Quantum secret sharing and tripartite information

Guangkuo Liu*, Peixue Wu†, Haneul Kim‡, and Marius Junge†

*JILA, NIST, and Department of Physics, University of Colorado, 440 UCB, Boulder, Colorado 80309, USA
†Department of Mathematics, University of Illinois at Urbana-Champaign, Urbana, Illinois, 61801, USA
‡Department of Electrical and Computer Engineering, University of Illinois at Urbana-Champaign, Urbana, IL 61801, USA

Abstract—We develop a connection between tripartite information $I_3$, quantum secret sharing protocols and multi-unitaries. This leads to a general framework of constructing ((2,3)) threshold schemes in arbitrary dimension. As an application, we propose a class of random codes generated by Haar-distributed random unitaries, in which all states have bounded tripartite entanglement with high probability. Moreover, using the $I_3$ criteria for imperfect sharing schemes, we discover examples of VIP secret sharing schemes.

I. INTRODUCTION

Quantum tripartite information, first introduced as “topological entropy” in [1] to characterize multi-party entanglement in a topologically ordered system, refers to the study of quantum information when it is shared among three or more parties. This area of research is concerned with understanding how quantum information behaves when it is shared among multiple parties and how it can be manipulated and processed in a tripartite quantum system. The study of quantum tripartite information is important for the development of quantum technologies such as quantum communication, quantum cryptography, and quantum computing. We refer the readers to [2], [3] and the references therein for a fruitful connection to tensor networks. Moreover, tripartite information can be used to measure delocalization of information in the bulk-boundary picture of the AdS/CFT correspondence, see e.g. [4].

In this paper we will develop a connection between tripartite information $I_3$ and quantum secret sharing protocols. Tripartite information is defined for any tripartite state $\rho \in P_1P_2P_3$ (we will abuse the notation by writing $\rho \in P_1P_2P_3$ for simplicity) by

$$ I_3(P_1 : P_2 : P_3) = I(R, P_1) + I(R, P_2) - I(R, P_1P_2) $$

as it is the case for conditional entropy, $I_3$ may have positive and negative values. A negative value is an indication of existing entanglement. In [4] it is shown that under the premise of the famous Hayden-Preskill-Gedanken experiment $I_3$ is always strictly negative.

In quantum information theory the equality case in entropic inequalities often occurs under specific algebraic requirements. Therefore it is natural to ask for equality in the obvious lower bound

$$ -2S(R) \leq I_3(P_1 : P_2 : P_3). $$

Note that the bound follows easily from the positivity of mutual information, see e.g. [6]. As pointed out by [5], see also [7], random unitaries and perfect tensor almost achieve equality of (1.2) in many cases. This leads to an interpretation of scrambling in terms of error correction and decoding, closely connected to the powerful tool of decoupling [8].

Motivated by previous work, we observe that there is a one-to-one correspondence between minimality of $I_3$ and the ((2,3)) quantum secret sharing scheme. In this paper a quantum secret sharing scheme is defined as a code space, i.e., a subspace $C$ of $P_1P_2P_3$.

Throughout the paper, we assume that $P_1, P_2, P_3$ are $d$-dimensional Hilbert spaces, and each $P_\alpha$, $\alpha = 1,2,3$ is spanned by $\{|i\}_P^\alpha$ for $0 \leq i < d$. Moreover, the quantum secret sharing scheme $C \subseteq P_1P_2P_3$ has the same dimension as each party. Therefore, we can assume that $C$ is spanned by the following vectors which form an orthonormal basis for $C$:

$$ \tilde{|i\rangle} = \frac{1}{\sqrt{d}} \sum_{s_1,s_2,s_3=0}^{d-1} \tilde{t}_{i,s_1,s_2,s_3} |s_1s_2s_3\rangle P_1P_2P_3, i = 0,1,\cdots,d-1. $$

Here the four-leg tensor coefficients $t_{i,s_1,s_2}$ satisfy

$$ \sum_{s_1,s_2,s_3} \tilde{t}_{i,s_1,s_2,s_3} t_{j,s_1,s_2,s_3} = d \delta_{ij}, $$

so that $\{|\tilde{i}\rangle\}_{0 \leq i \leq d-1}$ is an orthonormal basis for $C$. It is direct to check that if the four-leg tensor matrix $\sum_{i,s_1,s_2} t_{i,s_1,s_2} |s_2s_3\rangle \langle s_1|$ is a $d^2 \times d^2$ unitary matrix, then (I.4) holds.

