On the Capacity of Distributed Quantum Storage

Hua Sun, Syed A. Jafar

Abstract

A distributed quantum storage code maps a quantum message to N storage nodes, of arbitrary specified sizes, such that the stored message is robust to an arbitrary specified set of erasure patterns. The sizes of the storage nodes, and erasure patterns may not be homogeneous. The capacity of distributed quantum storage is the maximum feasible size of the quantum message (relative to the sizes of the storage nodes), when the scaling of the size of the message and all storage nodes by the same scaling factor is allowed. Representing the decoding sets as hyperedges in a storage graph, the capacity is characterized for various graphs, including MDS graph, wheel graph, Fano graph, and intersection graph. The achievability is related via quantum CSS codes to a classical secure storage problem. Remarkably, our coding schemes utilize non-trivial alignment structures to ensure recovery and security in the corresponding classical secure storage problem, which leads to similarly non-trivial quantum codes. The converse is based on quantum information inequalities, e.g., strong sub-additivity and weak monotonicity of quantum entropy, tailored to the topology of the storage graphs.

Hua Sun (email: hua.sun@unt.edu) is with the Department of Electrical Engineering at the University of North Texas. Syed A. Jafar (email: syed@uci.edu) is with the Department of Electrical Engineering and Computer Science (EECS) at the University of California Irvine.

1 Introduction

Robust storage of quantum information is a central technical challenge that stands in the way of the highly anticipated quantum technologies of the future. Efficient distributed quantum computing for instance requires efficient distributed storage of quantum information along with efficient recovery from failures of subsystems. There is a rich history of progress in quantum coding theory leading to a variety of efficient constructions of quantum error correction codes (QECCs) and bounds on optimal code parameters [1, 2]. Recently there is also interest in applying Shannon theoretic reasoning (based on properties of von Neumann entropies) to discover the fundamental limits of quantum storage [3, 4].

Distinct from coding theory which prioritizes practical code constructions with (relatively) short codelengths and/or low dimensional systems, a Shannon theoretic approach may prioritize asymptotic optimality guarantees, seeking tractability in the expanded space obtained by allowing arbitrarily long codelengths and/or arbitrarily large local dimensions while constraining only the *relative* values (i.e., ratios) of key parameters. The two distinct perspectives lead to different challenges and produce complementary insights. For example, consider the quantum Singleton bound, $n \geq k + 2(d-1)$ that is satisfied by any $[[n, k, d]]_q$ quantum code [5, 6, 7, 8], where n, k, d, q represent the number of physical qudits, the number of logical qudits, the minimum distance, and the local dimension of each qudit, respectively. Given a local dimension q, codes achieving this bound, called quantum maximum distance separable (QMDS) codes, may not exist. For instance if $q = 2$ (qubit systems) then there is no quantum code for one logical qubit $(k = 1)$, that tolerates the erasure of any one $(d - 1 = 1)$ physical qubit, and needs only three $(n = 3)$ physical qubits (the minimum feasible value is $n = 4$ in this case [9]). This is reflected in the QMDS conjecture [8, 10, 11] that remains a prominent open problem in coding theory. On the other hand, if the local dimension q is allowed to be arbitrarily large, then QMDS codes always exist and need only generic structures.[1] Remarkably, the Singleton bound is also a Shannon theoretic bound [3, 4], and once the local dimension constraint is relaxed (allowing arbitrarily large q) it immediately provides a *tight* information theoretic characterization of the optimal code parameters. The improved tractability afforded by relaxed local dimension constraints makes a Shannon theoretic approach suitable for exploring (asymptotically) optimal codes for more general settings, e.g., for *heterogeneous* storage systems.

A common simplifying assumption in studies of QECCs is that the subsystems comprising the quantum storage are homogeneous, i.e., they have the same size, and are equally likely to be impacted by noise. It is known, however, that noise characteristics depend very much on the hardware implementation, varying significantly from one physical qudit to another, and failures can be highly correlated. Noting that the performance of a QECC is strongly impacted by such disparities, recent works have emphasized the critical importance of studying optimal code designs for heterogeneous noise structures [12].

The concerns are further amplified if the storage is broadly *distributed*. Distributed storage systems are likely to employ a variety of quantum subsystems, differing in size and robustness level from one location to another. Furthermore, if these distributed storage systems are to some day mature to larger scales (paralleling existing classical datacenters), then the constituent subsystems will themselves need to approach large sizes, e.g., each constituent subsystem in a large scale distributed storage system may itself be a storage system employing an internal QECC. A Shannon

[1] This is also the case in classical coding theory, where the corresponding classical MDS conjecture remains open, but over large alphabet almost any randomly generated code is MDS.

theoretic approach may be especially well suited for the study of such systems. Last but not the least, since larger subsystems may be able to employ internal consistency checks within each location, the dominant failure mode in large scale distributed quantum storage systems (similar to classical datacenters) is likely to be errors in *known* locations, also known as erasures.

Motivated by these observations, and drawing inspiration from the formulations in [3, 4], in this work we undertake a Shannon theoretic study of the fundamental limits of heterogeneous distributed quantum storage systems subject to erasures. We model the distributed quantum storage as an N-partite quantum system $Q_1 \cdots Q_N$ where each $Q_n, n \in [N]$ is viewed as a storage node. The *relative sizes* of the storage nodes are specified via the parameters $\lambda_n, n \in [N]$. Since only the relative values are of interest it will be convenient to set $\min_{n\in[N]} \lambda_n = 1$. The set of erasure patterns that must be protected against is also specified. The sizes and the erasure patterns need not be homogeneous. We explore the *capacity* of such a distributed storage system, defined informally (see Section 2.2 for formal definitions) as the maximum (relative) amount (λ_0) of arbitrary quantum information (Q_0) that can be stored in the N storage nodes while respecting all specified storage size constraints and ensuring robustness against all specified erasure patterns.

Let us illustrate the problem with an example. Consider a distributed storage system with 4 storage nodes, Q_1, Q_2, Q_3, Q_4, of relative sizes $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ (these are arbitrary values specified by the problem, e.g., $\lambda_1 = 1, \lambda_2 = 2, \lambda_3 = 3, \lambda_4 = 4$). Say the erasure patterns are specified such that the nodes in any one of subsets $\{Q_1\}$, $\{Q_2, Q_3\}$, $\{Q_2, Q_4\}$, $\{Q_3, Q_4\}$ may be erased. Equivalently, the quantum information stored in this distributed storage system must be perfectly decodable from the surviving (unerased) set of nodes $\mathcal{D}(e) = \{Q_n : n \in e\}$, for any $e \in \mathcal{E} = \{\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3, 4\}\}$. Assume, without loss of generality in this case, that $\lambda_2 \leq \lambda_3 \leq \lambda_4$. A graphical representation of this storage system (labeled the 'wheel graph $\mathcal{W}_4$') appears in Figure 1.

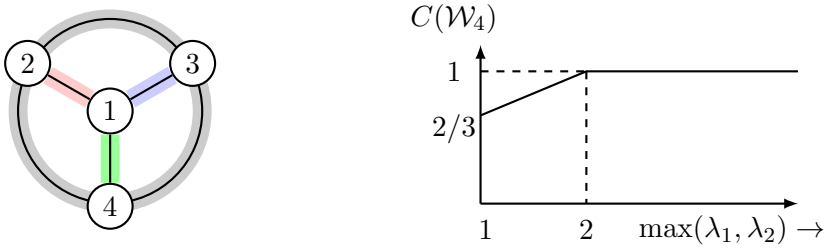


Figure 1: (Left) The 'wheel graph $\mathcal{W}_4$' representing a 4-partite quantum storage system $Q_1Q_2Q_3Q_4$, where each storage node Q_n is represented by a vertex n, $n \in [4]$, and decoding sets $\{Q_1, Q_2\}$, $\{Q_1, Q_3\}$, $\{Q_1, Q_4\}$, $\{Q_2, Q_3, Q_4\}$ are represented by the red, blue, green, and black hyperedges, respectively. (Right) The storage capacity $C(\mathcal{W}_4) = \min(\lambda_1, \lambda_2, (\lambda_1 + \lambda_2)/3)$ is shown as a function of $\max(\lambda_1, \lambda_2)$ assuming without loss of generality that $\min(\lambda_1, \lambda_2) = 1$ and $\lambda_2 \leq \lambda_3 \leq \lambda_4$.

The capacity of this storage system is the largest (relative) amount (λ_0) of quantum information Q_0 that can be stored in $Q_1Q_2Q_3Q_4$ such that Q_0 can be perfectly recovered from any $\mathcal{D}(e)$, $e \in \mathcal{E}$. For this storage system, we show (special case of Theorem 4 in Section 3.2.2) that the storage capacity is $C(\mathcal{W}_4) \triangleq \min\left(\lambda_1, \lambda_2, \frac{\lambda_1+\lambda_2}{3}\right)$. A capacity characterization requires matching achievability and converse arguments. For the converse we provide a Shannon theoretic proof that if there exists *any* storage scheme (not limited to any special class of codes, e.g., CSS codes [13, 14]) capable of storing arbitrary quantum information Q_0 of size $\log_2 |Q_0| = \kappa\lambda_0$ qubits into a 4-partite

quantum system $Q_1Q_2Q_3Q_4$ with sizes $\log_2|Q_n| \leq \kappa\lambda_n$ qubits, $n \in [4]$, for some scaling factor $\kappa > 0$ that can be chosen freely by the coding scheme, such that Q_0 can be recovered perfectly from any $\mathcal{D}(e)$, $e \in \mathcal{E}$, then we must have $\lambda_0 \leq C(\mathcal{W}_4) = \min\left(\lambda_1, \lambda_2, \frac{\lambda_1+\lambda_2}{3}\right)$. For achievability we provide a constructive proof that given $\lambda_1, \lambda_2, \lambda_3, \lambda_4$, and any $\epsilon > 0$, there exists a storage scheme capable of storing arbitrary quantum information Q_0 of size $\log_2|Q_0| \geq \kappa(C(\mathcal{W}_4) - \epsilon)$ qubits into a 4-partite quantum system $Q_1Q_2Q_3Q_4$ with sizes $\log_2|Q_n| \leq \kappa\lambda_n$ qubits, $n \in [4]$, for some scaling factor $\kappa > 0$, such that Q_0 can be recovered perfectly from $\mathcal{D}(e)$, $e \in \mathcal{E}$.

As evident from the example, distributed quantum storage systems can be conveniently represented as graphs with vertices identifying storage nodes along with their relative size parameters, and hyperedges identifying the decoding sets. Given a storage graph, in order to find a Shannon theoretic converse we apply quantum information inequalities, e.g., strong sub-additivity and weak monotonicity of quantum entropy, tailored to the specified storage structure. The converse proof for the wheel graph $\mathcal{W}_4$ example is presented in Section 4.2.

