Classical access structures of ramp secret sharing based on quantum stabilizer codes (extended abstract*)

Ryutaroh Matsumoto[1,2][0000−0002−5085−8879]

[1] Department of Information and Communication Engineering,
Nagoya University, Nagoya, Japan. ryutaroh.matsumoto@nagoya-u.jp
[2] Department of Mathematical Sciences, Aalborg University, Denmark.

Abstract. In this paper we consider to use the quantum stabilizer codes as secret sharing schemes for classical secrets. We give necessary and sufficient conditions for qualified and forbidden sets in terms of quantum stabilizers. Then we give a Gilbert-Varshamove-type sufficient condition for existence of secret sharing schemes with given parameters, and by using that sufficient condition, we show that roughly 19% of participants can be made forbidden independently of the size of classical secret, in particular when an n-bit classical secret is shared among n participants having 1-qubit share each. We also consider how much information is obtained by an intermediate set and express that amount of information in terms of quantum stabilizers. All the results are stated in terms of linear spaces over finite fields associated with the quantum stabilizers.

Keywords: secret sharing · quantum error-correcting code · symplectic form

1 Introduction

Secret sharing is a scheme to share a secret among multiple participants so that only *qualified* sets of participants can reconstruct the secret, while *forbidden* sets have no information about the secret [32]. A piece of information received by a participant is called a *share*. A set of participants that is neither qualified nor forbidden is said to be *intermediate*. Both secret and shares are traditionally classical information. There exists a close connection between secret sharing and classical error-correcting codes [3,7,10,11,18,20,28].

After the importance of quantum information became well-recognized, secret sharing schemes with quantum shares were proposed [8,14,15,16,33]. A connection between quantum secret sharing and quantum error-correcting codes has been well-known for many years [8,14,33]. Well-known classes of quantum error-correcting codes are the CSS codes [5,34], the stabilizer codes [4,6,13] and their nonbinary generalizations [2,17,26].

The access structure of a secret sharing scheme is the set of qualified sets, that of intermediate sets and that of forbidden sets. For practical use of secret sharing, one needs sufficient (and desirably necessary) conditions on qualified sets and forbidden sets.

It is natural to investigate access structures of secret sharing schemes constructed from quantum error-correcting codes. For secret sharing schemes with quantum secret and quantum shares, necessary and sufficient conditions for qualified sets and forbidden sets were clarified for the CSS codes [33,23] and the stabilizer codes [22].

For classical secret and quantum shares, the access structure was clarified in [23, Section 4.1] with [30, Theorem 1] for the CSS codes but has not been clarified for secret sharing schemes based on quantum stabilizer codes, as far as we know.

Advantages of using quantum shares for sharing a classical secret are that we can have smaller size of shares [14, Section 4], and that we can realize access structures that cannot be realized by classical shares [21,24]. For example, it is well-known that the size of classical shares cannot be smaller than that of the classical secret in a perfect secret sharing scheme, where *perfect* means that there is no intermediate set, while *ramp* or *non-perfect* means that there exist intermediate sets [35]. On the other hand, the superdense coding can be a secret sharing scheme sharing 2 bits by 2 qubits sent to 2 participants [14, Section 4]. Any participant has no information about the secret, while the 2 participants can reconstruct the secret. We see a perfect threshold scheme sharing 2-bit classical secret by 1-qubit shares. This paper will generalize Gottesman's secret sharing to the arbitrary number of participants and the arbitrary size of classical secrets.

In this paper we give necessary and sufficient conditions for qualified and forbidden sets in terms of the underlying linear spaces over finite fields of quantum stabilizers, and give sufficient conditions in terms of a quantity similar to relative generalized Hamming weight [19] of classical linear codes related to the quantum stabilizers. We also consider how much information is obtained by an intermediate set and express that amount of information in terms of the underlying linear spaces of quantum stabilizers. Then we translate our theorems over prime finite fields by the symplectic inner product into arbitrary finite fields, the Euclidean, and the hermitian inner products. Finally we give a Gilbert-Varshamove-type sufficient condition for existence of secret sharing schemes with given parameters, and by using that sufficient condition, we show that roughly 19% of participants can be made forbidden independently of the size of classical secret, which cannot be realized by classical shares.

2 Notations

Let p be a prime number, $\mathbf{F}_p$ the finite field with p elements, and $\mathbf{C}_p$ the p-dimensional complex linear space. The quantum state space of n qudits is denoted by $\mathbf{C}_p^{\otimes n}$ with its orthonormal basis $\{|\vec{v}\rangle \mid \vec{v} \in \mathbf{F}_p^n\}$.

