Sharing Classical Secrets with CSS Codes

Pradeep Kiran Sarvepalli[1, *] and Andreas Klappenecker[2, †]

[1]*Department of Physics and Astronomy*
University of British Columbia, Vancouver V6T 1Z1, Canada
[2]*Department of Computer Science*
Texas A&M University, College Station TX 77843-3112, USA

(Dated: May 11, 2009)

In this paper we investigate the use of quantum information to share classical secrets. While every quantum secret sharing scheme is a quantum error correcting code, the converse is not true. Motivated by this we sought to find quantum codes which can be converted to secret sharing schemes. If we are interested in sharing classical secrets using quantum information, then we show that a class of pure $[[n, 1, d]]_q$ CSS codes can be converted to perfect secret sharing schemes. These secret sharing schemes are perfect in the sense the unauthorized parties do not learn anything about the secret. Gottesman had given conditions to test whether a given subset is an authorized or unauthorized set; they enable us to determine the access structure of quantum secret sharing schemes. For the secret sharing schemes proposed in this paper the access structure can be characterized in terms of minimal codewords of the classical code underlying the CSS code. This characterization of the access structure for quantum secret sharing schemes is thought to be new.

Keywords: quantum secret sharing, CSS quantum codes, access structure, minimal codewords

I. INTRODUCTION

Quantum secret sharing schemes deal with the distribution of an arbitrary secret state among n parties (or shares) using quantum states such that only authorized subsets can reconstruct the secret. One can broadly classify quantum secret sharing schemes into the category of schemes allowing one to (a) share quantum secrets and (b) share classical secrets. This paper focuses on schemes of the second category (b).

Quantum secret sharing schemes of both categories were introduced by Hillery, Buzek, and Berthiaume [1]. Classically, one can always associate an error-correcting code to a perfect secret sharing scheme—though determining the access structure of the associated scheme is in general a very hard problem. Additionally, one can also derive a secret sharing scheme from a classical code, as was first illustrated by the work of Massey [2]. It is not surprising therefore that one finds connections between quantum secret sharing schemes and quantum codes. The connection between quantum secret sharing schemes and quantum codes was first made explicit in the work of Cleve et al. [3] and in greater depth by Gottesman in [4]. In fact Cleve et al [3] showed that quantum threshold schemes can be derived from quantum MDS codes and gave an explicit method for these schemes. More recently, Rietjens et al. [5] showed that a $((k, 2k-1))$ quantum threshold scheme exists if and only if a $[[2k - 1, 1, k]]_q$ quantum MDS code exists, thereby extending an earlier result found in [3]

However, the correspondence between quantum codes and quantum secret sharing schemes does not appear to be as strong as in the classical case. In general, one cannot derive a perfect quantum secret sharing scheme from a quantum code. However, if we restrict our secrets to being classical, then we can relate a pure $[[n, 1, d]]$ CSS code to a secret sharing scheme, as we will show below.

Using quantum information to secure classical secrets has been studied earlier in [1, 4, 6]. Gottesman had given a convenient characterization of the access structure of secret sharing schemes in [4]. For the schemes proposed in this paper we provide an alternative characterization which can perhaps be extended to more quantum state sharing schemes. The access structures of the secret sharing schemes proposed in this paper can be characterized using the notion of minimal codewords, a concept which was introduced by Massey [2] in the context of classical secret sharing. Additionally, we draw upon the work of Gottesman [4] to link these ideas.

A. Background: Quantum Secret Sharing

Let the parties of a secret sharing scheme be $P = \{P_1, \ldots, P_n\}$. Any subset of P that can reconstruct the secret is called an authorized set. Subsets which cannot reconstruct the secret are called unauthorized sets. The collection of authorized sets is called the access structure of the scheme and denoted by Γ. The collection of unauthorized sets is called the adversary structure and denoted by $\mathcal{A}$. Clearly, $\Gamma \cup \mathcal{A} = 2^P$, the power set of P. A minimal authorized set is one which can be used to reconstruct the secret but no proper subset of which can reconstruct the secret. Clearly any subset which contains a minimal authorized set is also authorized. The minimal access structure of the secret sharing scheme is the multiset consisting of minimal authorized sets. We denote a secret sharing scheme with (minimal) access structure Γ_m as (Σ, Γ_m).