To find achievable coding schemes, we take advantage of an important connection previously noted in literature in a few slightly different forms [15, 16]. This connection, via CSS codes, is essentially between our quantum distributed storage coding problem, and a corresponding classical secure storage problem. Through this connection (formalized in Theorem 2 and Corollary 1 in Section 3.1), quantum systems $Q_0, Q_1, \cdots, Q_N$ with sizes $\kappa\lambda_0, \kappa\lambda_1, \cdots, \kappa\lambda_N$ qudits (a qudit represents a q-dimensional quantum system) are mapped to classical symbols $Y_{Q_0}, Y_{Q_1}, \cdots, Y_{Q_N}$ in $\mathbb{F}_q^{\kappa\lambda_0}, \mathbb{F}_q^{\kappa\lambda_1}, \cdots, \mathbb{F}_q^{\kappa\lambda_N}$, respectively (provided q is a prime power so that the finite field $\mathbb{F}_q$ exists, and $\kappa\lambda_n \in \mathbb{N}$, $n \in \{0, \cdots, N\}$). Y_{Q_0} now represents as a classical secret, whereas $Y_{Q_1}, \cdots, Y_{Q_N}$ are the classical secret shares. The secret Y_{Q_0} (comprising $\kappa\lambda_0$ i.i.d. uniform symbols from $\mathbb{F}_q$) must be decodable from any set of secret shares $\mathcal{Y}_{\mathcal{D}(e)} = \{Y_{Q_n} : n \in e\}$, where $e \in \mathcal{E}$, and $\mathcal{E}$ is the set of decoding-set-indices inherited from the quantum distributed storage problem. Also, quite importantly, any set of secret shares corresponding to erased systems, i.e., $\{Y_{Q_n} : n \in [N] \setminus e\}$ must not reveal any information about the secret. The latter constraint is a consequence of the quantum no-cloning theorem. The key observation is the following. If there exists an $\mathbb{F}_q$-linear solution to this classical problem, then by utilizing the connection between the two problems, the solution translates into a quantum distributed storage code for our original problem.

For an illustration via our wheel graph $\mathcal{W}_4$ example, consider the size constraints, say $\lambda_1 = 1, \lambda_2 = \lambda_3 = \lambda_4 = 2$, for which the capacity $C(\mathcal{W}_4) = 1$. The mapping to the classical secure storage problem is shown in Figure 2, along with the optimal solution. The general solution for the $\mathcal{W}_4$ example with arbitrary size constraints λ_n is presented in Section 4.2.

The storage graph structures that emerge out of the heterogeneous aspects of distributed quantum storage, lead to rather non-trivial classical secure storage problems that have not been explored in the classical secret sharing and secure storage literature. Unlike homogeneous settings where generic structures tend to be optimal, these problems in general require *interference alignment* principles for optimal code design in order to efficiently satisfy the simultaneous decodability and security constraints. Even in the simple example of the wheel graph $\mathcal{W}_4$, alignment can be seen in the mirroring of the $a + b_1$ symbol in $Y_{Q_2}, Y_{Q_3}, Y_{Q_4}$. This is needed to ensure that any two of these shares (because the corresponding quantum storage nodes can be erased) do not reveal anything about the secret. Gaining insight into the role that interference alignment might play in quantum storage codes is a key motivation for the present work.

Notation: $[N]$ denotes the set $\{1, 2, \cdots, N\}$ and $[i : j]$ denotes the set $\{i, i+1, \cdots, j\}$ for $i \leq j, i, j, N \in \mathbb{N}$. $|X|$ denotes the cardinality of X if X is a set, the dimension of X if X is a vector, and

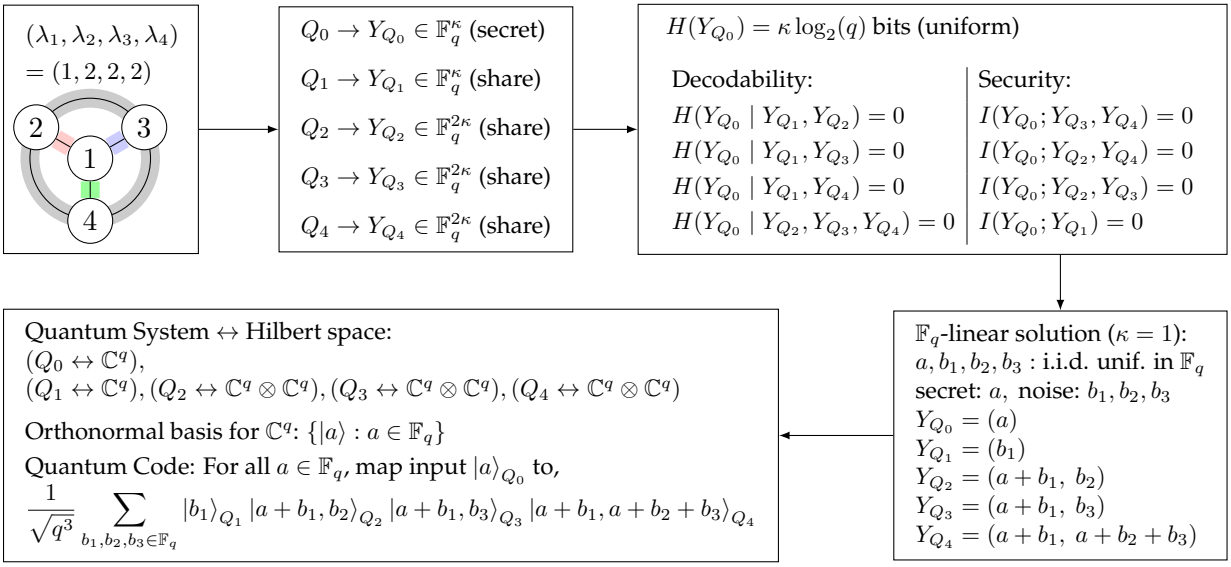


Figure 2: Sketch of achievability argument ($\lambda_0 = 1$) for a particular wheel graph $\mathcal{W}_4$ setting, with size constraints $(\lambda_1, \lambda_2, \lambda_3, \lambda_4) = (1, 2, 2, 2)$. Quantum nodes are mapped to classical nodes of corresponding sizes over $\mathbb{F}_q$, decodability and security constraints (stated here in entropic terms) define the classical secure storage problem, and an $\mathbb{F}_q$-linear solution to the classical problem is mapped to a quantum distributed storage code via a CSS code construction.

the dimension of the Hilbert space associated with X if X is a quantum system. For a set $\mathcal{X}$, the set of its cardinality-k subsets is denoted as $\binom{\mathcal{X}}{k} \triangleq \{\mathcal{Y} : \mathcal{Y} \subset \mathcal{X}, |\mathcal{Y}| = k\}$ and the set of all subsets of $\mathcal{X}$ is denoted as $2^{\mathcal{X}}$. For two sets $\mathcal{X}, \mathcal{Y}$, the notation $\mathcal{X} \setminus \mathcal{Y}$ denotes the set of elements that are in $\mathcal{X}$ but not in $\mathcal{Y}$. For matrices $\mathbf{M}_1, \mathbf{M}_2$ of compatible dimensions, $(\mathbf{M}_1, \mathbf{M}_2)$ and $(\mathbf{M}_1; \mathbf{M}_2)$ represent their horizontal and vertical concatenations, respectively. For a matrix $\mathbf{M}$, the notation $\langle \mathbf{M} \rangle$ denotes the vector space spanned by the columns of $\mathbf{M}$ (defined over the same field as the elements of $\mathbf{M}$). $\mathbf{I}_{k \times k}$ represents the $k \times k$ identity matrix and $\mathbf{0}_{k_1 \times k_2}$ represents the $k_1 \times k_2$ matrix with all its elements equal to 0; the subscript that indicates the matrix dimension may be omitted when it is clear from the context. For quantum systems X, Y, the notation $X \rightsquigarrow Y$ denotes that a unitary (isometric) map is applied to X so that it is transformed to Y. When X is a set of classical random variables or quantum systems, $H(X)$ denotes the joint Shannon or von Neumann (quantum) entropy of the elements in X. $\mathbb{F}_q$ denotes the finite field with q elements where q is a power of a prime.

2 Problem Statement

2.1 Preliminaries

Before we formally introduce our problem statement, let us recall some elementary aspects of modeling of quantum systems. A quantum system Q is associated with a Hilbert space $\mathcal{H}_Q$. The dimension of a quantum system Q, denoted $|Q|$, corresponds to the dimension of the Hilbert space $\mathcal{H}_Q$. In this work we only consider finite dimensional Hilbert spaces. Arbitrary states of Q are represented by density matrices, i.e., unit trace positive semidefinite matrices over $\mathcal{H}_Q$. Define $S(\mathcal{H}_Q)$ as the set of density matrices over $\mathcal{H}_Q$. Define the set of unit rank density matrices,

corresponding to pure states, as $S_1(\mathcal{H}_Q)$. Pure states can also be represented as unit vectors in $\mathcal{H}_Q$. For a composite system comprised of N quantum subsystems, if the subsystem Q_n is associated with the Hilbert space $\mathcal{H}_{Q_n}$, $n \in [N]$, then the composite system $Q_1 Q_2 \cdots Q_N$ is associated with the Hilbert space $\mathcal{H}_{Q_1} \otimes \mathcal{H}_{Q_2} \otimes \cdots \otimes \mathcal{H}_{Q_N}$. A *qudit*, representing a q-dimensional quantum system, is a conventional unit for expressing the size of a quantum system. When $q = 2$ the qudit is called a qubit.[2] The size of a quantum system Q is $\log_2 |Q|$ qubits, which is the same as $\log_q |Q|$ qudits. For the composite system $Q_1 Q_2 \cdots Q_N$, where each Q_n has size $\log_2 |Q_n|$ qubits, $n \in [N]$, the composite system has size $\log_2 |Q_1 Q_2 \cdots Q_N| = \log_2 |Q_1| + \log_2 |Q_2| + \cdots + \log_2 |Q_N|$ qubits.

2.2 Distributed Quantum Storage Capacity Formulation

A quantum *storage structure* is specified as a graph $\mathcal{G} = ((\lambda_1, \cdots, \lambda_N), \mathcal{E})$. The graph $\mathcal{G}$ has N vertices representing quantum storage nodes,

$$\mathcal{Q}(\mathcal{G}) = \{Q_1, Q_2, \cdots, Q_N\},$$

and a set of hyperedges, $\mathcal{E} \subset 2^{[N]}$, that defines the corresponding decoding sets,

$$\mathcal{D}(e) \triangleq \{Q_n : n \in e\}, \quad e \in \mathcal{E},$$

and their complements,

$$\mathcal{D}^c(e) \triangleq \{Q_n : n \in [N] \setminus e\}, \quad e \in \mathcal{E}.$$

A storage node is *redundant* if it is not included in any decoding set. A decoding set is *redundant* if it includes a smaller decoding set as a proper subset. We assume that the storage graphs have no redundant storage nodes, and no redundant decoding sets, i.e., for every $Q_n, n \in [N]$, there exists some $e \in \mathcal{E}$ such that $Q_n \in e$, and there are no $e, e' \in \mathcal{E}$ such that $e \subset e'$.

Each storage node Q_n has size constrained as $\log_q |Q_n| \leq \kappa \lambda_n$ qudits, for all $n \in [N]$. Here κ is a scaling factor, and a qudit represents a q-dimensional quantum system.

A quantum *message*, Q_0, is a quantum system with size $\log_q |Q_0| = \kappa \lambda_0$ qudits. Along with Q_0, define R, without loss of generality also of the same size $\log_q |R| = \kappa \lambda_0$ qudits, as a *reference* quantum system such that RQ_0 is an arbitrary pure state $|\varphi\rangle \langle\varphi|_{RQ_0} \in S_1(\mathcal{H}_R \otimes \mathcal{H}_{Q_0}) = S_1(\mathbb{C}^{q^{\kappa\lambda_0}} \otimes \mathbb{C}^{q^{\kappa\lambda_0}})$.

We say that storage $(\mathcal{G}, q, \kappa)$ *fits* Q_0 if and only if there exists a CPTP (completely positive trace preserving) encoding map,[3]

$$\text{ENC} : S(\mathcal{H}_{Q_0}) \to S(\mathcal{H}_{Q_1} \otimes \cdots \otimes \mathcal{H}_{Q_N}),$$

that maps the quantum message Q_0 to the storage nodes $Q_1 Q_2 \cdots Q_N$, and for each $e \in \mathcal{E}$, a CPTP decoding map,[4]

$$\text{DEC}^e : S(\otimes_{n \in e} \mathcal{H}_{Q_n}) \to S(\mathcal{H}_{Q_0}),$$

[2]The choice of units is a cosmetic issue, since translation from one unit to another is trivial, but if the quantum systems involved are naturally composed of q-dimensional subsystems for some $q \neq 2$ then using a qudit (instead of a qubit) as the unit may produce cleaner expressions.