For two vectors $\vec{a}, \vec{b} \in \mathbf{F}_p^n$, denote by $\langle \vec{a}, \vec{b} \rangle_E$ the standard Euclidean inner product. For two vectors $(\vec{a}|\vec{b})$ and $(\vec{a'}|\vec{b'}) \in \mathbf{F}_p^{2n}$, we define the standard symplectic inner product

$$\langle (\vec{a}|\vec{b}), (\vec{a'}|\vec{b'}) \rangle_s = \langle \vec{a}, \vec{b'} \rangle_E - \langle \vec{a'}, \vec{b} \rangle_E.$$

For an $\mathbf{F}_p$-linear space $C \subset \mathbf{F}_p^{2n}$, $C^{\perp s}$ denotes its orthogonal space in $\mathbf{F}_p^{2n}$ with respect to $\langle \cdot, \cdot \rangle_s$. Throughout this paper we always assume $\dim C = n - k$ and $C \subseteq C^{\perp s}$.

For $(\vec{a}|\vec{b}) \in \mathbf{F}_p^{2n}$, define the $p^n \times p^n$ complex unitary matrix $X(\vec{a})Z(\vec{b})$ as defined in [17]. An $[[n, k]]_p$ quantum stabilizer codes Q encoding k qudits into n qudits can be

defined as a simultaneous eigenspace of all $X(\vec{a})Z(\vec{b})$ ($(\vec{a}|\vec{b}) \in C$). Unlike [17] we do not require the eigenvalue of Q to be one.

It is well-known in mathematics [1, Chapter 7] that there always exists $C \subseteq C_{\max} \subseteq C^{\perp s}$ such that $C_{\max} = C_{\max}^{\perp s}$. Note that $C_{\max}$ is not unique and usually there are many possible choices of $C_{\max}$. We have $\dim C_{\max} = n$ and have an isomorphism $f : \mathbf{F}_p^k \to C^{\perp s}/C_{\max}$ as linear spaces without inner products. Since $C_{\max} = C_{\max}^{\perp s}$, $C_{\max}$ defines an $[[n, 0]]_p$ quantum stabilizer code Q_0. Without loss of generality we may assume $Q_0 \subset Q$. Let $|\varphi\rangle \in Q_0$ be a quantum state vector. Since $C_{\max} = C_{\max}^{\perp s}$, for a coset $V \in C^{\perp s}/C_{\max}$ and $(\vec{a}|\vec{b})$, $(\vec{a'}|\vec{b'}) \in V$, $X(\vec{a})Z(\vec{b})|\varphi\rangle$ and $X(\vec{a'})Z(\vec{b'})|\varphi\rangle$ differ by a constant multiple in $\mathbf{C}$ and physically express the same quantum state in Q. By an abuse of notation, for a coset $V \in C^{\perp s}/C_{\max}$ we will write $|V\varphi\rangle$ to mean $X(\vec{a})Z(\vec{b})|\varphi\rangle$ ($(\vec{a}|\vec{b}) \in V$).

For a given classical secret $\vec{m} \in \mathbf{F}_p^k$, we consider the following secret sharing scheme with n participants:

1. $f(\vec{m})$ is a coset of $C^{\perp s}/C_{\max}$. Prepare the quantum codeword $|f(\vec{m})\varphi\rangle \in Q$ corresponding to the classical secret $\vec{m}$.
2. Distribute each qudit in the quantum codeword $|f(\vec{m})\varphi\rangle$ to a participant.

We can also consider a secret sharing scheme for a k-qudit secret $|\vec{m}\rangle$ with n participants as follows:

1. Encode a given quantum secret $\sum_{\vec{m}\in\mathbf{F}_p^k} \alpha(\vec{m})|\vec{m}\rangle$ into the quantum codeword $\sum_{\vec{m}\in\mathbf{F}_p^k} \alpha(\vec{m})|f(\vec{m})\varphi\rangle \in Q$, where $\alpha(\vec{m}) \in \mathbf{C}$ are complex coefficients with $\sum_{\vec{m}\in\mathbf{F}_p^k} |\alpha(\vec{m})|^2 = 1$.
2. Distribute each qudit in the quantum codeword $\sum_{\vec{m}\in\mathbf{F}_p^k} \alpha(\vec{m})|f(\vec{m})\varphi\rangle$ to a participant.

Let $A \subset \{1, \ldots, n\}$ be a set of shares (or equivalently participants), $\overline{A} = \{1, \ldots, n\} \setminus A$, and $\mathrm{Tr}_{\overline{A}}$ the partial trace over $\overline{A}$. For a density matrix ρ, $\mathrm{col}(\rho)$ denotes its column space. When $\mathrm{col}(\rho_1), \ldots, \mathrm{col}(\rho_n)$ are orthogonal to each other, that is, $\rho_i\rho_j = 0$ for $i \neq j$, we can distinguish $\rho_1, \ldots, \rho_n$ by a suitable projective measurement with probability 1.