Quantum secret sharing has been a long-established topic in quantum information theory [9]. It has a variety of applications such as quantum money and quantum resource distribution. The key property of quantum secret sharing is that if the referee sends a state on the code space, only authorized subsets of the parties can reconstruct the secret perfectly while...
those that are unauthorized gain zero information. By ((2, 3)) quantum secret sharing scheme, or ((2, 3)) threshold scheme, it means any two parties can recover the state perfectly, and any single party gains zero information, i.e., $\rho^{P_i}$ is a maximally mixed state for any $a = 1, 2, 3$ where $\rho$ is a state on the code space.

Our observation can be summarized as the following theorem:

**Theorem I.1.** The following statements are equivalent:

1. The code space $\mathcal{C}$ spanned by (I.3) is a ((2, 3)) quantum secret sharing scheme.
2. For any state $\rho$ on the code space $\mathcal{C}$, the equality holds in (I.2). In other word, any state on the code space has minimal tripartite information.
3. The four-leg tensor matrix $\sum_{i_1j_1i_2j_2} t_{i_1j_1i_2j_2}|s_{i_1}s_{j_1}\rangle|s_{i_2}s_{j_2}\rangle$ is a $d^2 \times d^2$ multi-unitary.

The multi-unitary condition is that we have that $t := \sum_{i_1j_1i_2j_2} t_{i_1j_1i_2j_2}|s_{i_1}s_{j_1}\rangle|s_{i_2}s_{j_2}\rangle$ becomes a unitary for all three choices $a = 1, 2, 3$. We refer to next section for details and [10] for more discussions.

Using the predicted relation between sharing schemes and $I_3$, one can also produce new examples with small, but not necessarily minimal values of $I_3$, as in Page scrambling. Indeed, for a unitary $U = \sum_{i_1j_1i_2j_2} u_{i_1j_1i_2j_2}|i_1s_{j_1}\rangle|s_{i_2}s_{j_2}\rangle$ and we may define the tensor $t_{i_1j_1i_2j_2} = u_{i_1j_1i_2j_2}$ and then estimate tripartite information:

**Theorem I.2.** Let $u = \sum_{i_1j_1i_2j_2} u_{i_1j_1i_2j_2}|i_1s_{j_1}\rangle|s_{i_2}s_{j_2}\rangle$ be a Haar-distributed $d^2 \times d^2$ random unitary. Define the tensor $t_{i_1j_1i_2j_2} = u_{i_1j_1i_2j_2}$. Then with probability $1 - \delta$,

$$-2S(R) \leq I_3(P_1P_2P_3) \leq -2S(R) + C(\delta)$$

holds for all states on the code space given by (I.3), where $C(\delta) > 0$ is a dimension-free universal constant only depending on $\delta$.

Previous results were usually restricted to a maximally entangled state $|\psi\rangle$ and did not provide good enough concentration of measure to work for all densities simultaneously, see [11]. The above estimate, however, provides a concrete dimension-free relation which works for all states in the code space.

The paper is organized as follows. After some preliminaries, the equivalence of the three conditions, i.e., Theorem I.1 is presented in Section II. In Section III, we derive estimates of $I_3$ in terms of the norm of the four-leg tensor matrix $t_{i_1j_1i_2j_2}$ and some probabilistic estimates via random matrix techniques. The last section provides concrete examples of perfect secret sharing schemes that work for all dimension, and also an example of imperfect secret sharing schemes that always requires a fixed party to be present to recover a secret.

## II. Equivalence Conditions for Perfect Secret Sharing Schemes

This section dedicates to prove Theorem I.1. Let us first formally define what it means for two parties to recover the information. For example, if $P_1, P_2$ are authorized parties to recover the information of the code space spanned by (I.3), then there exists a unitary $U^{12}$ only acting on $P_1P_2$, such that

$$\rho^{P_i} \otimes |\chi\rangle^{P_3P_5}$$

for any $i = 0, 1, \ldots, d-1$ and $|\chi\rangle^{P_3P_5}$ is a pure state which is independent of $i$. It was shown in [12, Section 3.2] that (II.1) is possible if and only if $I(R, P_3) = 0$ for the maximally entangled state $|\phi\rangle = \frac{1}{\sqrt{d}} \sum_i |i\rangle^{R}\otimes|\tilde{i}\rangle$.