[3]While the map is specified between two sets of density matrices, it can be readily extended to all linear operators (matrices). Refer to Section 5.1 of [17] or Appendix B of [18].

[4]Note that we adopt a compound channel model, where there are $|\mathcal{E}|$ decoders, one for each erasure pattern.

that maps the storage nodes in the corresponding decoding set $\mathcal{D}(e)$ to an output $\widehat{Q}_0$ such that $R\widehat{Q}_0$ is in state $|\varphi\rangle$, i.e., the original message Q_0 and any entanglement with the reference system are perfectly recovered.

$$I_R \otimes \left(\mathrm{DEC}^e_{(Q_n:n\in e)\to\widehat{Q}_0} \circ \mathcal{N}^e_{(Q_n:n\in[N])\to(Q_n:n\in e)} \circ \mathrm{ENC}_{Q_0\to(Q_n:n\in[N])}\right)_{Q_0\to\widehat{Q}_0} (|\varphi\rangle\langle\varphi|)_{RQ_0} = (|\varphi\rangle\langle\varphi|)_{R\widehat{Q}_0},$$
$$\forall\, |\varphi\rangle\langle\varphi| \in S_1(\mathcal{H}_R \otimes \mathcal{H}_{Q_0}) = S_1(\mathbb{C}^{q^{\kappa\lambda_0}} \otimes \mathbb{C}^{q^{\kappa\lambda_0}}), \forall e \in \mathcal{E}. \tag{1}$$

Here the channel $\mathcal{N}^e(\cdot) \triangleq \mathrm{Tr}_{(Q_n:n\in[N]\setminus e)}(\cdot)$ simply erases the quantum systems $Q_n, n \in [N] \setminus e$.

Given storage $(\mathcal{G}, q, \kappa)$, we wish to determine how much quantum information can be stored, i.e., the largest λ_0 such that $(\mathcal{G}, q, \kappa)$ fits Q_0. While it is important from a coding theoretic perspective to answer the question for any given $\mathcal{G}, q, \kappa$, we will adopt a Shannon theoretic perspective and focus instead on a coarser (but more tractable) objective, the *storage capacity* (defined next) which relaxes the dependence on κ and q, by optimizing over these parameters.

The *storage capacity* of a storage graph $\mathcal{G}$ is defined as

$$C(\mathcal{G}) \triangleq \sup_{q,\kappa\in\mathbb{N}} \sup\{\lambda_0 : (\mathcal{G}, q, \kappa) \text{ fits } Q_0\}. \tag{2}$$

A subscript 'u' is added ($C_u(\mathcal{G})$) if the storage is uniform, i.e., $\lambda_1 = \lambda_2 = \cdots = \lambda_N = 1$.

Since the sizes of $Q_0, Q_1, \cdots, Q_N$ are allowed to scale proportionately, only the relative values of $\lambda_0, \lambda_1, \cdots, \lambda_N$ are important for storage capacity. Without loss of generality we will assume,

$$\min_{n\in[N]} \lambda_n = 1. \tag{3}$$

Remark 1. *Similar to the observation in [3], the storage capacity, as defined above corresponds to the Shannon theoretic capacity of the quantum erasure channel shown in Figure 3. The scaling factor κ corresponds in this case to the number of channel uses. Over κ channel uses, each Q_n represents the composite system $Q_n(1)Q_n(2)\cdots Q_n(\kappa) \equiv Q_n$ which has size $\kappa\lambda_n$ qudits, i.e., $\log_q |Q_n| = \kappa\lambda_n$, whereas each subsystem $Q_n(k)$ corresponding to channel use $k \in [\kappa]$ has size fixed as $\log_q |Q_n(k)| = \lambda_n$ qudits. Recall that in the Shannon theoretic formulation the number of channel uses κ can scale arbitrarily. The alphabet q can also be chosen arbitrarily in this channel as it only amounts to a choice of 'sub-packetization' of the composite quantum systems which is inconsequential for a Shannon theoretic capacity formulation (see e.g., Theorem VI.5 of [19]). The setting in Figure 3 corresponds to a 'compound channel' setting in the information theory literature (cf. [20] and the references therein). Here 'e' is a channel state that is chosen from a set of possible states $\mathcal{E}$, and then held fixed across all channel uses. The state (e) is known to the receiver. The transmitter knows only the set of possible realizations, $\mathcal{E}$, but not the actual realization (e).*

The following notion of a maximal storage graph will be useful.

Definition 1 (Maximal Storage Graph)**.** A quantum storage graph $\mathcal{G} = ((\lambda_1, \cdots, \lambda_N), \mathcal{E})$ is said to be *strongly maximal* if its capacity $C(\mathcal{G}) > 0$, but for all $\mathcal{G}' = ((\lambda'_1, \cdots, \lambda'_{N'}), \mathcal{E}')$ such that $\mathcal{G}$ is a proper[5] subgraph of $\mathcal{G}'$, the capacity $C(\mathcal{G}') = 0$. A quantum storage graph $\mathcal{G}$ is said to be *weakly maximal* if for all $\mathcal{G}'$ such that $\mathcal{G}$ is a proper subgraph of $\mathcal{G}'$, the capacity $C(\mathcal{G}') < C(\mathcal{G})$.

[5] $\mathcal{G} = ((\lambda_1, \cdots, \lambda_N), \mathcal{E})$ is said to be a proper subgraph of $\mathcal{G}' = ((\lambda'_1, \cdots, \lambda'_{N'}), \mathcal{E}')$ if either $N = N'$, $\mathcal{E} \subsetneq \mathcal{E}'$ (i.e., the vertex set is identical while the edge set is a proper subset) or $N < N'$, $\mathcal{E} \subsetneq \mathcal{E}'$ (note that if the vertex set is a proper subset, then it implies that the edge set must also be a proper subset as we assume there is no redundant storage node).

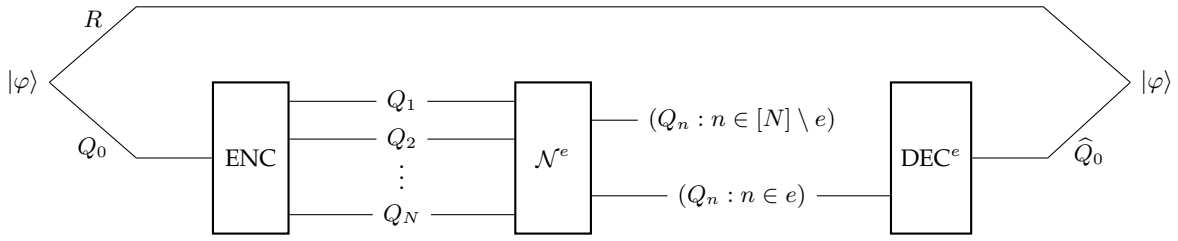


Figure 3: Erasure channel corresponding to the storage capacity problem. Given any $e \in \mathcal{E}$, the channel $\mathcal{N}^e$ erases the storage nodes Q_i for all $i \in [N] \setminus e$, leaving only storage nodes $Q_j, j \in e$ for the decoder DEC^e. Note that the encoder does not depend on e, because the positions of erasures are not known at the time of encoding, but the decoder is chosen based on the realization of e because the decoding is done with the knowledge of which storage nodes are erased.

3 Results

3.1 Capacity Bounds for Arbitrary Storage Graphs

We first present upper and lower bounds on the capacity of arbitrary storage graphs in the following two theorems, respectively. For a set of quantum storage nodes $\mathcal{S} \subset \mathcal{Q}(\mathcal{G}) = \{Q_1, Q_2, \cdots, Q_N\}$, define the compact notation $\Lambda(\mathcal{S}) = \sum_{i:Q_i \in \mathcal{S}} \lambda_i$.

Theorem 1. *The quantum storage capacity of $\mathcal{G} = ((\lambda_1, \cdots, \lambda_N), \mathcal{E})$ is bounded from above as,*

$$\textit{Intersection Bound:} \qquad C(\mathcal{G}) \leq \Lambda\Big(\mathcal{D}(e_i) \cap \mathcal{D}(e_j)\Big), \qquad \forall e_i, e_j \in \mathcal{E}, e_i \neq e_j, \tag{4}$$

$$\textit{Wheel Bound:} \qquad C(\mathcal{G}) \leq \frac{\Lambda(\mathcal{Q}_1) + \Lambda(\mathcal{Q}_2) + \cdots + \Lambda(\mathcal{Q}_k)}{2k-1}, \qquad \forall k \in [2 : n-2], \tag{5}$$

where $\{\mathcal{Q}_1, \mathcal{Q}_2, \cdots, \mathcal{Q}_n\}$ is a partition of $\mathcal{Q}(\mathcal{G})$ such that $\Lambda(\mathcal{Q}_2) \leq \Lambda(\mathcal{Q}_3) \leq \cdots \leq \Lambda(\mathcal{Q}_n)$ and each of $\mathcal{Q}_1 \cup \mathcal{Q}_2$, $\mathcal{Q}_1 \cup \mathcal{Q}_3$, $\cdots$, $\mathcal{Q}_1 \cup \mathcal{Q}_n$, and $\mathcal{Q}_2 \cup \mathcal{Q}_3 \cup \cdots \cup \mathcal{Q}_n$ contains a decoding set of $\mathcal{G}$ as a subset.

The proof of Theorem 1 is presented in Section 5.1. The intersection bound (4) is a consequence of the no-cloning theorem [21, 22] while the wheel bound (5) requires the use of the strong sub-additivity (sub-modularity) and weak monotonicity properties of quantum entropy [23, 24].

Theorem 2. *(CSS Bound) The quantum storage capacity of $\mathcal{G} = ((\lambda_1, \cdots, \lambda_N), \mathcal{E})$ is bounded from below as $C(\mathcal{G}) \geq k/\kappa$ if there exist $k, \delta, n, \kappa \in \mathbb{N}$, a finite field $\mathbb{F}_q$ and matrices $\mathbf{A} \in \mathbb{F}_q^{k \times n}, \mathbf{B} \in \mathbb{F}_q^{\delta \times n}$ with rank$(\mathbf{A}) = k$, rank$(\mathbf{A}; \mathbf{B}) = k + \delta$, such that for all $e \in \mathcal{E}$,*

$$0 = H(\boldsymbol{a} \mid \mathcal{Y}_{\mathcal{D}(e)}), \tag{6}$$

$$0 = I(\boldsymbol{a}; \mathcal{Y}_{\mathcal{D}^c(e)}). \tag{7}$$

The following notation is used here.

1. *$\mathcal{Y}_{\mathcal{S}} \triangleq \{Y_Q : Q \in \mathcal{S}\}$ for all $\mathcal{S} \subset \mathcal{Q}(\mathcal{G})$,*
2. *$(Y_{Q_1}, Y_{Q_2}, \cdots, Y_{Q_N}) \triangleq \boldsymbol{a}\mathbf{A} + \boldsymbol{b}\mathbf{B} \in \mathbb{F}_q^{1 \times n}$, where*

$$n = \kappa(\lambda_1 + \cdots + \lambda_N), \tag{8}$$

$$\mathbf{A} = (\mathbf{A}_1, \cdots, \mathbf{A}_N),\ \mathbf{A}_i \in \mathbb{F}_q^{k \times \kappa\lambda_i}, \tag{9}$$

$$\mathbf{B} = (\mathbf{B}_1, \cdots, \mathbf{B}_N),\ \mathbf{B}_i \in \mathbb{F}_q^{\delta \times \kappa\lambda_i}, \tag{10}$$

$$Y_{Q_i} = \boldsymbol{a}\mathbf{A}_i + \boldsymbol{b}\mathbf{B}_i \in \mathbb{F}_q^{1 \times |Y_{Q_i}|}, |Y_{Q_i}| = \log_q |Q_i| = \kappa\lambda_i, i \in [N], \tag{11}$$

3. $\boldsymbol{a}, \boldsymbol{b}$ *are* $1 \times k$ *and* $1 \times \delta$ *random vectors, respectively, with i.i.d. uniform elements in* $\mathbb{F}_q$.