Definition 1. *We say A to be c-qualified (classically qualified) if* $\mathrm{col}(\mathrm{Tr}_{\overline{A}}(|f(\vec{m})\varphi\rangle\langle f(\vec{m})\varphi|))$ *and* $\mathrm{col}(\mathrm{Tr}_{\overline{A}}(|f(\vec{m'})\varphi\rangle\langle f(\vec{m'})\varphi|))$ *are orthogonal to each other for different $\vec{m}$, $\vec{m'} \in \mathbf{F}_p^k$. We say A to be c-forbidden (classically forbidden) if* $\mathrm{Tr}_{\overline{A}}(|f(\vec{m})\varphi\rangle\langle f(\vec{m})\varphi|)$ *is the same density matrix regardless of classical secret $\vec{m}$. By a classical access structure we mean the set of c-qualified sets and the set of c-forbidden sets.*

For a quantum secret, the quantum qualified (q-qualified) sets and the quantum forbidden (q-forbidden) sets are mathematically defined in [30]. By a quantum access structure we mean the set of q-qualified sets and the set of q-forbidden sets.

Remark 2. When classical shares on A is denoted by S_A, the conventional definition of qualifiedness is $I(\vec{m}; S_A) = H(\vec{m})$ and that of forbiddenness is $I(\vec{m}; S_A) = 0$ [35], where $H(\cdot)$ denotes the entropy and $I(\cdot;\cdot)$ denotes the mutual information [9]. Let

$\rho_A = \sum_{\vec{m}\in\mathbf{F}_p^k} p(\vec{m})\mathrm{Tr}_{\overline{A}}(|f(\vec{m})\varphi\rangle\langle f(\vec{m})\varphi|)$, where $p(\vec{m})$ is the probability distribution of classical secrets $\vec{m}$. The quantum counterpart of mutual information for classical messages is the Holevo information $I(\vec{m};\rho_A)$ [29, Chapter 12]. A is c-qualified if and only if $I(\vec{m};\rho_A) = H(\vec{m})$, and is c-forbidden if and only if $I(\vec{m};\rho_A) = 0$. Therefore, Definition 1 is a natural generalization of the conventional definition in [35].

Example 3. We will see how one can express the secret sharing scheme based on superdense coding [14, Section 4] by a quantum stabilizer. Let $p = 2$, $n = 2$ and C be the zero-dimensional linear space consisting of only the zero vector. Then $C^{\perp_s} = \mathbf{F}_2^4$. We choose $C_{\max}$ as the space spanned by $(1,1|0,0)$ and $(0,0|1,1)$. For a classical secret $(m_1,m_2) \in \mathbf{F}_2^2$, define the map f as $f(m_1,m_2) = (m_1,0|m_2,0) + C_{\max} \in C^{\perp_s}/C_{\max}$. We can choose $[[2,0]]_2$ quantum code Q_0 as the one-dimensional complex linear space spanned by the Bell state

$$|\varphi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}},$$

which corresponds to the two-bit secret $(0,0)$. The secret (m_1,m_2) is encoded to

$$X(m_1,0)Z(m_2,0)|\varphi\rangle = \frac{|m_1 0\rangle + (-1)^{m_2}|(1-m_1)1\rangle}{\sqrt{2}}.$$

It is clear that the share set $\{1,2\}$ is c-qualified. When $A = \{1\}$ or $A = \{2\}$, we have

$$\mathrm{Tr}_{\overline{A}}(|f(\vec{m})\varphi\rangle\langle f(\vec{m})\varphi|) = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

which means $\{1\}$, $\{2\}$ and $\emptyset$ are c-forbidden. We have determined the classical access structure completely, and we see that this scheme is perfect [35] in the sense that there is no intermediate set.

3 Necessary and sufficient conditions on classically qualified and classically forbidden sets

Let $A \subset \{1,\ldots,n\}$. Define $\mathbf{F}_p^A = \{(a_1,\ldots,a_n|b_1,\ldots,b_n) \in \mathbf{F}_p^{2n} \mid (a_i,b_i) = 0 \text{ for } i \notin A\}$. Let P_A to be the projection map onto A, that is, $P_A(a_1,\ldots,a_n|b_1,\ldots,b_n) = (a_i|b_i)_{i\in A}$.

Theorem 4. *For the secret sharing scheme described in Section 2, A is c-qualified if and only if*

$$\dim C_{\max}/C = \dim C_{\max} \cap \mathbf{F}_p^A / C \cap \mathbf{F}_p^A. \tag{1}$$

A is c-forbidden if and only if

$$0 = \dim C_{\max} \cap \mathbf{F}_p^A / C \cap \mathbf{F}_p^A. \tag{2}$$

Proof. See [25]. □

Example 5. Consider the situation in Example 3. For $A = \{1\}$ or $A = \{2\}$, we see that $C_{\max} \cap \mathbf{F}_2^A$ and $C \cap \mathbf{F}_2^A$ are the zero linear space and that Eq. (2) holds. For $A = \{1,2\}$, Eq. (1) is clearly true.