In the procedure of quantum secret sharing, after decoding, the secret is sent to the referee. Thus it is convenient to assume the unitary $U^{12} : P_1 \otimes P_2 \rightarrow R \otimes P_3$ since $|R\rangle = |P_a\rangle = d, a = 1, 2, 3$. We will denote $P''_a$ as a copy of the original space. Our formal definition of ((2, 3)) quantum secret sharing scheme is given as follows:

**Definition II.1.** Suppose the code space $\mathcal{C} \subset P_1P_2P_3$ is spanned by (I.3). We say $\mathcal{C}$ is a ((2, 3)) quantum secret sharing scheme, if for any $a = 1, 2, 3$ there exists a unitary $U_a : RP'_a \rightarrow P_bP_c$, where $a, b, c$ are different and a pure state $|\chi_a\rangle^{P_bP_c}$, such that for any $i = 0, 1, \ldots, d-1$,

$$|\tilde{i}\rangle = (U_a \otimes id^{P'_a})|i\rangle^{R}\otimes|\chi_a\rangle^{P_bP_c}.$$ (II.2)

A direct consequence of the definition is that any state on the code space has minimal $I_3$ and the reduced density for any single party must be maximally mixed:

**Proposition II.1.** Let $C$ be a ((2, 3)) threshold scheme. Then for any state $\rho$ on the code space, its reduced densities for any party must be maximally mixed. Furthermore, we have

$I_3(P_1 : P_2 : P_3) = -2S(R)$.

Proof. Suppose $\rho = \sum_{ij} \rho_{ij} |i\rangle \langle j|$. Let $P_a$ denote any party, and $P_b, P_c$ the remaining parties. By definition, for some unitary $U_a : RP'_a \rightarrow P_bP_c$

$$\rho^{P_aP_bP_c} = U_a \otimes id^{P'_a} \left( \sum_{ij} \rho_{ij} |i\rangle \langle j| \otimes |\chi_a\rangle^{P_bP_c} \right) U_a^\dagger \otimes id^{P'_a}.$$
If we take the partial trace over $P_b$ and $P_c$, we get
\[ \tilde{\rho}^{P_a} = \text{Tr}_{P_bP_c}(\rho^{P_aP_bP_c}) = \text{Tr}_{P_a}(|\chi_a\rangle\langle \chi_a|^{P_aP_b}), \] (II.3)
which is independent of the choice of $\tilde{\rho}$. If we take partial trace over $P_a$, we get
\[ \tilde{\rho}^{P_aP_c} = \text{Tr}_{P_a} (\tilde{\rho}^{P_aP_bP_c}) = U_a \left( \sum_{ij} \rho_{ij} |i\rangle \langle j| \otimes \text{Tr}_{P_a} (|\chi_a\rangle \langle \chi_a|^{P_aP_b}) \right) U_a^†. \]

Since von Neumann entropy is invariant under unitary, we have
\[ S(P_bP_c) = S \left( \sum_{ij} \rho_{ij} |i\rangle \langle j| \right) + S \left( \text{Tr}_{P_a} (|\chi_a\rangle \langle \chi_a|^{P_aP_b}) \right) = S(R) + S(P_a). \]

Substituting this into the expression of $I_3$, we get $I_3 = -2S(R)$. To see why $\tilde{\rho}^{P_a}$ must be maximally mixed, it is sufficient to show the case $\tilde{\rho}^{P_aP_bP_c} = \sum_{ij} \frac{1}{d} |i\rangle \langle j| \otimes \text{Tr}_{P_a} (|\chi_a\rangle \langle \chi_a|^{P_aP_b})$, since the reduced density is independent of the choice of $\tilde{\rho}^{P_aP_bP_c}$. For this state, $I_3(P_1 : P_2 : P_3) = -2S(R) = -2\log d$. From the fact that $I_3$ is symmetric with respect to the choice of parties, we have
\[ I_3(P_1 : P_2 : P_3) = I_3(R : P_b : P_c) = -2S(P_a) + I(P_a, R) + I(P_a, P_b) + I(P_a, P_c), \]
for any party $P_a$, where $|\phi\rangle_a$ is the purification of $\tilde{\rho}$. Therefore, $-2\log d = I_3 \geq -2S(P_a)$ thus $S(P_a) \geq \log d$, which is possible only when $\tilde{\rho}^{P_a}$ is maximally mixed. \(\square\)

Conversely, if for any state $\tilde{\rho}$ on the code space, we have $I_3(P_1 : P_2 : P_3) = -2S(R)\tilde{\rho}$, then we have $I(R, P_a) = 0$ for any party $P_a$ by (I.1). In particular, we take the pure state $|\phi\rangle_a = 1/d \sum_i |i\rangle \langle i| P_a \tilde{\rho}^{P_a}$, then using the same argument as in [11, Section 3.2], there exist a unitary $U_a : RP_a^P \mapsto P_bP_c$ and a pure state $|\chi_a\rangle^{P_aP_b}$, such that for any $t = 0, 1, \ldots, d-1$, \[ |\tilde{i}\rangle = (U_a \otimes \text{id}^{P_c}) |i\rangle |\chi_a\rangle^{P_aP_b}. \]

Therefore, the code space is a $(2,3)$ secret sharing scheme.