Theorem 2 allows the construction of an achievable scheme for the quantum storage problem via a classical secure storage problem, i.e., k classical symbols $\boldsymbol{a}$ (comprising a 'secret' Y_{Q_0}) are stored over classical storage nodes $Y_{Q_1}, \cdots, Y_{Q_N}$ such that from any decoding set $\mathcal{Y}_{\mathcal{D}(e)}$, we may recover the classical symbols $\boldsymbol{a}$ (refer to (6)) while from the complement of any decoding set $\mathcal{Y}_{\mathcal{D}^c(e)}$, nothing is revealed about $\boldsymbol{a}$ (refer to (7)). Security is guaranteed with the help of independent classical uniform noise symbols $\boldsymbol{b}$. The classical decoding constraint (6) and the classical security constraint (7) (the random variables are classical so only Shannon entropies are involved) can be equivalently stated as rank constraints on matrices $\mathbf{A}, \mathbf{B}$, presented in the following corollary.

Corollary 1. *For any* $\mathcal{S} = \{Q_{i_1}, \cdots, Q_{i_{|\mathcal{S}|}}\} \subset \mathcal{Q}(\mathcal{G})$, *define*

$$\mathbf{A}_{\mathcal{S}} \triangleq (\mathbf{A}_{i_1}, \mathbf{A}_{i_2}, \cdots, \mathbf{A}_{i_{|\mathcal{S}|}}), \tag{12}$$

$$\mathbf{B}_{\mathcal{S}} \triangleq (\mathbf{B}_{i_1}, \mathbf{B}_{i_2}, \cdots, \mathbf{B}_{i_{|\mathcal{S}|}}). \tag{13}$$

Then the following equivalence relations hold.

$$(6) \quad \Leftrightarrow \quad \textit{rank}(\mathbf{A}_{\mathcal{D}(e)}; \mathbf{B}_{\mathcal{D}(e)}) - \textit{rank}(\mathbf{B}_{\mathcal{D}(e)}) = k \tag{14}$$

$$\Leftrightarrow \quad \langle \mathbf{I}_{k\times k}; \mathbf{0}_{\delta\times k} \rangle \subset \langle \mathbf{A}_{\mathcal{D}(e)}; \mathbf{B}_{\mathcal{D}(e)} \rangle, \tag{15}$$

$$(7) \quad \Leftrightarrow \quad \textit{rank}(\mathbf{A}_{\mathcal{D}^c(e)}; \mathbf{B}_{\mathcal{D}^c(e)}) = \textit{rank}(\mathbf{B}_{\mathcal{D}^c(e)}) \tag{16}$$

$$\Leftrightarrow \quad \langle \mathbf{I}_{k\times k}; \mathbf{0}_{\delta\times k} \rangle \cap \langle \mathbf{A}_{\mathcal{D}^c(e)}; \mathbf{B}_{\mathcal{D}^c(e)} \rangle = \{\mathbf{0}\}. \tag{17}$$

Interestingly, the code construction for the classical secure storage problem (6), (7) can be translated into a quantum storage code, which turns out to be equivalent to the canonical CSS quantum code (thus Theorem 2 is called the CSS bound). We note that Theorem 2 (and its connection to CSS codes) is not new and it has appeared in similar (sometimes equivalent or more general) forms in the literature (see e.g., [15], Theorem 1 of [16], and [25]). For the sake of completeness, a proof of Theorem 2 and Corollary 1 is included in Section 5.2 and Section 5.3, respectively.

Equipped with the converse bound in Theorem 1 and the achievability argument in Theorem 2, we are able to characterize the class of all storage graphs for which $C(\mathcal{G}) > 0$, and the exact capacity of small graphs with either $N \leq 4$ nodes or $|\mathcal{E}| \leq 3$ decoding sets. The result is stated in the following corollary.

Corollary 2. *For a storage graph* $\mathcal{G} = ((\lambda_1, \cdots, \lambda_N), \mathcal{E})$,

1. *the capacity* $C(\mathcal{G}) = 0$, *if and only if there exist* $e_i, e_j \in \mathcal{E}$ *such that* $e_i \cap e_j = \emptyset$;
2. *if* $N \leq 4$ *or* $|\mathcal{E}| \leq 3$, *then Theorem 1 provides a tight bound on the capacity* $C(\mathcal{G})$.

Note that the tight capacity characterization for small graphs ($N \leq 4$ or $|\mathcal{E}| \leq 3$) holds whether the storage is uniform or non-uniform. The proof of Corollary 2 is presented in Section 5.4.

3.2 Capacities of Certain Storage Graphs

3.2.1 MDS Graph $\mathcal{M}_{N,K}$

The MDS graph, defined as $\mathcal{M}_{N,K} = \left((\lambda_1, \cdots, \lambda_N), \binom{[N]}{K}\right)$, represents a code structure comprising N storage nodes, $\mathcal{Q}(\mathcal{M}_{N,K}) = \{Q_1, Q_2, \cdots, Q_N\}$, such that any K storage nodes form a decoding set, i.e., $\mathcal{E} = \binom{[N]}{K}$. The storage need not be uniform. Let us assume, without loss of generality, that $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_N$.

Theorem 3. *The capacity of the MDS graph $\mathcal{M}_{N,K}, 2K > N$ is*

$$C(\mathcal{M}_{N,K}) = \min_{\mathcal{I} \in \binom{\{Q_1, \cdots, Q_N\}}{2K-N}} \Lambda(\mathcal{I}) = \lambda_1 + \lambda_2 + \cdots + \lambda_{2K-N}. \tag{18}$$

For uniform storage, the capacity is $C_u(\mathcal{M}_{N,K}) = 2K - N$.

When $2K \leq N$, the capacity is $C(\mathcal{M}_{N,K})$ = 0 due to Corollary 2, because there exist decoding sets that have no intersection. Thus, we only need to consider the cases where $2K > N$. The converse follows from the intersection bound (4). The achievability for uniform storage is already well known, and can be shown by using random (generic) linear codes in the classical secure storage problem with constraints (6), (7) and then applying Theorem 2 to translate into quantum codes; the achievability for non-uniform storage is based on '*space sharing*' over the optimal codes of a number of distinct MDS graphs with uniform storage. An example for $\mathcal{M}_{4,3}$, i.e., with $N = 4, K = 3$, is given in Section 4.1. The proof of Theorem 3 is presented in Section 5.5.

3.2.2 Wheel Graph $\mathcal{W}_N$

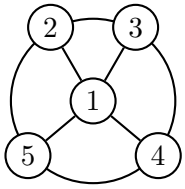
The wheel graph, defined as $\mathcal{W}_N = ((\lambda_1, \cdots, \lambda_N), \mathcal{E})$, has $N \geq 4$ storage nodes and N decoding sets, as follows.

$$\mathcal{E} = \big\{\{1,2\}, \{1,3\}, \cdots, \{1,N\}, \{2,3,\cdots,N\}\big\}. \tag{19}$$

Assume, without loss of generality, that $\lambda_2 \leq \lambda_3 \leq \cdots \leq \lambda_N$.

$\mathcal{W}_5$ is illustrated below.

$\mathcal{W}_5$:



Theorem 4. *The storage capacity of the wheel graph $\mathcal{W}_N, N \geq 4$ is bounded from above as*

$$C(\mathcal{W}_N) \leq \min\left(\lambda_1, \lambda_2, \frac{\lambda_1+\lambda_2}{3}, \frac{\lambda_1+\lambda_2+\lambda_3}{5}, \cdots, \frac{\lambda_1+\lambda_2+\cdots+\lambda_{N-2}}{2N-5}\right), \tag{20}$$

and the upper bound is tight in each of the following cases.

1. $C(\mathcal{W}_4) = \min\left(\lambda_1, \lambda_2, \frac{\lambda_1+\lambda_2}{3}\right)$.

2. $C(\mathcal{W}_5) = \min\left(\lambda_1, \lambda_2, \frac{\lambda_1+\lambda_2}{3}, \frac{\lambda_1+\lambda_2+\lambda_3}{5}\right)$.

3. *If* $\lambda_2 = \lambda_3 = \cdots = \lambda_N$, *then* $C(\mathcal{W}_N) = \min(\lambda_1, \lambda_2, \frac{\lambda_1+(N-3)\lambda_2}{2N-5})$. *In particular, for uniform storage,* $C_u(\mathcal{W}_N) = \frac{N-2}{2N-5}$.

In the upper bound of $C(\mathcal{W}_N)$, the first two terms λ_1, λ_2 follow from the intersection bound (4) while the remaining bounds follow from the wheel bound (5). When the upper bound is achievable, the code construction requires structured (instead of random) linear codes inspired by interference alignment principles. Whether the upper bound (20) is tight for $N \geq 6$ is an open problem. The case of $N = 4$, i.e., the wheel graph $\mathcal{W}_4$ is further illustrated in Section 4.2. The proof of Theorem 4 is presented in Section 5.6.

3.2.3 Fano Graph $\mathcal{F}_7$

The Fano graph, $\mathcal{F}_7 = ((\lambda_1, \cdots, \lambda_7), \mathcal{E})$, has 7 storage nodes and 7 decoding sets, as follows.

$$\mathcal{E} = \{\{1,2,4\}, \{4,5,6\}, \{1,3,6\}, \{2,6,7\}, \{3,4,7\}, \{1,5,7\}, \{2,3,5\}\}. \tag{21}$$

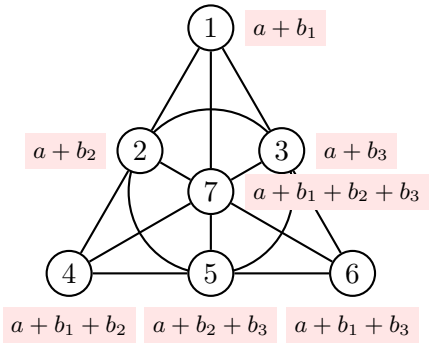


Figure 4: The Fano graph is shown. There are 7 storage nodes and 7 decoding sets. The decoding sets are the hyperedges corresponding to the 6 straight lines and the circle. The solution for the corresponding classical secure storage problem is shown with secret 'a' and noise 'b_1, b_2, b_3,' all i.i.d. uniform in $\mathbb{F}_q$ where $\mathbb{F}_q$ is any finite field with an even characteristic.

Theorem 5. *The capacity of the* 7*-node Fano graph* $\mathcal{F}_7$ *is* $C(\mathcal{F}_7) = 1$.

Note that the capacity does not depend on $\lambda_1, \cdots, \lambda_7$, so the capacity is the same for uniform as well as non-uniform storage. Recall the assumption (3) that $\min_{n\in[7]} \lambda_n = 1$.

