_{0,m}$, are defined by equations (9) *and* (8) *respectively. The encoding for Σ is determined by the stabilizer code with the stabilizer matrix given by*

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

The reconstruction procedure for an authorized set A is the transformation on S such that the encoded operators for the transformed stabilizer code are $X_1 = X \otimes I^{\otimes^{n-1}}$ and $Z_1 = Z \otimes I^{\otimes^{n-1}}$.

Proof. The proof of this theorem is structured as follows. Since Σ 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 $A \in \Gamma_{0,m}$ 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 equation (18) does define a stabilizer 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 equation (18). The dimension of S

is given by $k-1+n-k=n-1$. Thus S defines an $[[n,1,d']]_q$ 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 $(1|g)$ to be a minimal codeword c in C [33].

As the support of a minimal codeword in C is a circuit of $\mathcal{M}(V,\mathcal{C})$, it follows that there exists a minimal codeword c' in $C^\perp$ such that $\mathrm{supp}(c')=\mathrm{supp}(c)$, in particular there exists a vector $(\beta|\beta g')\in C^\perp$ such that $\mathrm{supp}(\beta g')=\mathrm{supp}(g)$ for some $\beta\in\mathbb{F}_q^\times$ and $g'\in\rho_0(C^\perp)$.

The mapping for the secret sharing scheme is given as follows:

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

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 $[\,g\,|\,\mathbf{0}\,]$, its representation over $\mathbb{F}_q^{2n}$.

Recovering the secret: Let $A\in\Gamma_{0,m}$, then $A\cup\{0\}\in\mathcal{C}$ and there exists a minimal codeword $c'\in C^\perp$ such that $\mathrm{supp}(c')=A\cup\{0\}$. Let c' be a minimal codeword in $C^\perp$ such that $c'_0=1$. We know that there exists a $c\in C$ such that $\mathrm{supp}(c)=\mathrm{supp}(c')$. We can choose $c_0=1$ since C is a linear code. Then, we have $\rho_0(c)\notin\sigma_0(C)$. Then 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 $[\mathbf{0}|\sigma_0(C)]$ in C. The various coset representatives are given by $(\alpha|\alpha g)$, $\alpha\in\mathbb{F}_q$. Two coset representatives r,r' represent the same coset if and only if $r_0=r'_0$. Therefore all the minimal codewords c, with $c_0=1$ are in the same coset as $(1|g)$. From this 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 $1\leq i\leq n$. Since $c'\in C^\perp$, we have

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

The above 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 of $G_{\sigma_0(C)}$ such that

$$\sum_{i\in\mathrm{supp}(\rho_0(c'))}c'_i s_i=0. \tag{21}$$

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

$$\left[\begin{array}{c}\overline{X}\\ \hline S\end{array}\right]=\left[\begin{array}{c|c}\rho_0(c') & \mathbf{0}\\ \hline G_{\sigma_0(C)} & \mathbf{0}\\ \mathbf{0} & G_{\rho_0(C)^\perp}\end{array}\right]$$
$$=\left[\begin{array}{ccccccc|c}c_1 & \cdots & c_l & 0 & \cdots & 0 & & \mathbf{0}\\ \hline s_1 & & \cdots & & & s_n & & \mathbf{0}\\ & & \mathbf{0} & & & & r_1 & \cdots\ r_n\end{array}\right],$$

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, i.e., $c_i\neq 0$ for $1\leq i\leq l$, and that $c_i=0$ for $i>l$, where $1\leq l\leq n$. Note that $l\geq 1$ because we must have $c\cdot c'=0$ and $l=0$ implies that $(1|0)\cdot(1|0)=0$ which is clearly not possible.

Let us transform the first column of S as per equation (21) i.e., $s_1\mapsto\sum_{i\in\mathrm{supp}(\rho_0(c'))}c'_i s_i$. Then we obtain

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

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. For binary schemes this involves only CNOT gates, for nonbinary schemes, we have to use the generalized CNOT gates [12]. Now let us transform the encoded X operator to the trivial operator given by X_1. This gives us

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

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 zero because the stabilizer must commute with the encoded X operator now given by X_1. 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 above, 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 $\Gamma_{0,m}$ are authorized sets.

Minimality of $\Gamma_{0,m}$: The sets in $\Gamma_{0,m}$ are minimal authorized sets because a proper subset of $\mathrm{supp}(c')$ is not in C and all operators with their support in $\mathrm{supp}(c')$ must lie outside $C(S)$, the centralizer of S. Such operators cannot extract any information about the encoded state as they correspond to detectable errors of the stabilizer code.

Completeness of Γ_0: By Fact 2, the access structure Γ_0 is self-dual, therefore $|\Gamma_0| = 2^{n-1}$. But the complement of everyone of these authorized sets is 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 Γ_0 and the quantum access structure is completely defined by Γ_0.