To finish the proof of Theorem 1.1, we need to connect the multi-unitary part. The following proposition will conclude the proof of the theorem:

**Proposition II.2.** $C$ is a $(2,3)$ secret sharing scheme if and only if $t_{i_1s_1s_3}$ is multi-unitary [10]:

1. the map $t := \sum_{i_1s_1s_3} t_{i_1s_1s_3}s_2s_3|is_1\rangle$ is unitary,
2. its reshuffling, $t^{R} := \sum_{i_1s_1s_2s_3} t_{i_1s_1s_2s_3}s_1s_3|is_2\rangle$ is unitary, and
3. its partial transposition (followed by a flip), $t^{R} := \sum_{i_1s_1s_2s_3} t_{i_1s_1s_2s_3}s_1s_2|is_3\rangle$ is unitary.

**Proof.** Suppose $t_{i_1s_1s_3}$ is multi-unitary, then it is easy to see that $C$ is a $(2,3)$ threshold scheme since the recovery unitary can be constructed directly by
\[ U_1 = \sum_{i_1s_1s_3} t_{i_1s_1s_3}s_2s_3|is_1\rangle |RP^{P}\rangle, \]
\[ U_2 = \sum_{i_1s_1s_3} t_{i_1s_1s_3}s_1s_3|is_2\rangle |RP^{P}\rangle, \]
\[ U_3 = \sum_{i_1s_1s_3} t_{i_1s_1s_3}s_1s_2|is_3\rangle |RP^{P}\rangle. \]

The corresponding pure state $|\chi\rangle^{P_aP_bP_c}$ is given by the maximally entangled state. We can directly check that (II.2) holds.

To show that $t_{i_1s_1s_3}$ is multi-unitary if $C$ is a $(2,3)$ secret sharing scheme, recall $|\chi_a\rangle^{P_aP_bP_c}$ is a purification of maximally mixed state, see (II.3), then there exists a local unitary $U^{P_a}$, such that
\[ |\chi_a\rangle^{P_aP_bP_c} = \text{id}^{P_a} \otimes U^{P_a} \left( \sum_s \frac{1}{\sqrt{d}} |s\rangle^{P_a} |s\rangle^{P_b} \right). \]

By incorporating the local unitary into $U_a : RP^a \mapsto P_bP_c$, we have
\[ |\tilde{i}\rangle = \left( (U_a \otimes \text{id}^{P_c}) |i\rangle \right) \left( \sum_s \frac{1}{\sqrt{d}} |s\rangle^{P_a} |s\rangle^{P_b} \right). \]

We may drop the tilde over $U_a$ for notational simplicity. By substituting the element of $U_1$ into (II.4), we get a tensor representation of the basis:
\[ |\tilde{i}\rangle = \sum_{s_1s_2s_3} \frac{1}{d} t_{i_1s_1s_3}s_1s_2s_3 |P^aP_bP_c. \]

\[ \sum_{t_{i_1s_1s_3}} t_{i_1s_1s_3}s_2s_3 |is_1\rangle |RP^{P}\rangle, \]
\[ \sum_{t_{i_1s_1s_3}} t_{i_1s_1s_3}s_1s_3 |is_2\rangle |RP^{P}\rangle, \]
\[ \sum_{t_{i_1s_1s_3}} t_{i_1s_1s_3}s_1s_2 |is_3\rangle |RP^{P}\rangle. \]

So one must have $t_{i_1s_1s_3} = |g_{j_1k_1l_1}| \delta_{s_1s_2}$. This is same as saying the maps:
\[ g := \sum_{j_1k_1l_1} |g_{j_1k_1l_1}| |j_1k_1l_1| \]
\[ t^{R} := \sum_{i_1s_1s_3} t_{i_1s_1s_3}s_1s_3 |is_2\rangle |\]

satisfy $g^{t^{R}} = \text{id}$. Since $g$ is a unitary, we have that $g = t^{R}$. So the reshuffling $t^{R}$ must also be unitary, i.e. the condition 2 of multi-unitary is satisfied. In addition, we have
\[ U_2 = \sum_{i_1s_1s_3} t_{i_1s_1s_3}s_1s_3 |P^aP_bP_c. \]
By repeating the same procedure for $U_3$ we can see that the partial transpose $T^r := \sum_{i,s_1,s_2,s_3} t_{i,s_1,s_2,s_3} |s_1 s_2 s_3\rangle\langle s_3| s_3$ must also be unitary and it gives the coefficient expression of $U_3$:

$$U_3 = \sum_{i,s_1,s_2,s_3} t_{i,s_1,s_2,s_3} |s_1 s_2 s_3\rangle\langle s_3| s_3^{R^t}.$$  