Proof. Without loss of generality, suppose $\min_{n\in[7]} \lambda_n = \lambda_1 = 1$. The converse follows from the intersection bound (4) as

$$C(\mathcal{F}_7) \leq \Lambda(\{Q_1, Q_2, Q_4\} \cap \{Q_1, Q_3, Q_6\}) = \lambda_1 = 1.$$

The achievability follows from Theorem 2. Since reducing the sizes of quantum systems cannot increase the storage capacity, it suffices to show achievability for $\lambda_1 = \lambda_2 = \cdots = \lambda_7 = 1$. The corresponding classical secure storage code is shown in Figure 4 where $k = \kappa = \lambda_1 = \cdots = \lambda_7 = 1$. It is not difficult to verify that the decoding constraint (6) and the security constraint (7) hold over

any finite field $\mathbb{F}_q$ with even characteristic. For example, consider the decoding set $\{Q_4, Q_5, Q_6\}$ for which the corresponding classical decoding constraint is satisfied because of the following equation,

$$a = (a + b_1 + b_2) + (a + b_2 + b_3) + (a + b_1 + b_3),$$

which holds only over the binary (extension) field. Similarly, consider the classical security condition corresponding to the decoding set $\{Q_4, Q_5, Q_6\}$. Its complement is the set $\{Q_1, Q_2, Q_3, Q_7\}$, and the corresponding classical storage $a + b_1, a + b_2, a + b_3, a + b_1 + b_2 + b_3$ reveals nothing about the secret a, i.e.,

$$\begin{aligned}
&I(a; a + b_1, a + b_2, a + b_3, a + b_1 + b_2 + b_3) \\
&= I(a; a + b_1, a + b_2, a + b_3) + I(a; a + b_1 + b_2 + b_3 \mid a + b_1, a + b_2, a + b_3) && (22)\\
&= 0 + H(a + b_1 + b_2 + b_3 \mid a + b_1, a + b_2, a + b_3), && (23)\\
&= 0, && (24)
\end{aligned}$$

only if $\mathbb{F}_q$ has an even characteristic. This is important in the last step (24), because over a field of even characteristic, $a + b_1 + b_2 + b_3$ is determined by (is the sum of) $a + b_1, a + b_2, a + b_3$. Thus the classical code has characteristic dependent alignment structure.

□

3.2.4 Intersection Graph $\sqcap_{\Delta,m}$

Defined for $\Delta > m$, the intersection graph $\sqcap_{\Delta,m} = ((\lambda_1, \cdots, \lambda_N), \mathcal{E})$, has $N = \binom{\Delta}{m}$ storage nodes and Δ decoding sets. Let $\pi : \binom{[\Delta]}{m} \to [N] = \{1, 2, \cdots, \binom{\Delta}{m}\}$ be an aribtrary bijection, that determines the labeling of the storage nodes. For any set $\mathcal{S} \in \binom{[\Delta]}{m}$, define the compact notation $\overline{\mathcal{S}} \triangleq \pi(\mathcal{S})$. Thus, the set of storage nodes is identified as,

$$\mathcal{Q}(\sqcap_{\Delta,m}) = \left\{ Q_{\overline{\mathcal{S}}} : \mathcal{S} \in \binom{[\Delta]}{m} \right\}. \tag{25}$$

We will refer to $\mathcal{S} \in \binom{[\Delta]}{m}$ as the 'label' of the quantum storage node $Q_{\overline{\mathcal{S}}}$. Define

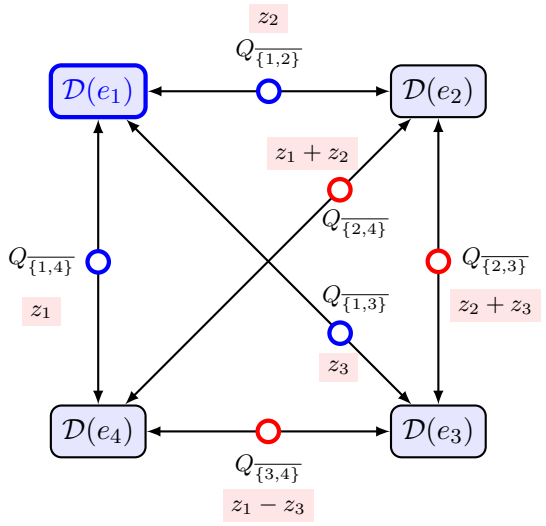
$$\begin{aligned}
e_i &= \left\{ \overline{\mathcal{S}} : i \in \mathcal{S},\ \mathcal{S} \in \binom{[\Delta]}{m} \right\}, \qquad i \in [\Delta], && (26)\\
\mathcal{E} &= \{e_1, e_2, \cdots, e_\Delta\}, && (27)
\end{aligned}$$

so that for each e_i, $i \in [\Delta]$, the decoding set $\mathcal{D}(e_i)$ is defined as

$$\mathcal{D}(e_i) = \{Q_n : n \in e_i\} = \left\{ Q_{\overline{\mathcal{S}}} : i \in \mathcal{S}, \mathcal{S} \in \binom{[\Delta]}{m} \right\}. \tag{28}$$

In words, the decoding set $\mathcal{D}(e_i)$ contains all $\binom{\Delta-1}{m-1}$ storage nodes $Q_{\overline{\mathcal{S}}}$ whose label $\mathcal{S}$ contains i. Note that the intersection of any two decoding sets, $\mathcal{D}(e_i), \mathcal{D}(e_j)$ comprises all $\binom{\Delta-2}{m-2}$ storage nodes whose labels contain both i and j.

For intersection graphs we consider only uniform storage, as this already leads to non-trivial code structures. The intersection graph $\sqcap_{\Delta,m}$ is interesting because on the one hand, the storage structure is 'smooth,' thus somewhat homogeneous. Here by smoothness we mean that any



$$\begin{bmatrix} z_1 & z_2 & z_3 \end{bmatrix} = \begin{bmatrix} a & b_1 & b_2 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$
$$= \begin{bmatrix} a+b_1+b_2 & b_1 & b_2 \end{bmatrix}$$

Figure 5: The intersection graph $\sqcap_{4,2}$ is shown. Storage nodes $\{Q_{\overline{\mathcal{S}}}\}$ appear as empty circles, decoding sets $\{\mathcal{D}(e_i)\}$ as filled rectangles. Arrows from storage nodes to decoding sets indicate membership of the decoding set. Decoding set $\mathcal{D}(e_1)$ and its participating nodes are shown in blue, and the nodes in the complement $\mathcal{D}^c(e_1)$ are shown in red. Also shown is the optimal classical secure storage code over any finite field $\mathbb{F}_q$, with secret $(a \in \mathbb{F}_q)$ and noise $(b_1, b_2 \in \mathbb{F}_q)$, respectively. The optimal classical code translates into an optimal quantum code via Theorem 2.

storage node belongs to *exactly* m decoding sets and all storage nodes have the same size. On the other hand, despite this smoothness of the intersection graph, its capacity characterization involves non-trivial structured alignment of the code spaces. Figure 5 illustrates the intersection graph $\sqcap_{4,2}$ along with an optimal solution to the corresponding classical secure storage problem.

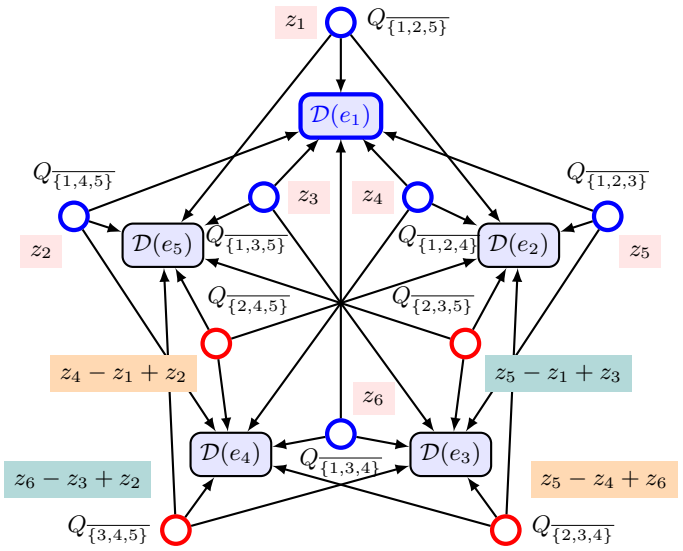
We are able to characterize the uniform storage capacity of intersection graphs in the following theorem.

Theorem 6. *The capacity of the intersection graph $\sqcap_{\Delta,m}$ with uniform storage is,*

$$C_u(\sqcap_{\Delta,m}) = \binom{\Delta-2}{m-2}. \tag{29}$$

The converse follows from the intersection bound (4). The achievability relies on a rather delicate *alignment* based classical secure storage code, in conjunction with Theorem 2. The proof of Theorem 6 is presented in Section 5.7.

As noted, optimal solutions to intersection graphs involve non-trivial alignment structures. Let us briefly preview this aspect. Consider the simple example of the intersection graph $\sqcap_{4,2}$ in Figure 5. Note that the classical secret (a) and noise (b_1, b_2) symbols are first linearly '*precoded*' into the symbols (z_1, z_2, z_3) and then the coding is performed on the z_i symbols. It is not difficult to verify that with the 'precoding' from the secret and noise symbols to z_i symbols, shown explicitly in Figure 5, and the storage code over z_i shown in the graph, all decoding and security constraints are satisfied. It is also worthwhile to note that the precoding aspect is not particularly interesting from a Shannon theoretic perspective. This is because, as it turns out, the precoding requires no special structure over large q. Indeed, for large q, almost any random choice of the linear precoding



$$\begin{bmatrix} z_1 & z_2 & z_3 & z_4 & z_5 & z_6 \end{bmatrix} = \begin{bmatrix} a_1 & a_2 & a_3 & b_1 & b_2 & b_3 \end{bmatrix} \mathbf{M}_{6\times 6}$$

A generic $\mathbf{M}$ suffices for large q.

Figure 6: The intersection graph $\sqcap_{5,3}$ is illustrated, along with an optimal solution to the corresponding classical secure storage problem.

matrix will turn out to be sufficient. The critical aspect of the solution is the required non-trivial alignment structure, which is revealed in the next step following the precoding, i.e., in the coding that is performed over the z_i symbols.

A bit more insightful example is illustrated in Figure 6 which illustrates the intersection graph $\sqcap_{5,3}$ along with the solution to its corresponding secure storage problem. Leaving a more detailed discussion of this example to Section 4.3, let us note here that the solution shown in Figure 6 assumes large q so that generic precoding suffices. Recall that alphabet sizes are not constrained under the Shannon theoretic formulation. However, finding optimal solutions over smaller finite fields may be an interesting open problem from a coding theoretic perspective.

An intuitive sketch of the solution to the classical secure storage problem for intersection graphs is as follows. A generic precoding step maps $k = \binom{\Delta-2}{m-2}$ (capacity of the code, $\kappa = 1$) secrets $(a_1, \cdots, a_k)$ along with $n-k$ noise symbols $(b_1, \cdots, b_{n-k})$ to the $n = \binom{\Delta-1}{m-1}$ (size of a decoding set) symbols $z_1, \cdots, z_n$. A classical code over these z_i symbols determines the storage associated with each node such that the nodes in any decoding set can recover all n of z_i symbols. To guarantee security it is important to ensure that the $N-n$ nodes outside the decoding set remain secured by the $n-k$ noise dimensions. This is a challenging requirement because the complement of a decoding set, $\mathcal{D}^c(e_i)$ has $N - n = \binom{\Delta-1}{m}$ nodes, which is *greater* than the number of noise symbols $n - k = \binom{\Delta-2}{m-1}$. Yet, in the optimal solution, any $\mathcal{D}^c(e_i)$ leaks no information about the secrets $a_1, \cdots, a_k$, precisely due to the crucial *alignment* structure of the classical code. For example in Figure 6, $\mathcal{D}^c(e_1)$ contains 4 nodes (the red nodes), and there are only 3 independent noise symbols (b_1, b_2, b_3). Yet, the code is able to satisfy the security requirement because only 3 of the 4 symbols in $\mathcal{D}^c(e_1)$ carry independent information, whereas the 4^{th} symbol is simply a linear combination of the other 3. In other words, the information contained in the 4^{th} symbol appears along a dimension that *aligns* within the 3 dimensions already occupied by the other 3 symbols, and the 3 independent noise symbols suffice to protect those 3 information dimensions from leaking any secrets. Further details are left to Section 4.3.