Example 6. In this example, we show that a different choice of $C_{\max}$ gives a different access structure. Let C be as Example 5, and $C_{\max}$ be the linear space generated by $(0,0|1,0)$ and $(0,0|0,1)$. A classical secret (m_1, m_2) is now encoded to $|m_1 m_2\rangle$. For $A = \{1\}$ or $A = \{2\}$, both (1) and (2) are false and both $A = \{1\}$ and $A = \{2\}$ are intermediate sets. This example shows that the choice of $C_{\max}$ is important.

Next we give sufficient conditions in terms of the coset distance [11] or the first relative generalized Hamming weight [19]. To do so, we have to slightly modify them. For $(\vec{a}|\vec{b}) = (a_1, \ldots, a_n|b_1, \ldots, b_n) \in \mathbf{F}_p^n$, define its symplectic weight $\mathrm{swt}(\vec{a}|\vec{b}) = |\{i \mid (a_i, b_i) \neq (0,0)\}|$. For $V_2 \subset V_1 \subset \mathbf{F}_p^{2n}$, we define their coset distance as $d_s(V_1, V_2) = \min\{\mathrm{swt}(\vec{a}|\vec{b}) \mid (\vec{a}|\vec{b}) \in V_1 \setminus V_2\}$.

Theorem 7. *If $|A| \leq d_s(C_{\max}, C) - 1$ then A is c-forbidden. If $|A| \geq n - d_s(C^{\perp_s}, C_{\max}) + 1$ then A is c-qualified.*

Proof. See [25]. □

Example 8. Consider the situation in Example 5. We have $d_s(C^{\perp}, C_{\max}) = 1$, which implies that 2 shares is a c-qualified set. We also have $d_s(C_{\max}, C) = 2$, which implies that 1 share is a c-forbidden set.

4 Amount of information possessed by an intermediate set

Let $A \subset \{1, \ldots, n\}$ with $A \neq \emptyset$ and $A \neq \{1, \ldots, n\}$. In this section we study the amount of information possessed by A.

Proposition 9. *Let $\{(\vec{a}_1|\vec{b}_1)+C\cap\mathbf{F}_p^A, \ldots, (\vec{a}_\ell|\vec{b}_\ell)+C\cap\mathbf{F}_p^A\}$ be a basis of $C_{\max}\cap\mathbf{F}_p^A/C\cap\mathbf{F}_p^A$. The number of density matrices in $\Lambda = \{\mathrm{Tr}_{\overline{A}}(|f(\vec{m}_1)\varphi\rangle\langle f(\vec{m})\varphi|) \mid \vec{m} \in \mathbf{F}_p^k\}$ is p^ℓ.*

For a fixed density matrix $\rho \in \Lambda$, the number of classical secrets $\vec{m}$ such that $\rho = \mathrm{Tr}_{\overline{A}}(|f(\vec{m}_1)\varphi\rangle\langle f(\vec{m})\varphi|)$ is exactly $p^{k-\ell}$.

Proof. See [25]. □

Definition 10. *In light of Proposition 9, the amount of information possessed by a set A of participants is defined as*

$$\log_2 p \times \dim C_{\max} \cap \mathbf{F}_p^A / C \cap \mathbf{F}_p^A. \tag{3}$$

Remark 11. When the probability distribution of classical secrets $\vec{m}$ is uniform, the quantity in Definition 10 is equal to the Holveo information [29, Chapter 12] counted in $\log_p$. Firstly, the set Λ in Proposition 9 consists of non-overlapping projection matrices and each matrix commutes with every other matrices in Λ. So the Holevo information is just equal to the classical mutual information [9] between random variable X on $\mathbf{F}_p^k$ and random variable Y on $\mathbf{F}_p^\ell$, where Y is given as a surjective linear function of X. Therefore $I(X;Y) = H(Y) - \underbrace{H(Y|X)}_{=0} = \ell$.

We say that a secret sharing scheme is r_i-reconstructible if $|A| \geq r_i$ implies A has $i \log_2 p$ or more bits of information [12]. We say that a secret sharing scheme is t_i-private if $|A| \leq t_i$ implies A has less than $i \log_2 p$ bits of information [12]. In order to express r_i and t_i in terms of combinatorial properties of C, we introduce a slightly modified version of the relative generalized Hamming weight [19].

Definition 12. *For two linear spaces $V_2 \subset V_1 \subset \mathbf{F}_p^{2n}$, define the i-th relative generalized symplectic weight*

$$d_s^i(V_1, V_2) = \min\{|A| \mid \dim \mathbf{F}_p^A \cap V_1 - \dim \mathbf{F}_p^A \cap V_2 \geq i\}. \tag{4}$$

Note that $d_s^1 = d_s$. The following theorem generalizes Theorem 7.

Theorem 13.

$$t_i \geq d_s^i(C_{\max}, C) - 1,$$
$$r_{k+1-i} \leq n - d_s^i(C^{\perp s}, C_{\max}) + 1.$$

Proof. See [25]. □

Example 14. Consider the situation of Example 8. We have $d_s^1(C_{\max}, C) = d_s^2(C_{\max}, C) = 2$, and $d_s^1(C^{\perp s}, C_{\max}) = d_s^2(C^{\perp s}, C_{\max}) = 1$. Unlike the relative generalized Hamming weight, we do not have the strict monotonicity in i of d_s^i.