$\square$

III. Random estimates

In this section, we investigate code subspace which almost achieves secret sharing. Our principle is to give an upper bound of $I_3$ so that it is not far from its minumum. As usual we start with a code space $C \subseteq P_1 P_2 P_3$ and a fixed orthonormal basis

$$|\tilde{i}\rangle = \sum_{s_1,s_2,s_3} \frac{1}{\sqrt{d}} |s_1 s_2 s_3\rangle.$$  

different from previous sections,

$$\sum_{i,s_1,s_2,s_3} t_{i,s_1,s_2,s_3} |s_1 s_2 s_3\rangle P_i P_j \langle s_3| s_3^{R^t}$$

does not need to be multi-unitary. We can still define the linear maps

$$T_1 : R^r P^t_1 \rightarrow P_2 P_3 := \sum_{i,s_1,s_2,s_3} t_{i,s_1,s_2,s_3} |s_1 s_2 s_3\rangle P_i P_j \langle s_3| s_3^{R^t},$$

$$T_2 : R^r P^t_2 \rightarrow P_1 P_3 := \sum_{i,s_1,s_2,s_3} t_{i,s_1,s_2,s_3} |s_1 s_2 s_3\rangle P_i P_j \langle s_3| s_3^{R^t},$$

and

$$T_3 : R^r P^t_3 \rightarrow P_1 P_2 := \sum_{i,s_1,s_2,s_3} t_{i,s_1,s_2,s_3} |s_1 s_2 s_3\rangle P_i P_j \langle s_3| s_3^{R^t},$$

where $R^r, P^t_i$ are copies of $R, P_i$. For linear maps $T$, $\|T\|$ denotes its operator norm in this paper.

**Lemma III.1.** For all $\rho P^t_1 P^t_2$ on the code space,

$$D(\rho R^t \otimes \rho P^t_1) \leq 2 \log \|T_1\|.$$  

**Proof.** By definition of the code space, we have

$$|\tilde{i}\rangle P_i P_j P_k = (id P_i \otimes T_1) \sum_{s_1} \frac{1}{\sqrt{d}} |s_1\rangle |s_1 s_2 s_3\rangle P_i P_j P_k.$$  

Let $\rho = \sum_i \lambda_i |\psi_i\rangle \langle \psi_i| P_i P_j P_k$ be the spectral decomposition, then by superposition,

$$|\psi_i\rangle P_i P_j P_k = (id P_i \otimes T_1) \sum_{s_1} \frac{1}{\sqrt{d}} |s_1\rangle |s_1 s_2 s_3\rangle P_i P_j P_k.$$  

So the purification satisfies

$$|\phi\rangle^{RP_1 P_2 P_3} := \sum_i \sqrt{\lambda_i} |\psi_i\rangle R |\psi_i\rangle P_i P_j P_k$$

$$= id P_i \otimes T_1 \left( \sum_{i,s} \sqrt{\lambda_i/d} |s_1\rangle |s_1 s_2 s_3\rangle P_i P_j \otimes |\psi_i\rangle R |s_1\rangle P_i \right)$$

Denote $|\chi\rangle$ as the vector on the right hand side before applying $id P_i \otimes T_1$. Then we get

$$\rho^{RP_1} = Tr_{P_2 P_3}(|\phi\rangle \langle \phi|)$$

$$= Tr_{P_2 P_3} ((id P_i \otimes T_1) |\chi\rangle \langle |id P_i \otimes T_1|^\dagger)$$

$$\leq \|T_1\|^2 Tr_{P_i} \langle \chi| \langle \chi\rangle$$

$$= \|T_1\|^2 \sum_i \lambda_i |\psi_i\rangle \langle \psi_i| \otimes id \frac{d}{d}.$$  

Recall that (see [61]) for any two states $\rho, \sigma$

$$D(\rho||\sigma) \leq D_\infty(\rho||\sigma) = \inf \{\lambda | \rho \leq 2^\lambda \sigma\},$$

and

$$D(\rho^{RP_1} || \rho \otimes P^t_1) \leq D(\rho^{RP_1} || \rho \otimes id \frac{d}{d})$$

In particular,

$$D(\rho^{RP_1} || \rho \otimes P^t_1) \leq \log \|T_1\|^2.$$  

The assertion follows.  

**Corollary III.2.** Let $C \subseteq P_1 P_2 P_3$ be a coding subspace and $t$ be the tensor as above. Then

$$-2S(R) \leq I_3(P_1 : P_2 : P_3) \leq -2S(R) + 2 \log \|T_1\| + 2 \log \|T_2\| + 2 \log \|T_3\|,$$

for any state $\rho$ on the code space.

**Proof.** We have seen above that

$$I_3(R : P_1 : P_2) \leq -2S(R) + I(R, P_1) + I(R, P_2) + I(R, P_3).$$

Therefore applying Lemma III.1 three times, we get the assertion.  