3.3 Maximal Storage Graphs

In this section, we briefly explore the maximality of storage graphs. Strongly maximal storage graphs are completely characterized in the following theorem.

Theorem 7. *A storage graph $\mathcal{G} = ((\lambda_1, \cdots, \lambda_N), \mathcal{E})$ is strongly maximal if and only if for every $\mathcal{S} \subset \mathcal{Q}(\mathcal{G}) = \{Q_1, \cdots, Q_N\}$, there exists at least one $\mathcal{D}(e), e \in \mathcal{E}$ that is either completely included or completely excluded by $\mathcal{S}$, i.e., $\mathcal{S} \cap \mathcal{D}(e) \in \{\emptyset, \mathcal{D}(e)\}$.*

Theorem 7 is proved through a more refined treatment of the 'if and only if' condition for $C(\mathcal{G}) > 0$ in Corollary 2. The details are presented in Section 5.8.

Remark 2. *If we replace the non-uniform storage capacity $C(\mathcal{G})$ by the uniform storage capacity $C_u(\mathcal{G})$ in the definition of strongly maximal storage graph, the 'if and only if' condition in Theorem 7 remains the same. This is seen by checking that every step in the proof of Theorem 7 (see Section 5.8) holds for $C_u(\mathcal{G})$ as well, so the same proof applies.*

Let us characterize the maximality of the storage graphs that we have considered.

Corollary 3. *The following maximality properties are noted.*

1. *The MDS graph $\mathcal{M}_{N,K}, 2K > N$ is weakly maximal for all N, K, and strongly maximal iff $2K - N = 1$.*
2. *The wheel graph $\mathcal{W}_N, N \geq 4$ is strongly maximal.*
3. *The Fano graph $\mathcal{F}_7$ is strongly maximal.*
4. *The intersection graph $\sqcap_{\Delta,m}, \Delta > m$ is strongly (weakly) maximal iff $\Delta = 3, m = 2$.*

For strong maximality, we simply apply the 'if and only if' condition in Theorem 7. Weak maximality requires more specialized treatment (e.g., carefully chosen additional decoding sets to test if the capacity decreases). The proof of Corollary 3 is presented in Section 5.9.

4 Examples

4.1 MDS Graph $\mathcal{M}_{4,3}$

The converse follows immediately from the intersection bound (4). Let us consider the achievability. First, consider the uniform storage case. Let us start from the MDS graph $\mathcal{M}_{3,2}$ and show that $C_u(\mathcal{M}_{3,2}) = 1$ is achievable, which will be used in characterizing $C(\mathcal{M}_{4,3})$. We set

$$Y_{Q_1} = b, Y_{Q_2} = a + b, Y_{Q_3} = 2a + b, \tag{30}$$

where a, b are i.i.d. uniform elements in $\mathbb{F}_3$, so from any two Y_Q, we may recover a and from any single Y_Q, nothing is revealed about a. Noting that $k = \kappa = 1, n = 3, \lambda_1 = \lambda_2 = \lambda_3 = 1$, we apply Theorem 2 to obtain the desired quantum code. Thus, $C_u(\mathcal{M}_{3,2}) \geq 1$.

Next we proceed to $\mathcal{M}_{4,3}$ and show that $C_u(\mathcal{M}_{4,3}) = 2$ is achievable. We set

$$Y_{Q_1} = b, Y_{Q_2} = a_1 + b, Y_{Q_3} = a_2 + b, Y_{Q_4} = a_1 + a_2 + b, \tag{31}$$

where a_1, a_2, b are i.i.d. uniform elements in $\mathbb{F}_3$. Note that from any three Y_Q, we can recover $\boldsymbol{a} = (a_1, a_2)$ and from any single Y_Q, nothing is revealed about $\boldsymbol{a} = (a_1, a_2)$. Noting that $k = 2, \kappa = 1$, and applying Theorem 2, produces the quantum code. Thus, $C_u(\mathcal{M}_{4,3}) \geq 2$.

Next, consider the non-uniform storage case. We show that $C(\mathcal{M}_{4,3}) = \lambda_1 + \lambda_2$ is achievable. Assume λ_1, λ_2 are positive integers (the case of arbitrary real numbers will be treated in the general proof in Section 5.5). As $C_u(\mathcal{M}_{4,3}) \geq 2$, we are able to store a quantum message $Q_0(1)$ of size $\lambda_0(1) = 2\lambda_1$ qudits in $\mathcal{M}_{4,3}$ while utilizing λ_1 qudits of storage from each $Q_i, i \in [4]$. Now there remain unused 0 qudits in Q_1, $\lambda_2 - \lambda_1$ qudits in Q_2, $\lambda_3 - \lambda_1$ qudits in Q_3, $\lambda_4 - \lambda_1$ qudits in Q_4. Recall that $\lambda_1 \leq \lambda_2 \leq \lambda_3 \leq \lambda_4$, and the storage in Q_1 is fully utilized. We now view Q_2, Q_3, Q_4 as an $\mathcal{M}_{3,2}$ MDS graph in order to store another quantum message $Q_0(2)$. It is important to note that the original $\mathcal{M}_{4,3}$ MDS constraint with storage node set $\{Q_1, Q_2, Q_3, Q_4\}$ ensures that any 3 surviving (unerased) Q_i from Q_1, Q_2, Q_3, Q_4 will contain at least two of Q_2, Q_3, Q_4, and the $\mathcal{M}_{3,2}$ MDS graph with storage node set $\{Q_2, Q_3, Q_4\}$ guarantees the quantum message $Q_0(2)$ can be perfectly recovered. As the uniform storage capacity $C_u(\mathcal{M}_{3,2}) \geq 1$, we are able to store the quantum message $Q_0(2)$ of size $\lambda_0(2) = \lambda_2 - \lambda_1$ qudits in $\mathcal{M}_{3,2}$ by utilizing $\lambda_2 - \lambda_1$ qudits of storage from each of Q_2, Q_3, Q_4. After this step, Q_2 is fully utilized, Q_3 is left with $\lambda_3 - \lambda_2$ qudits, and Q_4 is left with $\lambda_4 - \lambda_2$ qudits. These remaining qudits are not used. Overall we have stored quantum message $Q_0 = Q_0(1)Q_0(2)$ of size $\lambda_0 = \lambda_0(1) + \lambda_0(2) = (2\lambda_1) + (\lambda_2 - \lambda_1) = \lambda_1 + \lambda_2$ qudits over the MDS graph $\mathcal{M}_{4,3}$ where each storage node $Q_i, i \in [4]$ has size λ_i qudits. Thus, we have shown $C(\mathcal{M}_{4,3}) \geq \lambda_1 + \lambda_2$, as desired.

4.2 Wheel Graph $\mathcal{W}_4$

We show that $C(\mathcal{W}_4) = \min\left(\lambda_1, \lambda_2, \frac{\lambda_1+\lambda_2}{3}\right)$. From this $C_u(\mathcal{W}_4) = \frac{2}{3}$ follows because uniform storage corresponds to $\lambda_1 = \lambda_2 = 1$. The converse and achievability proofs are presented sequentially.

Converse: Since the problem formulation (1) requires perfect recovery for any pure state of RQ_0, for the converse bound let us consider the case where Q_0 is maximally entangled with the reference R. As every CPTP map has an isometric (unitary) extension, let us assume without loss of generality that the encoder is a *unitary* transformation that maps Q_0 and ancilla qudits to $Q_1Q_2Q_3Q_4Q_5$. The artificial system Q_5 is included as the purifying system. This allows the possibility that $RQ_1Q_2Q_3Q_4$ is mixed, while $RQ_1Q_2Q_3Q_4Q_5$ is pure. Note that Q_5 is not included in any decoding set.

Since $RQ_1Q_2Q_3Q_4Q_5$ is pure, and $I(R; Q_3, Q_4, Q_5) = 0$ (because $\{Q_1, Q_2\}$ is a decoding set, refer to (73) for a proof), we have

$$H(R, Q_3, Q_4, Q_5) = H(Q_1, Q_2) \tag{32}$$

$$\overset{(73)}{\implies} H(R) + H(Q_3, Q_4, Q_5) \leq H(Q_1) + H(Q_2). \tag{33}$$

Similarly,

$$H(R) + H(Q_2, Q_4, Q_5) \leq H(Q_1) + H(Q_3) \tag{34}$$

$$\overset{(33)+(34)}{\implies} 2H(R) + H(Q_2, Q_3, Q_4, Q_5) + H(Q_4, Q_5) \leq 2H(Q_1) + H(Q_2) + H(Q_3) \tag{35}$$

$$\implies 2H(R) + H(R, Q_1) + H(Q_4) + H(Q_5 \mid Q_4) \leq 2H(Q_1) + H(Q_2) + H(Q_3) \tag{36}$$

$$\implies 3H(R) + H(Q_4) + H(Q_5 \mid Q_4) \leq H(Q_1) + H(Q_2) + H(Q_3), \tag{37}$$

and similarly,

$$3H(R) + H(Q_3) + H(Q_5 \mid Q_3) \leq H(Q_1) + H(Q_2) + H(Q_4). \tag{38}$$

Here (34) follows symmetrically from (33) as $\{Q_1, Q_3\}$ is also a decoding set; strong sub-additivity is used to obtain (35); (36) follows from the fact that $RQ_1Q_2Q_3Q_4Q_5$ is pure so that $H(Q_2, Q_3, Q_4, Q_5) = H(R, Q_1)$; (37) is due to the fact that $H(R, Q_1) = H(R) + H(Q_1)$ as $\{Q_2, Q_3, Q_4\}$ is a decoding set so that from (73), $I(R; Q_1) = 0$; and (38) follows similarly from (37) as we may switch Q_3 and Q_4.

Adding (37), (38) and applying weak monotonicity, $H(A \mid B) + H(A \mid C) \geq 0$ with $(A, B, C) = (Q_5, Q_4, Q_3)$, we obtain the following bound (where Q_5 disappears).

$$\begin{aligned}
6H(R) + H(Q_3) + H(Q_4) &\leq 2H(Q_1) + 2H(Q_2) + H(Q_3) + H(Q_4) && (39)\\
\implies H(R) &\leq \frac{H(Q_1) + H(Q_2)}{3} && (40)\\
\implies \kappa\lambda_0 = H(R) \leq \frac{H(Q_1) + H(Q_2)}{3} &\leq \frac{\log_q |Q_1| + \log_q |Q_2|}{3} = \kappa\frac{\lambda_1 + \lambda_2}{3} && (41)\\
\implies C(\mathcal{W}_4) = \sup \lambda_0 &\leq \frac{\lambda_1 + \lambda_2}{3}. && (42)
\end{aligned}$$

Achievability: We first present two component codes that will be used later.

1. $\lambda_0 = 1$ code for storage graph $\mathcal{W}_4$ with $(\lambda_1, \lambda_2, \lambda_3, \lambda_4) = (2, 1, 1, 1)$.

   Let $\kappa = 1$ and $q > 9$ be any prime number. Use the following classical secure storage code.

   $$Y_{Q_1} = (b_1, b_2),\ Y_{Q_2} = a + b_1 + b_2, \tag{43}$$
   $$Y_{Q_3} = a + 2b_1 + 3b_2,\ Y_{Q_4} = a + 4b_1 + 9b_2, \tag{44}$$

   where a, b_1, b_2 are i.i.d. uniform elements in $\mathbb{F}_q$. It is readily verified that the decoding constraint (6) and the security constraint (7) are satisfied, so Theorem 2 produces the claimed quantum code.