5 Translations to arbitrary finite fields and to the ordinary Hamming weight

5.1 Translation to arbitrary finite fields

Let $q = p^\mu$ with $\mu \geq 1$, and $\{\gamma_1, \ldots, \gamma_\mu\}$ be a fixed $\mathbf{F}_p$-basis of $\mathbf{F}_q$. Ashikhmin and Knill [2] proposed the following translation from $\mathbf{F}_q$ to $\mathbf{F}_p$ for quantum stabilizer codes. Let M be an $\mu \times \mu$ invertible matrix over $\mathbf{F}_p$ whose (i, j) element is $\mathrm{Tr}_{q/p}[\gamma_i \gamma_j]$, where $\mathrm{Tr}_{q/p}$ is the trace map from $\mathbf{F}_q$ to $\mathbf{F}_p$. Let ϕ be an $\mathbf{F}_p$-linear isomorphism from $\mathbf{F}_p^{2\mu n}$ to $\mathbf{F}_q^{2n}$ sending $(a_{1,1}, \ldots, a_{1,\mu}, a_{2,1}, \ldots, a_{n,\mu} | b_{1,1}, \ldots, b_{1,\mu}, b_{2,1}, \ldots, b_{n,\mu})$ to

$$\left(\sum_{j=1}^{\mu} a_{1,j}\gamma_j, \ldots, \sum_{j=1}^{\mu} a_{n,j}\gamma_j | \sum_{j=1}^{\mu} b'_{1,j}\gamma_j, \ldots, \sum_{j=1}^{\mu} b'_{n,j}\gamma_j \right),$$

where $(b'_{i,1}, \ldots, b'_{i,\mu}) = (b_{i,1}, \ldots, b_{i,\mu})M^{-1}$ for $i = 1, \ldots, n$.

Ashikhmin and Kinill proved the following.

Proposition 15. *[2] Let $C \subset \mathbf{F}_q^{2n}$. Then $\dim_{\mathbf{F}_p} \phi^{-1}(C) = \mu \dim_{\mathbf{F}_q} C$, and $\phi^{-1}(C)^{\perp s} = \phi^{-1}(C^{\perp s})$, where $\dim_{\mathbf{F}_q}$ is the dimension of a linear space considered over $\mathbf{F}_q$.*

Let $C \subset C_{\max} = C_{\max}^{\perp s} \subset C^{\perp s} \subset \mathbf{F}_q^{2n}$ with $\dim_{\mathbf{F}_q} C = n-k$. Then we have $\phi^{-1}(C) \subset \phi^{-1}(C_{\max}) = \phi^{-1}(C_{\max})^{\perp s} \subset \phi^{-1}(C)^{\perp s} \subset \mathbf{F}_p^{2\mu n}$ and we can construct a secret sharing scheme by $\phi^{-1}(C) \subset \phi^{-1}(C_{\max})$. It encodes $k\mu \log_2 p = k \log_2 q$ bits of classical secrets $\vec{m} \in \mathbf{F}_q^k$ into μn qudits in $\mathbf{C}_p$, which can also be seen as n qudits in $\mathbf{C}_q$, where $\mathbf{C}_q$ is the q-dimensional complex linear space. Let $A \subset \{1, \ldots, n\}$. By abuse of notation, by $\mathbf{F}_p^A$ we mean $\{(a_{1,1}, \ldots, a_{1,\mu}, a_{2,1}, \ldots, a_{n,\mu} | b_{1,1}, \ldots, b_{1,\mu}, b_{2,1}, \ldots, b_{n,\mu}) \in \mathbf{F}_p^{2\mu n} \mid a_{i,j} = b_{i,j} = 0$ for $i \notin A$ and $j = 1, \ldots, \mu\}$.

We consider each qudit in $\mathbf{C}_q$ of the quantum codeword as a share, and examine the property of a share set A. We have

$$\dim_{\mathbf{F}_q} C_{\max} \cap \mathbf{F}_q^A / C \cap \mathbf{F}_q^A = \mu \dim_{\mathbf{F}_p} \phi^{-1}(C_{\max}) \cap \mathbf{F}_p^A / \phi^{-1}(C) \cap \mathbf{F}_p^A. \tag{5}$$

Equation (5) together with Theorem 4 imply

- A is qualified if and only if $\dim_{\mathbf{F}_q} C_{\max} \cap \mathbf{F}_q^A / C \cap \mathbf{F}_q^A = \dim_{\mathbf{F}_q} C_{\max} / C$, and
- A is forbidden if and only if $\dim_{\mathbf{F}_q} C_{\max} \cap \mathbf{F}_q^A / C \cap \mathbf{F}_q^A = 0$.