With all the preparations, we are able to propose a class of random codes which deliver bounded $I_3$ estimates for all states. Assume the underlying Hilbert space $H = R P_1$ with dimension $n = d^2$. Our random code is given by Haar-distributed random unitary $u$ on $H$:

Let $u : RP^t_1 \rightarrow P_2 P_3$ be a Haar-distributed random unitary, and

$$|\tilde{i}\rangle = \frac{1}{\sqrt{d}} \sum_{s_1,s_2,s_3} u_{i,s_1,s_2,s_3} |s_1 s_2 s_3\rangle.$$  

Then we can show the following explicit estimate:

**Theorem III.3.** Suppose $\delta \in (0, 1/2)$ is given. Then with probability $1 - \delta$, the estimate

$$I_3(P_1 : P_2 : P_3) \leq -2S(R) + 36 + 3 \log \log \frac{1}{\delta}$$

holds for all states on the code space.

In order to prove the above theorem, the following technical result is enough. The main idea is to connect the estimates of semi-norms of random unitaries to estimates of semi-norms of complex random Gaussian matrices, which are easier to estimate. The trick is based on random matrix theory and essentially contained in [13]. We refer the reader to [14] for the complete details of the proof.
Proposition III.4. Suppose $\delta \in (0, 1/2)$ is given. Then with probability $1 - \delta$, we have

$$\max\{||u||, ||u^R||, ||u^T||\} \leq 64\sqrt{\log(1/\delta)}.$$  \hspace{1cm} (III.2)

Using Lemma III.1, the proof of the theorem is obvious because the estimates of the operator norm of the linear maps are given.

IV. EXAMPLES

A. A perfect secret sharing protocol for arbitrary dimension

We first characterize a permutation code space $C \subset P_1P_2P_3$ by fixing its basis to be

$$\langle e \rangle^{P_1P_2P_3} = \frac{1}{\sqrt{d}} \sum_{s=1}^{d} |\sigma^i_a(s)\rangle P^i_1|\sigma^i_b(s)\rangle P^i_2|\sigma^i_c(s)\rangle P^i_3,$$

where $\sigma^i_j$ denotes a permutation operator in $S_d$ for $j \in \{1, 2, 3\}$, and $\sigma^i_j$ denotes the composition of $\sigma^i_j$ for $i$ times. Note that this is a generalization of a well-known example in [9], [12], [15] of ((2,3)) threshold scheme given by

$$\langle 0 \rangle = \frac{1}{\sqrt{3}} (|000\rangle + |111\rangle + |222\rangle),$$

$$\langle 1 \rangle = \frac{1}{\sqrt{3}} (|012\rangle + |120\rangle + |201\rangle),$$

$$\langle 2 \rangle = \frac{1}{\sqrt{3}} (|021\rangle + |102\rangle + |210\rangle).$$

Proposition IV.1. The code space $C$ is a ((2,3)) threshold scheme if and only if for any $a \neq b \in \{1, 2, 3\}$,

$$\sigma^i_a(s) \neq \sigma^i_b(s) \text{ for all } s \in \{1, \ldots, d\}, i \in \{1, \ldots, d-1\}.$$  \hspace{1cm} (IV.2)

Proof. Using the minimality of $I_3$ condition, we need to show that the condition (IV.2) is equivalent to $I_3 = -2S(R) = -2\log d$ for the state $\rho = \sum_{i} 1/d |i\rangle\langle i|$. It is easy to show that for any $a \in \{1, 2, 3\}$,

$$\rho^{P_a} = \frac{1}{d} \sum_{s} |s\rangle\langle s|^{P_a},$$

and therefore we have $S(P_a) = \log d$. Moreover, for any $a \neq b \in \{1, 2, 3\}$,

$$\rho^{P_aP_b} = \frac{1}{d} \sum_{s} |\sigma^i_a(s)\rangle\langle \sigma^i_b(s)|^{P_aP_b},$$

so $S(P_aP_b) \leq 2\log d$, with equality holds if and only if $\{|\sigma^i_a(s)\rangle\langle \sigma^i_b(s)|\}_{d=1}^{d}$ forms an orthonormal basis. Note that the orthonormality requirement is equivalent to the condition (IV.2). In addition,

$$I_3 = \sum_j S(P_j) - \sum_{a \neq b} S(P_aP_b) + S(R) \geq 3\log d - 3 \cdot 2 \log d + \log d = -2 \log d,$$

with equality obtained if and only if equality hold for $S(P_aP_b) \leq 2 \log d$. Thus condition (IV.2) is satisfied if and only if $C$ is a ((2,3)) threshold scheme.

Using a concrete set of permutations that satisfies (IV.2), we now provide a ready-to-use ((2,3)) threshold scheme. It should be noted that this protocol works for all dimensions $d$, which is an improvement over the existing examples of minimal $I_3$.