2. $\lambda_0 = 1$ code for storage graph $\mathcal{W}_4$ with $(\lambda_1, \lambda_2, \lambda_3, \lambda_4) = (1, 2, 2, 2)$.

   Let $\kappa = 1$ and q be any prime. Use the following classical (structured) secure storage code.

   $$Y_{Q_1} = b_1,\ Y_{Q_2} = (a + b_1, b_2), \tag{45}$$
   $$Y_{Q_3} = (a + b_1, b_3),\ Y_{Q_4} = (a + b_1, a + b_2 + b_3), \tag{46}$$

   where a, b_1, b_2, b_3 are i.i.d. uniform elements in $\mathbb{F}_q$. It is straightforward to verify (6) and (7) hold. An interesting aspect of this code is that $Y_{Q_2}, Y_{Q_3}, Y_{Q_4}$ contain the same element $a + b_1$, inspired by noise alignment (same noise as in Y_{Q_1}) and signal alignment principles [26, 27, 28, 29].

Next we show how to use the above two component codes to achieve $C(\mathcal{W}_4) = \min\left(\lambda_1, \lambda_2, \frac{\lambda_1+\lambda_2}{3}\right)$. There are three cases. Choose a prime $q > 9$ so that both component codes are defined. Since rationals are dense over the reals, it suffices to consider rational λ_1, λ_2. Moreover, since the scaling

factor κ can be chosen freely, there is no loss of generality in the assumption that λ_1, λ_2, and the number of qudits used below (i.e., $\lambda_0(1) = (2\lambda_1 - \lambda_2)/3$ in (47), $\lambda_0(2) = (2\lambda_2 - \lambda_1)/3$ in (48)) are *integers*.

1. When $\lambda_1 \leq \lambda_2/2$, $\min\left(\lambda_1, \lambda_2, \frac{\lambda_1+\lambda_2}{3}\right) = \lambda_1$. Use the second component code to store λ_1 qudits of Q_0 in (Q_1, Q_2, Q_3, Q_4) while utilizing storage in the amounts $(\lambda_1, 2\lambda_1, 2\lambda_1, 2\lambda_1)$ qudits, respectively. Let us verify that the number of qudits utilized in Q_i is not greater than the size of Q_i. This is so because $\lambda_1 \leq \lambda_2/2$ and $\lambda_2 \leq \lambda_3 \leq \lambda_4$. So the scheme works.

2. When $\lambda_2/2 \leq \lambda_1 \leq 2\lambda_2$, $\min\left(\lambda_1, \lambda_2, \frac{\lambda_1+\lambda_2}{3}\right) = \frac{\lambda_1+\lambda_2}{3}$.

   Use the first component code to store $\lambda_0(1) = (2\lambda_1 - \lambda_2)/3 \geq 0$ qudits of Q_0 in (Q_1, Q_2, Q_3, Q_4) by utilizing $(2\lambda_0(1), \lambda_0(1), \lambda_0(1), \lambda_0(1))$ qudits of storage. (47)

   Use the second component code to store $\lambda_0(2) = (2\lambda_2 - \lambda_1)/3 \geq 0$ qudits of Q_0 in (Q_1, Q_2, Q_3, Q_4) by utilizing $(\lambda_0(2), 2\lambda_0(2), 2\lambda_0(2), 2\lambda_0(2))$ qudits of storage. (48)

   In total, we have stored $\lambda_0 = \lambda_0(1) + \lambda_0(2) = (\lambda_1 + \lambda_2)/3$ qudits of Q_0 in (Q_1, Q_2, Q_3, Q_4) while utilizing $(2\lambda_0(1)+\lambda_0(2), \lambda_0(1)+2\lambda_0(2), \lambda_0(1)+2\lambda_0(2), \lambda_0(1)+2\lambda_0(2))$ qudits of storage. We verify that the amount of storage utilized by the scheme from the storage node Q_i is not greater than the size of Q_i, because,

   $$2\lambda_0(1) + \lambda_0(2) = \lambda_1, \tag{49}$$

   $$\lambda_0(1) + 2\lambda_0(2) = \lambda_2 \leq \lambda_3 \leq \lambda_4. \tag{50}$$

   So the scheme works.

3. When $2\lambda_2 \leq \lambda_1$, $\min\left(\lambda_1, \lambda_2, \frac{\lambda_1+\lambda_2}{3}\right) = \lambda_2$. Use the first component code to store λ_2 qudits of Q_0 in (Q_1, Q_2, Q_3, Q_4) by utilizing storage in the amounts $(2\lambda_2, \lambda_2, \lambda_2, \lambda_2)$ qudits, respectively. The utilized storage in Q_i is not greater than the size of Q_i because $2\lambda_2 \leq \lambda_1$ and $\lambda_2 \leq \lambda_3 \leq \lambda_4$. So the scheme works.

4.2.1 From Classical to Quantum: Illustration of Theorem 2

We take the classical code (45), (46) as an example to illustrate the translation to a quantum code in Theorem 2.

First, consider the quantum encoding procedure. Set $\lambda_0 = \kappa = 1$ and $q = 2$, i.e., Q_0 has 1 qubit. We only consider the encoding of Q_0 and defer the inclusion of the entangled reference system to the general proof of Theorem 2 in Section 5.2. It suffices to consider the encoding and decoding of the computational basis $|a\rangle, a = 0, 1$ (as the coding operations are linear, the code for any superposition of $|0\rangle$, $|1\rangle$ is also implied).

$$|a\rangle \quad \rightsquigarrow \quad \sum_{\boldsymbol{b}} |a\mathbf{A} + \boldsymbol{b}\mathbf{B}\rangle = \frac{1}{\sqrt{2^3}} \sum_{b_1,b_2,b_3 \in \mathbb{F}_2} |b_1\rangle_{Q_1} |a + b_1, b_2\rangle_{Q_2} |a + b_1, b_3\rangle_{Q_3} |a + b_1, a + b_2 + b_3\rangle_{Q_4}, \tag{51}$$

where $(\lambda_1, \lambda_2, \lambda_3, \lambda_4) = (1, 2, 2, 2)$, i.e., Q_1, Q_2, Q_3, Q_4 contain 1 qubit, 2 qubits, 2 qubits, and 2 qubits respectively in the final output (corresponding to the 4 kets above).

Second, consider the quantum decoding procedure.

1. Consider decoding set $\{Q_1, Q_2\}$. The decoding sets $\{Q_1, Q_3\}, \{Q_1, Q_4\}$ are similar.

$$\frac{1}{\sqrt{2^3}} \sum_{b_1,b_2,b_3 \in \mathbb{F}_2} |b_1\rangle |a+b_1, b_2\rangle |a+b_1, b_3\rangle |a+b_1, a+b_2+b_3\rangle \tag{52}$$

$$\rightsquigarrow \quad \frac{1}{\sqrt{2^3}} \sum_{b_1,b_2,b_3 \in \mathbb{F}_2} |a\rangle |a+b_1, a+b_2\rangle |a+b_1, b_3\rangle |a+b_1, a+b_2+b_3\rangle \tag{53}$$

(define $a+b_1 = c_1, a+b_2 = c_2, b_3 = c_3$)

$$= \quad \frac{1}{\sqrt{2^3}} \sum_{b_1,b_2,b_3 \in \mathbb{F}_2} |a\rangle |c_1, c_2\rangle |c_1, c_3\rangle |c_1, c_2+c_3\rangle \tag{54}$$

(c_1, c_2, c_3 also takes all values in $\mathbb{F}_2$)

$$= \quad \frac{1}{\sqrt{2^3}} \sum_{c_1,c_2,c_3 \in \mathbb{F}_2} |a\rangle |c_1, c_2\rangle |c_1, c_3\rangle |c_1, c_2+c_3\rangle \tag{55}$$

$$= \quad |a\rangle \frac{1}{\sqrt{2^3}} \sum_{c_1,c_2,c_3 \in \mathbb{F}_2} |c_1, c_2\rangle |c_1, c_3\rangle |c_1, c_2+c_3\rangle \tag{56}$$

so that $|a\rangle$ is unentangled from the rest of the codeword and recovered with no error. Note that the storage nodes Q_3, Q_4 that are outside the considered decoding set are not touched in decoding.

2. Consider decoding set $\{Q_2, Q_3, Q_4\}$.

$$\frac{1}{\sqrt{2^3}} \sum_{b_1,b_2,b_3 \in \mathbb{F}_2} |b_1\rangle |a+b_1, b_2\rangle |a+b_1, b_3\rangle |a+b_1, a+b_2+b_3\rangle \tag{57}$$

$$\rightsquigarrow \quad \frac{1}{\sqrt{2^3}} \sum_{b_1,b_2,b_3 \in \mathbb{F}_2} |b_1\rangle |a+b_1, b_2\rangle |a+b_1, b_3\rangle |a+b_1, a\rangle \tag{58}$$

$$\rightsquigarrow \quad \frac{1}{\sqrt{2^3}} \sum_{b_1,b_2,b_3 \in \mathbb{F}_2} |b_1\rangle |b_1, b_2\rangle |b_1, b_3\rangle |b_1, a\rangle \tag{59}$$

$$= \quad \left(\frac{1}{\sqrt{2^3}} \sum_{b_1,b_2,b_3 \in \mathbb{F}_2} |b_1\rangle |b_1, b_2\rangle |b_1, b_3\rangle |b_1\rangle \right) |a\rangle \tag{60}$$

so that $|a\rangle$ is recovered.

4.3 Intersection Graph $\sqcap_{5,3}$

Consider the uniform storage case where $\lambda_i = 1, \forall i$. For the converse, consider the intersection bound (4).

$$C_u(\sqcap_{5,3}) \quad \leq \quad \Lambda\Big(\mathcal{D}(e_1) \cap \mathcal{D}(e_2)\Big) = \Lambda\left(\left\{Q_{\overline{\mathcal{S}}} : 1 \in \mathcal{S}, 2 \in \mathcal{S}, \mathcal{S} \in \binom{[5]}{3}\right\}\right) \tag{61}$$

$$= \quad \Lambda\left(\{Q_{123}, Q_{124}, Q_{125}\}\right) = \binom{5-2}{3-2} = 3, \tag{62}$$

where $Q_{\overline{\{i,j,k\}}}$ is abbreviated as Q_{ijk} to simplify the notation.

For the achievability, we use Theorem 2 and translate from the following classical (structured) secure storage code. Set $k = 3, \kappa = 1$ and for this example, think of q as a sufficiently large prime power (explicit choice will be given in the general proof in Section 5.7). Set

$$\begin{aligned}
&Y_{Q_{123}}, Y_{Q_{124}}, Y_{Q_{125}}, Y_{Q_{134}}, Y_{Q_{135}}, Y_{Q_{145}} \text{ each as a generic (random linear)} \\
&\quad \text{combination of } a_1, a_2, a_3, b_1, b_2, b_3, && (63)\\
&Y_{Q_{234}} = Y_{Q_{123}} - Y_{Q_{124}} + Y_{Q_{134}}, && (64)\\
&Y_{Q_{235}} = Y_{Q_{123}} - Y_{Q_{125}} + Y_{Q_{135}}, && (65)\\
&Y_{Q_{245}} = Y_{Q_{124}} - Y_{Q_{125}} + Y_{Q_{145}}, && (66)\\
&Y_{Q_{345}} = Y_{Q_{134}} - Y_{Q_{135}} + Y_{Q_{145}}, && (67)
\end{aligned}$$

where $a_1, a_2, a_3, b_1, b_2, b_3$ are i.i.d. uniform elements in $\mathbb{F}_q$. The storage nodes in $\mathcal{D}(e_1)$ (i.e., storage nodes whose label contains '1') are each assigned a generic linear combination of $a_1, a_2, a_3, b_1, b_2, b_3$ (refer to (63)). The storage nodes that are not in $\mathcal{D}(e_1)$ (i.e., those whose label does not contain '1') are assigned linear combinations of those in $\mathcal{D}(e_1)$ according to an alternating sign structure as specified above. For example, consider $Y_{Q_{234}}$ in (64), which is set as a linear combination of $Y_{Q_\mathcal{S}}$ where $\mathcal{S}$ are all sets obtained by replacing one of the elements of $\{2, 3, 4\}$ with '1'.