The above observation shows that Theorems 4 and 7 also hold for $\mathbf{F}_q$. In addition, Eq. (5) means that a share set A has ($\log_2 q \times \dim_{\mathbf{F}_q} C_{\max} \cap \mathbf{F}_q^A / C \cap \mathbf{F}_q^A$)-bits of information about the secret $\vec{m} \in \mathbf{F}_q^k$, also generalizes the proof argument of Theorem 13, and implies that Theorem 13 also holds for $\mathbf{F}_q$. In the sequel we consider a qudit in $\mathbf{C}_q$ as each share, and dim means the dimension over $\mathbf{F}_q$.

5.2 Translation to the Hamming distance and the hermitian inner product

Many of results in the symplectic construction of quantum error-correcting codes over $\mathbf{F}_q$ are translated to $\mathbf{F}_{q^2}$-linear codes with the hermitian inner product [2,17,26]. For $\vec{x} \in \mathbf{F}_{q^2}^n$ define $\vec{x^q}$ as the component-wise q-th power of $\vec{x}$. For two vectors $\vec{x}, \vec{y} \in \mathbf{F}_{q^2}$, define the hermitian inner product as $\langle \vec{x}, \vec{y} \rangle_h = \langle \vec{x^q}, \vec{y} \rangle_E$. For $D \subset \mathbf{F}_{q^2}^n$, $D^{\perp h}$ denotes the orthogonal space of D with respect to the hermitian inner product.

Only in Sections 5.2 and 5.3, for $A \subset \{1,\ldots, n\}$, define $\mathbf{F}_q^A = \{(a_1, \ldots, a_n) \in \mathbf{F}_q^n \mid a_i = 0$ for $i \notin A\}$, and define P_A to be the projection map onto A, that is, $P_A(a_1, \ldots, a_n) = (a_i)_{i \in A}$.

Theorem 16. *Let $D \subset \mathbf{F}_{q^2}^n$ be an $\mathbf{F}_{q^2}$-linear space. We assume* $\dim D = k'$ *and there exists $D_{\max}$ such that $D \subset D_{\max} \subset D^{\perp h}$ and $D_{\max} = D_{\max}^{\perp h}$, which implies* $\dim D_{\max} = n/2$. *Then D defines a secret sharing scheme based on the quantum stabilizer defined by D encoding $n - 2k'$ symbols in $\mathbf{F}_q$. A set $A \subset \{1, \ldots, n\}$ is c-qualified if and only if* $\dim D_{\max}/D = \dim D_{\max} \cap \mathbf{F}_{q^2}^A / D \cap \mathbf{F}_{q^2}^A$. *A set $A \subset \{1, \ldots, n\}$ is c-forbidden if and only if* $0 = \dim D_{\max} \cap \mathbf{F}_{q^2}^A / D \cap \mathbf{F}_{q^2}^A$. *If $|A| \geq n - d_H(D^{\perp h}, D_{\max}) + 1$ then A is c-qualified, and if $|A| \leq d_H(D_{\max}, D) - 1$ then A is c-forbidden, where d_H is the coset distance [11], or equivalently, the first relative generalized Hamming weight [19].*

Proof. The proof is almost the same as [17]. □

5.3 Translation to the Hamming distance and the Euclidean inner product

Let $C_2 \subset C_1 \subset \mathbf{F}_q^n$. A method to construct C is to use $\{(\vec{a}|\vec{b}) \mid \vec{a} \in C_2, \vec{b} \in C_1^{\perp E}\}$ [6,17], where "$\perp E$" denotes the Euclidean dual. We have $C^{\perp s} = \{(\vec{a}|\vec{b}) \mid \vec{a} \in C_1, \vec{b} \in C_2^{\perp E}\}$.

Theorem 17. *Let $E \subset \mathbf{F}_q^n$ be the $\mathbf{F}_q$-linear space. We assume $\dim E = k'$ and there exists $E_{\max}$ such that $E \subset E_{\max} \subset E^{\perp E}$ and $E_{\max} = E_{\max}^{\perp E}$, which implies $\dim E_{\max} = n/2$. Then E defines a secret sharing scheme based on the quantum stabilizer defined by E encoding $n - 2k'$ symbols in $\mathbf{F}_q$. A set $A \subset \{1, \ldots, n\}$ is c-qualified if and only if $\dim E_{\max}/E = \dim E_{\max} \cap \mathbf{F}_q^A / E \cap \mathbf{F}_q^A$. A set $A \subset \{1, \ldots, n\}$ is c-forbidden if and only if $0 = \dim E_{\max} \cap \mathbf{F}_q^A / E \cap \mathbf{F}_q^A$. If $|A| \geq n - d_H(E^{\perp E}, E_{\max}) + 1$ then A is c-qualified, and if $|A| \leq d_H(E_{\max}, E) - 1$ then A is c-forbidden.*

Proof. The proof is almost the same as [17]. □

6 Gilbert-Varshamov-type existential condition

In this section, we give a sufficient condition for existence of $C \subset C_{\max} = C_{\max}^{\perp s} \subset C^{\perp s} \subset \mathbf{F}_q^{2n}$.