Of course, the secret sharing scheme must specify more than the access structure. It must specify a means to encode the secret into the n different shares and how any authorized set can recover the secret. In the language of quantum error correction these two tasks translate into encoding and decoding of a quantum state which has been transmitted through a noisy quantum channel, in this case the quantum erasure channel. A secret sharing scheme is said to be perfect if

  i) an authorized set exactly reconstructs the secret

  ii) an unauthorized cannot extract any information about the secret

Essentially, any perfect secret sharing scheme must satisfy two requirements. On one hand, there is the requirement of secrecy; any unauthorized set must know nothing about the secret. On the other hand, there is the requirement of recoverability; any authorized set must be able to reconstruct the secret. One can also give a quantum information theoretic characterization of these requirements as was done in [7]. A characterization of these requirements for quantum secret sharing schemes can be found in [4], see also [3]. In particular, for classical secrets this formulation is given as follows, see [4, Theorem 9] for details.

Lemma 1 (Gottesman)**.** *Suppose we have a set of orthonormal states* $|\psi_i\rangle$ *encoding a classical secret. Then a set* T *is an unauthorized set iff*

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

independent of i *for all operators* F *on* T. *The set* T *is authorized iff*

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

for all operators E *on the complement of* T.

We can state these conditions more informally. For an unauthorized set T, there is no measurement that can be be performed on the qubits in the support of T that can extract any information about the states $|\psi_i\rangle$. Since an authorized set T is to recover the secret, it can in effect correct erasures on the complement of T. If the conditions hold for any orthonormal basis of the space spanned by $|\psi_i\rangle$, then these states can also be used for sharing quantum states, see for instance [4, Theorem 1], [3, Theorem 7].

Remark 2. *We need not consider all operators on* T, *we only need to consider a basis of the operators on* T. *For q-ary quantum systems schemes this basis of error operators can be identified with vectors in* $\mathbb{F}_q^{2n}$.

We assume some background in (nonbinary) quantum codes, the reader can refer to [8] for more details. Let q be the power of a prime p. Let $B = \{|x\rangle \mid x \in \mathbb{F}_q\}$ denote an orthonormal basis for $\mathbb{C}^q$. For $a, b \in \mathbb{F}_q$, we define operators $X(a)$ and $Z(b)$ by

$$X(a)\,|x\rangle = |x+a\rangle \quad Z(b)\,|x\rangle = \omega^{\mathrm{tr}_{q/p}(bx)}\,|x\rangle, \tag{3}$$

where $x \in \mathbb{F}_q$, $\omega = e^{j2\pi/p}$, and $j = \sqrt{-1}$. These operators form a basis for error operators over a single qudit. Over n qudits, we define the error operator

$$X(a)Z(b) = X(a_1)Z(b_1) \otimes \cdots \otimes X(a_n)Z(b_n)$$

for $a = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$ and $b = (b_1, \ldots, b_a) \in \mathbb{F}_q^n$. The error operators $\mathcal{E} = \{X(a)Z(b) \mid a, b \in \mathbb{F}_q^n\}$ form a basis for error operators over n qudits. We shall often denote $X(a)Z(b)$ by its representative over $\mathbb{F}_q^{2n}$ as $(a|b)$. We say that an error operator $X(a)Z(b)$ has a support over $T \subseteq \{1, \ldots, n\}$ if $(a_t, b_t) \neq (0, 0)$ for all $t \in T$, and $(a_t, b_t) = (0, 0)$ otherwise.

II. SHARING CLASSICAL SECRETS

In this section we shall show that a pure $[[n, 1, d]]$ CSS code can be converted into a secret sharing scheme. We shall also characterize the access structure of the scheme by using the notion of minimal codewords. Throughout this section we assume that the $[[n, 1, d]]$ code under consideration has been derived from a classical code $C \supseteq C^\perp$ with the parameters $[n, k, d]_q$ whose parity check matrix is given as $H = \begin{bmatrix} I_{n-k} & P \end{bmatrix}$. The dual code $C^\perp$ is defined as $C^\perp = \{x \in \mathbb{F}_q^n \mid x \cdot c = 0 \text{ for all } c \in C\}$. The stabilizer (matrix) of the CSS code is given as

$$S = \left[\begin{array}{c|c} H & 0 \\ 0 & H \end{array}\right]. \tag{4}$$

Recall that the errors detectable by the CSS code are in $\mathbb{F}_q^{2n} \setminus (C \oplus C)$ or $C^\perp \oplus C^\perp$, where $C \oplus C$ is the direct sum of C with itself. The undetectable errors are in $(C \oplus C) \setminus C^\perp \oplus C^\perp$.

To define the minimal access structure of the secret sharing scheme we need the notion of minimal codewords. Let $x, y \in \mathbb{F}_q^n$, then x is said to cover y if the support of x contains the support of y. Alternatively, y_i is zero whenever $x_i = 0$, where we assume that $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$. A codeword $x \in C$ is said to be a minimal codeword if

  i) its left most component is 1 and

  ii) it does not cover any other codeword of C except scalar multiples of x.