Example IV.2. Let $C \subset P_1P_2P_3$ be generated by

$$|\bar{i}\rangle = \frac{1}{\sqrt{d}} \sum_{s=1}^{d} |s\rangle P^i_1|s + k_1i\rangle P^i_2|s + k_2i\rangle P^i_3,$$

where $k_1 \neq k_2$, and both $k_1$ and $k_2$ are coprime with $d$. The additions are mod $d$.

It is not hard to verify that this is indeed a permutation code space in the form of (IV.1), and that it satisfies (IV.2). Therefore, the code space is a ((2,3)) threshold scheme.

B. An imperfect secret sharing protocol with a VIP party

We provide an secret sharing protocol such that after the referee send a secret to $P_1$, $P_2$ and $P_3$,

- $\{P_1, P_3\}$ or $\{P_2, P_3\}$ together can reconstruct the secret, but
- $\{P_1, P_2\}$ together cannot reconstruct the secret.

It is as if the party $P_3$ is a VIP, since in order to reconstruct the secret, party $P_3$ has to be present. However, $P_3$ is not too powerful because he alone still cannot decode the message. We define the code space $C \subset P_1P_2P_3$ by fixing the basis

$$|\bar{i}\rangle = \frac{1}{\sqrt{d}} \sum_{j,k,l=1}^{d} t_{ijkl} |jkl\rangle P^i_1P^i_2P^i_3,$$

where $t_{ijkl} := \frac{1}{\sqrt{d}} \delta_{\lambda k u_i|i}$,  \hspace{1cm} (IV.4)

where $\lambda_k$ is a shift operator and $u_i$ is a phase shift operator such that

$$\lambda_k : |j\rangle \mapsto |j + k\rangle, \quad u_i : |i\rangle \mapsto u^i |i\rangle,$$  \hspace{1cm} (IV.5)

where $w = e^{2\pi i/d}$. One can define the maps as usual,

$$t^{P_1P_2} := \sum_{i,j} t_{ijkl} |ikl\rangle P^i_1P^j_2,$$

$$t^{P_2P_3} := \sum_{i,j} t_{ijkl} |ikl\rangle P^j_2P^i_3,$$

$$t^{P_3P_1} := \sum_{i,j} t_{ijkl} |ikl\rangle P^i_3P^j_1,$$

We can verify that indeed $t^{P_1P_2}P^i_3$ and $t^{P_2P_3}P^i_1$ are unitaries but $t^{P_3P_1}P^i_2$ is not a unitary, thus giving the pairs $\{P_1, P_3\}$ and $\{P_2, P_3\}$ the ability to recover the secret, but not $\{P_1, P_2\}$.

We show the calculation for $t^{P_1P_2}P^i_3$ as an example:

$$t^{P_1P_2}P^i_3 := \left(t^{P_1P_2}\right)^\dagger_{i,j,k,l} \sum_{i,j} t_{ijkl} |ikl\rangle |k' l'\rangle,$$

where

$$\sum_{i,j} t_{ijkl} t_{ij'k'l'} := \frac{1}{d} \sum_{i,j} (|i\rangle u_i^\dagger |j\rangle t_{ijkl} |i\rangle |\lambda_k u_i|i\rangle = \frac{1}{d} \text{Tr}\left(u_i^\dagger u_i\right) \delta_{\lambda k u_i|i} = \delta u_i \delta_{\lambda k u_i|i},$$

Authorized licensed use limited to the terms of the applicable license agreement with IEEE. Restrictions apply.
One can also verify that $\sum_{i, t} t_{ij} k_{il} t_{ij}^{*} k_{il}^{*} = \delta_{ji} \delta_{ll'}$. Thus the maps $t^{R} P_{1} \rightarrow P_{2} P_{3}$ and $t^{R} P_{2} \rightarrow P_{1} P_{3}$ are unitary. But we have $\sum_{i, t} t_{ij} k_{il} k_{il'} = \delta_{ii'} \delta_{ll'}$, so the map $t^{R} P_{1} \rightarrow P_{2} P_{3}$ is not unitary.

From Theorem I.1, if there were a decoding scheme for $\{P_{1}, P_{2}\}$, the error-correcting unitary must be uniquely defined to be equal to $t^{R} P_{1} \rightarrow P_{1} P_{2}$. But here we do not have the unitarity, so there is no decoding scheme for parties $\{P_{1}, P_{2}\}$.