Theorem 18. *If positive integers n, k, δ_t, δ_r satisfy*

$$\frac{q^{n+k} - q^n}{q^{2n} - 1} \sum_{i=1}^{\delta_r - 1} \binom{n}{i} (q^2 - 1) + \frac{q^n - q^k}{q^{2n} - 1} \sum_{i=1}^{\delta_t - 1} \binom{n}{i} (q^2 - 1) < 1, \tag{6}$$

then there exist $C \subset C_{\max} = C_{\max}^{\perp s} \subset C^{\perp s} \subset \mathbf{F}_q^{2n}$ such that $\dim C = n - k$, $d_s(C^{\perp s}, C_{\max}) \geq \delta_r$ and $d_s(C_{\max}, C) \geq \delta_t$.

Proof. See [25]. □

We will derive an asymptotic form of Theorem 18.

Theorem 19. *Let R, ϵ_t and ϵ_r be nonnegative real numbers ≤ 1. Define $h_q(x) = -x \log_q x - (1 - x) \log_q (1 - x)$. For sufficiently large n, if*

$$h_q(\epsilon_t) + \epsilon_t \log_q (q^2 - 1) < 1, \tag{7}$$

$$h_q(\epsilon_r) + \epsilon_r \log_q (q^2 - 1) < 1 - R, \tag{8}$$

then there exist $C \subset C_{\max} \subset C^{\perp s} \subset \mathbf{F}_q^{2n}$ such that $\dim C = n - \lfloor nR \rfloor$, $d_s(C^{\perp s}, C_{\max}) \geq \lfloor n\epsilon_t \rfloor$ and $d_s(C_{\max}, C) \geq \lfloor n\epsilon_t \rfloor$.

Proof. Proof can be done by almost the same argument as [27, Section III.C]. □

Theorem 19 has a striking implication that we can construct a secret sharing scheme with a fraction $h_q^{-1}(1/\log_q(q^2 - 1))$ of participants being forbidden independently of the size (i.e. R in Theorem 19) of classical secrets for large n. For the smallest $q = 2$, $h_q^{-1}(1/\log_q(q^2 - 1))$ is close to 0.19, and we can make roughly 19% of participants forbidden. Such properties cannot be realized by classical shares.

Acknowledgment

The research problem was formulated in a discussion with Diego Ruano during the author's stay at the University of Valladolid, Spain. Without the discussion with him, this paper would not exist. This research was partly supported by JSPS Grant No. 17K06419.

References

1. Aschbacher, M.: Finite Group Theory, Cambridge Studies in Advanced Mathematics, vol. 10. Cambridge University Press, Cambridge, UK, 2nd edn. (2000)
2. Ashikhmin, A., Knill, E.: Nonbinary quantum stabilizer codes. IEEE Trans. Inform. Theory **47**(7), 3065–3072 (Nov 2001)
3. Bains, T.: Generalized Hamming weights and their applications to secret sharing schemes, master thesis, University of Amsterdam (2008) (supervised by R. Cramer, G. van der Geer, and R. de Haan).
4. Calderbank, A.R., Rains, E.M., Shor, P.W., Sloane, N.J.A.: Quantum error correction and orthogonal geometry. Phys. Rev. Lett. **78**(3), 405–408 (Jan 1997)
5. Calderbank, A.R., Shor, P.W.: Good quantum error-correcting codes exist. Phys. Rev. A **54**(2), 1098–1105 (Aug 1996)
6. Calderbank, A.R., Rains, E.M., Shor, P.W., Sloane, N.J.A.: Quantum error correction via codes over GF(4). IEEE Trans. Inform. Theory **44**(4), 1369–1387 (Jul 1998)
7. Chen, H., Cramer, R., Goldwasser, S., de Haan, R., Vaikuntanathan, V.: Secure computation from random error correccting codes. In: Advances in Cryptology–EUROCRYPT 2007. Lecture Notes in Computer Science, vol. 4515, pp. 291–310. Springer-Verlag (2007). https://doi.org/10.1007/978-3-540-72540-4_17
8. Cleve, R., Gottesman, D., Lo, H.K.: How to share a quantum secret. Phys. Rev. Lett. **83**(3), 648–651 (Jul 1999). https://doi.org/10.1103/PhysRevLett.83.648
9. Cover, T.M., Thomas, J.A.: Elements of Information Theory. Wiley Interscience, 2nd edn. (2006)
10. dela Cruz, R., Meyer, A., Solé, P.: Extension of Massey scheme for secret sharing, Proc. ITW 2010, Dublin, Ireland (2010). https://doi.org/10.1109/CIG.2010.5592719
11. Duursma, I.M., Park, S.: Coset bounds for algebraic geometric codes. Finite Fields Appl. **16**(1), 36–55 (Jan 2010). https://doi.org/10.1016/j.ffa.2009.11.006
12. Geil, O., Martin, S., Matsumoto, R., Ruano, D., Luo, Y.: Relative generalized Hamming weights of one-point algebraic geometric codes. IEEE Trans. Inform. Theory **60**(10), 5938–5949 (Oct 2014). https://doi.org/10.1109/TIT.2014.2345375
13. Gottesman, D.: Class of quantum error-correcting codes saturating the quantum Hamming bound. Phys. Rev. A **54**(3), 1862–1868 (Sep 1996)
14. Gottesman, D.: Theory of quantum secret sharing. Phys. Rev. A **61**(4), 042311 (Mar 2000). https://doi.org/10.1103/PhysRevA.61.042311
15. Hillery, M., Bužek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**, 1829–1834 (Mar 1999). https://doi.org/10.1103/PhysRevA.59.1829
16. Karlsson, A., Koashi, M., Imoto, N.: Quantum entanglement for secret sharing and secret splitting. Phys. Rev. A **59**, 162–168 (Jan 1999).
17. Ketkar, A., Klappenecker, A., Kumar, S., Sarvepalli, P.K.: Nonbainary stabilizer codes over finite fields. IEEE Trans. Inform. Theory **52**(11), 4892–4924 (Nov 2006)
18. Kurihara, J., Uyematsu, T., Matsumoto, R.: Secret sharing schemes based on linear codes can be precisely characterized by the relative generalized Hamming weight. IEICE Trans. Fundamentals **E95-A**(11), 2067–2075 (Nov 2012). https://doi.org/10.1587/transfun.E95.A.2067