A codeword which only satisfies ii) is said to be a minimal support. Every minimal codeword is of course a minimal support. Minimal codewords were first introduced by Massey in the context of classical secret sharing schemes, enabling a one to one correspondence with minimal authorized sets. Minimal supports play an important role in studying the local equivalence of stabilizer states. We also need the following lemma.

Lemma 3. *Let* Q *be a pure* $[[n, 1, d]]_q$ *CSS code derived from* $C^\perp \subseteq C \subseteq \mathbb{F}_q^n$. *For any two vectors* $x, y \in C \setminus C^\perp$ *we have* $x \cdot y \neq 0$. *If* $q = 2$, *we have* $x \cdot y = 1$ *and* d *odd.*

Proof. Given the parameters of the quantum code the codes C and $C^\perp$ must have the parameters $[n, k, d]_q$ and $[n, n - k = k - 1, d]_q$ respectively. Since $C \neq C^\perp$, it follows that there is at least one vector c in $C \setminus C^\perp$, that satisfies $c \cdot c \neq 0$. Because $\dim C - \dim C^\perp = 1$ we infer that c and $C^\perp$ generate C. Therefore for any two vectors x, y in $C \setminus C^\perp$ we can write them as $x = \alpha c + s_x$ and $y = \beta c + s_y$ for some $s_x, s_y \in C^\perp$ and $\alpha, \beta \in \mathbb{F}_q^\times$. Hence, $x \cdot y = (\alpha c + s_x) \cdot (\beta c + s_y) = \alpha\beta(c \cdot c) \neq 0$. If $q = 2$, then it follows that $x \cdot y = 1$. In particular $x \cdot x = 1$, which implies that the weight of x must be odd. Since the minimum distance depends on the weight of elements in $C \setminus C^\perp$, we conclude that d is odd. $\qquad\square$

A. Proposed Secret Sharing Scheme

First we shall describe the scheme and then show that it is indeed a valid secret sharing scheme.

Theorem 4. *Let Q be a pure $[[n, 1, d]]_q$ CSS code derived from a classical code $C^\perp \subseteq C \subseteq \mathbb{F}_q^n$. Let $\mathcal{E}$ be the encoding given by the CSS code*

$$\mathcal{E} : |i\rangle \mapsto \sum_{x \in C^\perp} |x + ig\rangle \quad i \in \mathbb{F}_q, \tag{5}$$

where $g \in C \setminus C^\perp$ and $g \cdot g = \beta$. Distribute the n qudits as the n shares for a secret sharing scheme, Σ. The minimal access structure Γ_m is given by

$$\Gamma_m = \big\{ \mathrm{supp}(c) \,|\, c \text{ is a minimal codeword in } C \setminus C^\perp \big\} \tag{6}$$

Let $c = \alpha g + s_c$ be a minimal codeword for some $s_c \in C^\perp$. The reconstruction for the authorized set $\mathrm{supp}(c)$ derived from c is to compute

$$(\alpha\beta)^{-1} \sum_{j \in \mathrm{supp}(c)} c_j S_j, \tag{7}$$

where S_j is the share of the jth party.

Proof. The proof of this theorem is a little long, so we shall break it into parts. First we shall show that the minimal codewords define authorized sets i.e., they can recover the secret. Next we shall show that the associated authorized sets are minimal. Thirdly, we shall show that Γ is complete i.e., every minimal authorized set is in Γ.

1) Recoverability: Let c be a codeword in $C \setminus C^\perp$, not necessarily minimal. Then c can be written as $c = \alpha g + s_c$ for some $s_c \in C$ and $\alpha \in \mathbb{F}_q^\times$. Adjoining an ancilla and computing the dot product with $c = \alpha g + s_c$ we get

$$|0\rangle \big|ig + C^\perp\big\rangle \mapsto \sum_{x \in C^\perp} |c \cdot x + c \cdot ig\rangle |x + ig\rangle,$$

$$= \sum_{x \in C^\perp} |c \cdot x + \alpha g \cdot ig + s_c \cdot ig\rangle |x + ig\rangle,$$

Since $c, g \in C \setminus C^\perp$ and $x, s_c \in C^\perp$ we have $c \cdot x = s_c \cdot ig = 0$. Let $g \cdot g = \beta$, then by Lemma 3, $\beta \neq 0$ and is invertible in $\mathbb{F}_q$. It follows

$$|0\rangle \big|ig + C^\perp\big\rangle \mapsto |\alpha\beta i\rangle \sum_{x \in C^\perp} |x + ig\rangle.$$

Since both α and β are known the secret can be recovered from the ancilla which is in the state $|\alpha\beta i\rangle$. This proves that these subsets can reconstruct the secret and they indeed define authorized sets. So every code word in $C \setminus C^\perp$ can define an authorized set but it need not be minimal. Consequently every minimal codeword in $C \setminus C^\perp$ also defines an authorized set.