Finally, the purity of Σ follows from the explicit encoding procedure given. That Σ 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, [6]. However, every self-dual code induces a identically self-dual matroid. Consequently, we have the following corollary that 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*

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

Then there exists an ideal pure state quantum secret sharing scheme Σ on n parties whose minimal access structure is

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

The encoding for Σ is determined by the stabilizer code with the stabilizer matrix given by

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

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

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

The reconstruction procedure for an authorized set A of Σ is the transformation on S such that the encoded operators for the transformed stabilizer are X_1 and Z_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.

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

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. (For clarity we show only nonzero entries).

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

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

Now let us form a (CSS) stabilizer code with 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:

$$\begin{aligned} |0\rangle &\mapsto |0000000\rangle + |1000111\rangle + |0101011\rangle + |0011110\rangle \\ &+ |1101100\rangle + |1011001\rangle + |0110101\rangle + |1110010\rangle \\ |1\rangle &\mapsto |1111111\rangle + |0111000\rangle + |1010100\rangle + |1100001\rangle \\ &+ |0010011\rangle + |0100110\rangle + |1001010\rangle + |0001101\rangle \end{aligned}$$

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 $(1, 1, 0, 0, 0, 0, 1|\mathbf{0})$ i.e. $X_1 X_2 X_7$ 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 $(1, 0, 0, 0)^t$. If we computed the linear combination of the columns $1, 2, 7$ into the first column we get

the following action on stabilizer of the code.

$$S \mapsto \left[\begin{array}{ccccccc|ccccccc} 0&0&0&0&1&1&1 & \multicolumn{7}{c}{\multirow{3}{*}{$\mathbf{0}$}} \\ 0&1&0&1&0&1&1 & \multicolumn{7}{c}{} \\ 0&0&1&1&1&1&0 & \multicolumn{7}{c}{} \\ \hline \multicolumn{7}{c|}{\multirow{3}{*}{$\mathbf{0}$}} & 1&1&0&0&1&1&0 \\ \multicolumn{7}{c|}{} & 0&1&0&1&0&1&1 \\ \multicolumn{7}{c|}{} & 0&0&1&1&1&1&0 \end{array}\right]$$

The encoded operator $(1,1,0,0,0,0,1|\mathbf{0})$ maps to $(1,1,0,0,0,0,1|\mathbf{0})$. If we now transform the encoded operator to $(1,0,0,0,0,0,0|\mathbf{0})$ the stabilizer gets further transformed as

$$S \mapsto \left[\begin{array}{ccccccc|ccccccc} 0&0&0&0&1&1&1 & \multicolumn{7}{c}{\multirow{3}{*}{$\mathbf{0}$}} \\ 0&1&0&1&0&1&1 & \multicolumn{7}{c}{} \\ 0&0&1&1&1&1&0 & \multicolumn{7}{c}{} \\ \hline \multicolumn{7}{c|}{\multirow{3}{*}{$\mathbf{0}$}} & 0&1&0&0&1&1&0 \\ \multicolumn{7}{c|}{} & 0&1&0&1&0&1&1 \\ \multicolumn{7}{c|}{} & 0&0&1&1&1&1&0 \end{array}\right]$$

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 codeword in $C^{\perp}$ with $c_0 = 1$ defines an authorized set for the scheme. Suppose that c is a minimal codeword 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 [11] and Smith [27], based on monotone span programs. These constructions are not optimal in general. Our method gives optimal schemes with information rate one. 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 derived from matroids. Another interesting question would be to derive ideal quantum secret sharing schemes from non-representable ISD matroids.

Acknowledgment

We thank Hoi-Kwong Lo for pointing out an inaccuracy in an earlier version of 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, 2009. This research was supported by NSERC, CIFAR and MITACS.

[1] A. Beimel and N. Livne. On matroids and nonideal secret sharing. *IEEE Trans. Inform. Theory*, 54(6):2626–2643, 2008.

[2] M. Ben-Or, C. Crepeau, D. Gottesman, A. Hassidim, and A. Smith. Secure multiparty quantum computation with (only) a strict honest majority. *Foundations of Computer Science*, pages 249–260, 2006.

[3] G. R. Blakley. Safeguarding cryptographic keys. In *Proc. of the National Computer Conference*, pages 313–317, 1979.

[4] E. F. Brickell and D. M. Davenport. On the classification of ideal secret sharing schemes. *J. Cryptology*, 4:123–134, 1991.

[5] R. Cleve, D. Gottesman, and H.-K. Lo. How to share a quantum secret. *Phys. Rev. Lett.*, 83(3):648–651, 1999.