Moreover, we must note that this is not the trivial case where all the secret is contained in $P_{3}$. It can be shown that
$$\|t^{R} P_{2} \rightarrow P_{1} P_{2}\|^{2} = d.$$

Thus from Lemma III.1, $I(R, P_{3}) \leq \log d$ for any $\tilde{\rho}$ on the code space. So at least we can show for the maximally mixed state $\sum_{i} |i\rangle\langle i|/d$,
$$I(R, P_{3}) \leq \log d < 2 \log d = I(R, P_{1} P_{2} P_{3}),$$
which implies that party $P_{3}$ alone cannot recover the secret.

Moreover, we have
$$-2S(R) \leq I_{3}(\tilde{\rho}) \leq -2S(R) + \log d,$$
for any $\tilde{\rho} \in C$. (IV.6)

Interestingly, we see that $I_{3}$ remains non-positive for both the pure state ($I_{3} = 0$) and the maximally mixed state ($I_{3} = -\log d$). Our conjecture is that $I_{3} \leq 0$ holds for all $\tilde{\rho} \in C$. This property is called monogamy and has significant implications in the context of holography and AdS/CFT correspondence [16].

V. CONCLUSION

In summary, our note develops a connection between tripartite information $I_{3}$ and secret sharing protocols. In particular, we observed that the sharing protocol is perfect if and only if the tripartite information is minimal for all states in the secret sharing protocol. Moreover, we showed that perfect secret sharing protocol is also equivalent to the fact that the recovery unitaries are multi-unitary.

Based on the connection of tripartite information and perfect secret sharing protocol, we find imperfect sharing schemes with bounded tripartite information and VIP models with preference to one to three parties.

VI. ACKNOWLEDGMENTS

MJ was supported by NSF Grant DMS 2247114, NSF Grant DMS 1800872 and NSF RAISE-TAQS 1839177. The authors thank the referee for helpful suggestions. MJ is the corresponding author: mjunge@illinois.edu.

REFERENCES

[1] Alexei Kitaev and John Preskill. Topological entanglement entropy. Phys. Rev. Lett., 96:110404, Mar 2006.
[2] Sepehr Nezami and Michael Walter. Multipartite entanglement in stabilizer tensor networks. Phys. Rev. Lett., 125:241602, Dec 2020.
[3] Oskar Schnacl, Niklas Böltner, Sebastian Paechel, Salvatore R. Mannina, Stefan Kehrein, and Markus Schmitt. Tripartite information, scrambling, and the role of hilbert space partitioning in quantum lattice models. Physical Review B, 100(22), Dec 2019.
[4] Patrick Hayden, Sepehr Nezami, Xiao-Liang Qi, Nathaniel Thomas, Michael Walter, and Zhao Yang. Holographic duality from random tensor networks. J. High Energy Phys., (11):009, front matter+55, 2016.
[5] Pavan Hosur, Xiao-Liang Qi, Daniel A. Roberts, and Beni Yoshida. Chaos in quantum channels. Journal of High Energy Physics, 2016(2), Feb 2016.
[6] Mark M. Wilde. Quantum Information Theory. Cambridge University Press, 2013.
[7] Patrick Hayden and John Preskill. Black holes as mirrors: Quantum information in random subsystems. Journal of High Energy Physics, 2007, 09 2007.
[8] Patrick Hayden, Michal Horodecki, Andreas Winter, and Jon Yard. A decoupling approach to the quantum capacity. Open Systems & Information Dynamics, 15(01):7–19, 2008.
[9] Richard Cleve, Daniel Gottesman, and Ho-Kwong Lo. How to share a quantum secret. Phys. Rev. Lett., 83:668–651, Jul 1999.
[10] Dardo Goyeneche, Daniel Alsina, José I. Latorre, Arnau Riera, and Karol Życzkowski. Absolutely maximally entangled states, combinatorial designs, and multiunitary matrices. Phys. Rev. A, 92:032316, Sep 2015.
[11] Don N. Page. Information in black hole radiation. Phys. Rev. Lett., 71:3734–3746, Dec 1993.
[12] Ahmed Almheiri, Xi Dong, and Daniel Harlow. Bulk locality and quantum error correction in ads/cft. Journal of High Energy Physics, 2015(4), Apr 2015.
[13] Michael B. Marcus and Gilles Pisier. Random Fourier series with applications to harmonic analysis, volume 101 of Annals of Mathematics Studies. Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1981.
[14] Marius Junge, Chloe Kim, Guanglei Liu, and Peixue Wu. Quantum secret sharing and tripartite information. arXiv preprint arXiv:2012.08445, 2020.
[15] Sreraman Muralidharan, Chang-Ling Zou, Linshu Li, Jianming Wen, and Liang Jiang. Overcoming erasure errors with multilevel systems. New Journal of Physics, 19(1):013026, 2017.
[16] Patrick Hayden, Matthew Headrick, and Alexander Maloney. Holographic mutual information is monogamous. Physical Review D, 87(4), Feb 2013.