19. Luo, Y., Mitrpant, C., Han Vinck, A.J., Chen, K.: Some new characters on the wire-tap channel of type II. IEEE Trans. Inform. Theory **51**(3), 1222–1229 (Mar 2005). https://doi.org/10.1109/TIT.2004.842763
20. Martínez-Peñas, U.: On the similarities between generalized rank and Hamming weights and their applications to network coding. IEEE Trans. Inform. Theory, **62**(7), 4081–4095 (July 2016).
21. Matsumoto, R.: Quantum stabilizer codes can realize access structures impossible by classical secret sharing. IEICE Trans. Fundamentals **E100-A**(12), 2738–2739 (Dec 2017)
22. Matsumoto, R.: Unitary reconstruction of secret for stabilizer based quantum secret sharing. Quant. Inf. Process. **16**(8), 202 (Aug 2017)
23. Matsumoto, R.: Coding theoretic construction of quantum ramp secret sharing. IEICE Trans. Fundamentals **E101-A**(8), 1215–1222 (Aug 2018). https://doi.org/10.1587/transfun.E101.A.1215
24. Matsumoto, R.: Exploring quantum supremacy in access structures of secret sharing by coding theory. In: Proc. 2018 ISITA. pp. 331–333. Singapore (Oct 2018), arXiv:1803.10392
25. Matsumoto, R.: Classical Access Structures of Ramp Secret Sharing Based on Quantum Stabilizer Codes (2018), arXiv:1811.05217
26. Matsumoto, R., Uyematsu, T.: Constructing quantum error-correcting codes for p^m-state systems from classical error-correcting codes. IEICE Trans. Fundamentals **E83-A**(10), 1878–1883 (Oct 2000)
27. Matsumoto, R., Uyematsu, T.: Lower bound for the quantum capacity of a discrete memoryless quantum channel. Journal of Mathematical Physics **43**(9), 4391–4403 (Sep 2002). https://doi.org/10.1063/1.1497999
28. McEliece, R.J., Sarwate, D.V.: On sharing secrets and Reed-Solomon codes. Comm. ACM **24**(9), 583–584 (Sep 1981). https://doi.org/10.1145/358746.358762
29. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge, UK (2000)
30. Ogawa, T., Sasaki, A., Iwamoto, M., Yamamoto, H.: Quantum secret sharing schemes and reversibility of quantum operations. Phys. Rev. A **72**(3), 032318 (Sep 2005). https://doi.org/10.1103/PhysRevA.72.032318
31. Pless, V.S., Huffman, W.C., Brualdi, R.A.: An introduction to algebraic codes. In: Pless, V.S., Huffman, W.C. (eds.) Handbook of Coding Theory, pp. 3–139. Elsevier, Amsterdam (1998)
32. Shamir, A.: How to share a secret. Comm. ACM **22**(11), 612–613 (Nov 1979). https://doi.org/10.1145/359168.359176
33. Smith, A.D.: Quantum secret sharing for general access structures (Jan 2000), arXiv:quant-ph/0001087
34. Steane, A.M.: Multiple particle interference and quantum error correction. Proc. Roy. Soc. London Ser. A **452**(1954), 2551–2577 (Nov 1996)
35. Stinson, D.R.: Cryptography Theory and Practice. Chapman & Hall/CRC, 3rd edn. (2006)