2) Minimality of the authorized sets: Now let c be a minimal codeword. We shall show that in this case that any proper subset of $\mathrm{supp}(c)$ cannot reconstruct the secret. Let T be a proper subset of $\mathrm{supp}(c)$. Let the error operator $E = (a|b)$ be supported in T where $a, b \in \mathbb{F}_q^n$, then $(a|b)$ cannot be a codeword in $C \oplus C$. Suppose it were a codeword in $C \oplus C$, then both $a, b \in C$. Since E is nontrivial at least one of a and b is nonzero and covered by c, but then c would not be a minimal codeword. Therefore any error on T must be in $\mathbb{F}_q^{2n} \setminus (C \oplus C)$. But this means that any such operator is detectable by the quantum code Q. If it is detectable, then it must not reveal any information about the encoded states. In particular, it implies that T satisfies equation (1). Therefore every proper subset of $\mathrm{supp}(c)$ is an unauthorized set. This shows that $\mathrm{supp}(c)$ is a minimal authorized set.

3) Completeness of Γ_m: Next we show that all minimal authorized sets are in Γ_m. Assume that there exists a minimal authorized set T which is not in Γ_m. Then T must satisfy equation (2). Additionally, T fails to satisfy equation (1) while every proper subset of T being an unauthorized set does satisfy equation (1). This forces the existence of an operator $E = (a|b)$, with $\mathrm{supp}(E) = T$, that violates equation (1). Now E cannot be in $\mathbb{F}_q^n \setminus (C \oplus C)$ or $C^\perp \oplus C^\perp$, as these operators are detectable and cannot violate equation (1). Therefore, E must be in $(C \oplus C) \setminus (C^\perp \oplus C^\perp)$. Further, $(a|b) \in C \oplus C$ implies that $a, b \in C$. Now both a, b cannot be in $C^\perp \subset C$ as then $(a|b)$ would be entirely in $C^\perp \oplus C^\perp$ and it would be detectable and cannot define an authorized set. So at least one of a, b is in $C \setminus C^\perp$. Without loss of generality let us assume that $a \in C \setminus C^\perp$. But we already saw in step 1), that any codeword in $C \setminus C^\perp$ defines an authorized set. So $\mathrm{supp}((a|0)) = \mathrm{supp}(a)$ is itself an authorized set. Since $(a|b)$ is a minimal authorized set, $\mathrm{supp}(a) = \mathrm{supp}(a|b) = T$.

Suppose that a is not a minimal codeword. Then there is some vector in C that is covered by a and is not a scalar multiple of a. First we show that there exists no $d \in C$ such that $\mathrm{supp}(d) \subsetneq T$. If $\mathrm{supp}(d)$ was a proper subset of $\mathrm{supp}(a)$, then d cannot be in $C \setminus C^\perp$

as it would then define an authorized set that is a proper subset of the minimal authorized set T. If d is in $C^\perp$, then there exists a linear combination of a and d with support strictly a subset of T. Further this linear combination is also in $C \setminus C^\perp$ and by step 1) it would define an authorized set violating the minimality of T. Therefore any $d \in C$ covered by a and not a scalar multiple of a must have $\text{supp}(d) = T$. But this implies that C contains a linear combination of a and d with support strictly less than T violating our previous conclusion that there exists no such element in C. Therefore a is a minimal codeword of C and it lies in $C \setminus C^\perp$. (If the left most component of a is not 1 we can choose a scalar multiple of it so that it is 1. In any case, a and its scalar multiples have same support and they correspond to the same (minimal) authorized set).

$\square$

Since a codeword of minimum distance does not cover any other codeword, there always exists a scalar multiple of it which is a minimal codeword. Therefore, the minimal access structure always contains the sets corresponding to the support of the every minimum distance codeword in $C \setminus C^\perp$.

Corollary 5. *In the secret sharing scheme specified in Theorem 4, the support of every minimum distance codeword in $C \setminus C^\perp$ gives rise to a minimal authorized set.*

If $q = 2$, then we can simplify the reconstruction process, we only need to take the parity of the parties in the minimal authorized set.