[6] R. Cramer, V. Daza, I. Gracia, J. J. Urroz, G. Leander, J. Martí-Farré, and C. Padró. On codes, matroids, and secure multiparty computation from secret-sharing schemes. *IEEE Trans. Inform. Theory*, 54(6):2644–2657, 2008.

[7] Markham D. and B. Sanders. Graph states for quantum secret sharing. *Phys. Rev. A*, 78(0423093), 2008.

[8] D. Dieks. Communication by EPR devices. *Physics Lett. A*, 6(22):271–272, 1982.

[9] S. Gaertner, C. Kurtsiefer, M. Bourennane, and H. Weinfurter. Experimental demonstration of four-party quantum secret sharing. *Phys. Rev. Lett.*, 98(020503), 2002.

[10] J. Dj. Golić. On matroid characterization of ideal secret sharing schemes. *J. Cryptology*, 11:95–86, 1998.

[11] D. Gottesman. Theory of quantum secret sharing. *Phys. Rev. A*, 61(042311), 2000.

[12] M. Grassl, M. Rötteler, and T. Beth. Efficient quantum circuits for non-qubit quantum error-correcting codes. *Internat. J. Found. Comput. Sci.*, 14(5):757–775, 2003.

[13] M. Hillery, V. Buzek, and A. Berthaume. Quantum secret sharing. *Phys. Rev. A*, 59(3):1829–1834, 1999.

[14] H. Imai, J. Müller-Quade, A. Nascimento, P. Tuyls, and A. Winter. An information theoretical model for quantum secret sharing schemes. *Quantum Information & Computation*, 5(1):068–079, 2004.

[15] A. Karlsson, M. Koashi, and N. Imoto. Quantum entanglement for secret sharing and secret splitting. *Phys. Rev. A*, 59(1):162–168, 1999.

[16] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, and P. K. Lam. Quantum state sharing. *Proc. SPIE*, 5468(100), 2004.

[17] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, and P. K. Lam. Tripartite quantum state sharing. *Phys. Rev. Lett.*, 92(177903), 2004.

[18] J. Martí-Farré and C. Padró. On secret sharing schemes, matroids and polymatroids. In *Fourth IACR Theory of Cryptography Conference TCC 2007, Lecture Notes in Computer Science, 4392*, pages 273–290, 2007.

[19] K. M. Martin. Discrete structures in the theory of secret sharing. PhD. Thesis, 1991.

[20] J. L. Massey. Minimal codewords and secret sharing. In *Proc. 6th Joint Swedish-Russian Workshop on Information Theory, Mölle, Sweden*, pages 276–279, 1993.

[21] J. Oxley. What is a matriod? eprint: http://www.math.lsu.edu/õxley/survey4.pdf, 2004.

[22] K. Rietjens, B. Schoenmakers, and P. Tuyls. Quantum information theoretical analysis of various constructions for quantum secret sharing. In *Proc. 2005 IEEE Intl. Symposium on Information Theory, Adelaide, Australia*, pages 1598–1602, 2005.

[23] P. D. Seymour. A forbidden minor characterization of matroid ports. *Quart. J. Math. Oxford Ser.*, 27:407–413, 1976.

[24] P. D. Seymour. On secret-sharing matroids. *J. Combinatorial Theory, B*, 56:69–73, 1992.

[25] A. Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.

[26] J. Simonis and A. Ashikhmin. Almost affine codes. *Designs, Codes, and Cryptography*, 14:179–197, 1998.

[27] A. Smith. Quantum secret sharing for general access structures. eprint: arXiv:quant-ph/0001087, 2000.

[28] D. E. Stinson. An explication of secret sharing schemes. *Designs, codes and crypography*, 2:357–390, 1992.

[29] W. Tittel, H. Zbinden, and N. Gisin. Experimental demonstration of quantum secret sharing. *Phys. Rev. A*, 63(0423013), 2001.

[30] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.

[31] L. Xiao, G. L. Long, Fu-G. Deng, and J.-W Pan. Efficient multiparty quantum-secret -sharing schemes. *Phys. Rev. A*, 69(052307), 2004.

[32] Strictly, [4, Theorem 2] only requires the matroid to be representable over a near field.

[33] If $(1|g)$ is not minimal, then there exists some codeword $(1|g')$ or $(0|a)$ such that its support is strictly contained in $\mathrm{supp}(1|g)$. If $\mathrm{supp}(0|a) \subset \mathrm{supp}(1|g)$, then we can find a codeword $(1|g')$, from a linear combination of $(1|g)$ and $(0|a)$, such that $\mathrm{supp}(1|g') \subset \mathrm{supp}(1|g)$ and $\mathrm{supp}(0|a) \not\subset \mathrm{supp}(1|g')$. In either case there is a codeword of the form $(1|g')$ whose support is strictly smaller than $\mathrm{supp}(1|g)$. If $(1|g')$ 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.