Corollary 6. *Let Q be a pure $[[n, 1, d]]_2$ CSS code derived from a classical code $C^\perp \subseteq C \subseteq \mathbb{F}_2^n$. Let $\mathcal{E}$ be the encoding given by the CSS code*

$$\mathcal{E} : |i\rangle \mapsto \sum_{x \in C^\perp} |x + ig\rangle \quad i \in \mathbb{F}_2, \qquad (8)$$

where $g \in C \setminus C^\perp$. Distribute the n qubits as the n shares for a secret sharing scheme, Σ. The minimal access structure Γ_m is given by

$$\Gamma_m = \big\{ \text{supp}(c) \,|\, c \text{ is a minimal codeword in } C \setminus C^\perp \big\} (9)$$

The reconstruction for an authorized set is to simply compute the parity of the set (into an ancilla).

The secret can be encoded using the encoding methods of CSS codes, see [9]. Reconstructing the secret for these schemes is extremely simple as shown below. We will need the multiplier gate $M(c)$ and the generalized CNOT gate, A shown below.
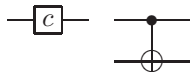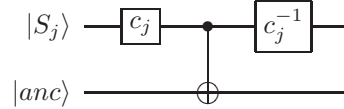

i)   ii)

Their action on the basis states is given as:

i) $M(c) |x\rangle = |cx\rangle, c \in \mathbb{F}_q^\times$
ii) $A |x\rangle |y\rangle = |x\rangle |x + y\rangle$

The recovery as given in equation (7) is computed by performing the following operation for each $c_j \neq 0$.

The final scaling by $(\alpha\beta)^{-1}$ can be done classically.

B.   Illustration

We illustrate the strategy using a $[[11, 1, 3]]$ CSS code [10] it can be derived from a code C with the following generator and parity check matrices.

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \end{bmatrix} \qquad (10)$$

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \end{bmatrix} \qquad (11)$$

Let us encode the secret

$$|s\rangle \mapsto \sum_{c \in C^\perp} |c + se\rangle, \qquad (12)$$

where $e = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}$. The secret sharing scheme assumes that we distribute each qubit as a share. The minimal access structure of the secret sharing scheme is given by Γ_m.

$$\Gamma_m = \left\{ \begin{array}{c} \{3, 10, 11\}; \{6, 9, 11\}; \{4, 7, 11\}; \{2, 5, 11\}; \\ \{1, 8, 11\}; \{2, 3, 4, 6, 8\}; \\ \{4, 5, 6, 8, 10\}; \{1, 3, 4, 5, 6\}; \{1, 2, 4, 6, 10\}; \\ \{3, 4, 5, 8, 9\}; \{2, 4, 8, 9, 10\}; \{1, 2, 3, 4, 9\}; \\ \{1, 4, 5, 9, 10\}; \{3, 5, 6, 7, 8\}; \{2, 6, 7, 8, 10\}; \\ \{1, 2, 3, 6, 7\}; \{1, 5, 6, 7, 10\}; \{5, 7, 8, 9, 10\}; \\ \{2, 3, 7, 8, 9\}; \{1, 3, 5, 7, 9\}; \{1, 2, 7, 9, 10\} \end{array} \right\}$$

It can be checked that the parity of any of these subsets will give s. Further, any subset that contains an element of Γ_m as a subset can also perform reconstruction. Please note that this is not a threshold scheme, there exist minimal authorized sets of size three and five.

III.   CONCLUSION

In this paper we have given new methods to share classical secrets using quantum information. We have been

able to strengthen the connection between quantum secret sharing schemes and quantum error correcting codes and given a new characterization of the access structure in terms of minimal codewords. This characterization is potentially of larger applicability, and its extension to additive quantum codes and quantum secrets will be explored elsewhere.

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

[2] J. L. Massey, in *Proc. 6th Joint Swedish-Russian Workshop on Information Theory, Mölle, Sweden* (1993), pp. 276–279.

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

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

[5] K. Rietjens, B. Schoenmakers, and P. Tuyls, in *Proc. 2005 IEEE Intl. Symposium on Information Theory, Adelaide, Australia* (2005), pp. 1598–1602.

[6] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999).

[7] H. Imai, J. Müller-Quade, A. Nascimento, P. Tuyls, and A. Winter, Quantum Information & Computation **5**, 068 (2004).

[8] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, IEEE Trans. Inform. Theory **52**, 4892 (2006).

[9] M. Grassl, M. Rötteler, and T. Beth, Internat. J. Found. Comput. Sci. **14**, 757 (2003).

[10] M. Grassl (2000), Lower Bounds and Encoding Circuits of Weakly Self-Dual CSS Codes http://avalon.ira.uka.de/home/grassl/QECC/CSS.