Next, we use a dimension counting argument to show that the decoding constraint (6) and the security constraint (7) are satisfied. First, consider (6). From $\mathcal{D}(e_1)$, (63) shows that $\{Y_Q : Q \in \mathcal{D}(e_1)\}$ contains 6 generic linear combinations of $a_1, a_2, a_3, b_1, b_2, b_3$ and thus may be set so that a_1, a_2, a_3 can be recovered. $\mathcal{D}(e_i), i \in [2:5]$ are similar, so let us consider $\mathcal{D}(e_2)$. From (64) - (66),

$$(Y_{Q_{123}}, Y_{Q_{124}}, Y_{Q_{125}}, Y_{Q_{234}}, Y_{Q_{235}}, Y_{Q_{245}}) \overset{\text{invertible}}{\longleftrightarrow} (Y_{Q_{123}}, Y_{Q_{124}}, Y_{Q_{125}}, Y_{Q_{134}}, Y_{Q_{135}}, Y_{Q_{145}}) \tag{68}$$

so that $\mathcal{D}(e_2)$ recovers a_1, a_2, a_3 as well.

Second, consider (7). We wish to show that nothing is revealed about a_1, a_2, a_3 from $\mathcal{Y}_{\mathcal{D}^c(e_i)}$ where $\mathcal{D}^c(e_i)$ contains $\binom{5}{3} - \binom{4}{2} = 4$ linear combinations of $a_1, a_2, a_3, b_1, b_2, b_3$. This is guaranteed by ensuring the 4 linear combinations in $\mathcal{Y}_{\mathcal{D}^c(e_i)}$ occupy 3 dimensions and the 3 dimensions are fully covered by b_1, b_2, b_3 (so that a_1, a_2, a_3 are perfectly protected). We discuss next how this is guaranteed by the design in (63) - (67).

Let us start from the simpler case for $\mathcal{D}^c(e_i)$ when $i \in [2:5]$. As the cases are similar, we consider $\mathcal{D}^c(e_2) = \{Q_{134}, Q_{135}, Q_{145}, Q_{345}\}$ for concreteness. From (67), we see that $Y_{Q_{345}}$ is a function of $Y_{Q_{134}}, Y_{Q_{135}}, Y_{Q_{145}}$ so that indeed $\mathcal{Y}_{\mathcal{D}^c(e_2)} = \{Y_{Q_{134}}, Y_{Q_{135}}, Y_{Q_{145}}, Y_{Q_{345}}\}$ contains at most 3 dimensions, $Y_{Q_{134}}, Y_{Q_{135}}, Y_{Q_{145}}$, wherein the b symbols lie in generic spaces so that indeed (7) can be satisfied (a detailed proof is deferred to Section 5.7).

We are now left with only $\mathcal{D}^c(e_1) = \{Q_{234}, Q_{235}, Q_{245}, Q_{345}\}$. Indeed, this is the most interesting case. From the surface, it might seem that $\mathcal{Y}_{\mathcal{D}^c(e_1)} = \{Y_{Q_{234}}, Y_{Q_{235}}, Y_{Q_{245}}, Y_{Q_{345}}\}$ contains 4 independent dimensions. However, this is not the case, as we show that, perhaps surprisingly, $Y_{Q_{345}}$ is a linear combination of $Y_{Q_{234}}, Y_{Q_{235}}, Y_{Q_{245}}$ as follows,

$$\begin{aligned}
& Y_{Q_{234}} - Y_{Q_{235}} + Y_{Q_{245}} \\
\overset{(64)-(66)}{=}\ & (Y_{Q_{123}} - Y_{Q_{124}} + Y_{Q_{134}}) - (Y_{Q_{123}} - Y_{Q_{125}} + Y_{Q_{135}}) + (Y_{Q_{124}} - Y_{Q_{125}} + Y_{Q_{145}}) && (69)\\
=\ & Y_{Q_{134}} - Y_{Q_{135}} + Y_{Q_{145}} \overset{(67)}{=} Y_{Q_{345}}. && (70)
\end{aligned}$$

Thus, $\mathcal{Y}_{\mathcal{D}^c(e_1)}$ has only 3 dimensions as desired (as a result of 'alignment') and $Y_{Q_{234}}, Y_{Q_{235}}, Y_{Q_{245}}$ contain generic linear combinations of b_1, b_2, b_3 so that (7) can be satisfied.

To summarize, non-trivial linear dependence exists by design in the above code construction. It is noteworthy that related alignment structures have appeared in the context of private information retrieval (private computation) [30], coded caching (for function retrieval) [31], and secure aggregation [32, 33].

5 Proofs

5.1 Proof of Theorem 1

Let us start with a lemma on the properties of quantum entropy and mutual information that will be used in the proof of Theorem 1. Unless stated explicitly otherwise, the quantum information measure terms are with respect to the joint state of the reference system R and all quantum storage nodes $Q_1, \cdots, Q_N$, denoted as $\rho_{RQ_1\cdots Q_N}$. Recall from (1) that our problem formulation requires perfect recovery for *every* pure state of RQ_0, so in particular perfect recovery is required for a maximally entangled state RQ_0 where Q_0 is maximally mixed, i.e., $H(R,Q_0)_{|\varphi\rangle_{RQ_0}} = 0$ and $H(R) = H(Q_0)_{|\varphi\rangle_{RQ_0}} = \log_q |Q_0| = \kappa\lambda_0$. In what follows, we assume RQ_0 is maximally entangled.

Lemma 1. *For a storage graph $\mathcal{G} = ((\lambda_1, \cdots, \lambda_N), \mathcal{E})$, and maximally entangled RQ_0, we have*

$$\textit{(Perfect recovery)} \qquad I(R;\mathcal{D}(e)) = 2\kappa\lambda_0, \quad \forall e \in \mathcal{E}, \tag{71}$$

$$\textit{(Monogamy of entanglement)} \qquad I(R;\mathcal{Q}_1) + I(R;\mathcal{Q}_2) \le 2\kappa\lambda_0, \quad \forall \mathcal{Q}_1 \cap \mathcal{Q}_2 = \emptyset, \mathcal{Q}_1, \mathcal{Q}_2 \subset \mathcal{Q}(\mathcal{G}), \tag{72}$$

$$\textit{(No-cloning)} \qquad I(R;\mathcal{D}^c(e)) = 0, \quad \forall e \in \mathcal{E}. \tag{73}$$

Proof: (71) was first proved by Schumacher and Nielsen [34]. Intuitively, it says that as the original quantum message Q_0 can be perfectly recovered, then $\mathcal{D}(e)$ must contain all entanglement with the reference system R (note that $I(R;Q_0)_{|\varphi\rangle_{RQ_0}} = 2\kappa\lambda_0$). A short proof based on quantum data processing inequality is as follows. For any $e \in \mathcal{E}$, after passing through the decoding mapping, the mutual information cannot increase, i.e.,

$$I(R;\mathcal{D}(e)) \ge I(R;\widehat{Q}_0)_{|\varphi\rangle_{R\widehat{Q}_0}} = I(R;Q_0)_{|\varphi\rangle_{RQ_0}} = 2H(R), \tag{74}$$

as decoding is perfect, i.e., $|\varphi\rangle_{R\widehat{Q}_0} = |\varphi\rangle_{RQ_0}$. Combining with the fact that $I(R;\mathcal{D}(e)) \le 2H(R) = 2\kappa\lambda_0$ completes the proof of (71).

(72), which we refer to as monogamy of entanglement, is a simple consequence of weak monotonicity.

$$I(R;\mathcal{Q}_1) + I(R;\mathcal{Q}_2) = 2H(R) - \big(\underbrace{H(R \mid \mathcal{Q}_1) + H(R \mid \mathcal{Q}_2)}_{\ge 0}\big) \tag{75}$$

$$\le 2H(R) = 2\kappa\lambda_0. \tag{76}$$

(73), which we refer to as no-cloning, follows by combining (71) and (72) (setting $\mathcal{Q}_1 = \mathcal{D}(e)$ and $\mathcal{Q}_2 = \mathcal{D}^c(e)$) and using the property that quantum mutual information is non-negative. Intuitively, (73) says that as the decoding set $\mathcal{D}(e)$ contains all entanglement with R, the complement $\mathcal{D}^c(e)$ and R must be in a product state so that cloning is not possible.

□

Equipped with Lemma 1, we now prove the intersection bound (4). Consider two decoding sets $\mathcal{D}(e_i), \mathcal{D}(e_j)$, where $e_i, e_j \in \mathcal{E}$.

$$
\begin{aligned}
2\kappa\lambda_0 &\overset{(71)}{=} I(R;\mathcal{D}(e_i)) && (77)\\
&= I(R;\mathcal{D}(e_i)\cap\mathcal{D}(e_j),\mathcal{D}(e_i)\setminus\mathcal{D}(e_j)) && (78)\\
&= I(R;\mathcal{D}(e_i)\setminus\mathcal{D}(e_j)) + I(R;\mathcal{D}(e_i)\cap\mathcal{D}(e_j)\mid\mathcal{D}(e_i)\setminus\mathcal{D}(e_j)) && (79)\\
&= \underbrace{I(R;\mathcal{D}^c(e_j))}_{\overset{(73)}{=}0} - \underbrace{I(R;\mathcal{D}^c(e_j)\setminus(\mathcal{D}(e_i)\setminus\mathcal{D}(e_j))\mid\mathcal{D}(e_i)\setminus\mathcal{D}(e_j))}_{\geq 0}\\
&\quad + \underbrace{I(R;\mathcal{D}(e_i)\cap\mathcal{D}(e_j)\mid\mathcal{D}(e_i)\setminus\mathcal{D}(e_j))}_{\leq 2H(\mathcal{D}(e_i)\cap\mathcal{D}(e_j))} && (80)\\
&\leq 2H(\mathcal{D}(e_i)\cap\mathcal{D}(e_j)) && (81)\\
&\leq 2\log_q \Pi_{Q\in\mathcal{D}(e_i)\cap\mathcal{D}(e_j)}|Q| && (82)\\
&= 2\sum_{k:Q_k\in\mathcal{D}(e_i)\cap\mathcal{D}(e_j)} \kappa\lambda_k = 2\kappa\Lambda\Big(\mathcal{D}(e_i)\cap\mathcal{D}(e_j)\Big) && (83)\\
\implies C(\mathcal{G}) &= \sup\lambda_0 \leq \Lambda\Big(\mathcal{D}(e_i)\cap\mathcal{D}(e_j)\Big). && (84)
\end{aligned}
$$

Next we prove the wheel bound (5) as a generalization of the converse bound for the wheel graph $\mathcal{W}_4$ presented in Section 4.2.

Consider the maximally entangled pure state RQ_0, mapped through an isometric extension of the encoding CPTP map to pure state $RQ_1\cdots Q_N Q_{N+1}$, where Q_{N+1} is an artificial purifying system and is not in any decoding set.

Consider any $k\in[2:n-2]$ and $\{\mathcal{Q}_1,\mathcal{Q}_2\},\cdots,\{\mathcal{Q}_1,\mathcal{Q}_k\},\{\mathcal{Q}_1,\mathcal{Q}_{k+1}\},\{\mathcal{Q}_1,\mathcal{Q}_{k+2},\cdots,\mathcal{Q}_n\}$ that each contains a decoding set, so from (73), $I(R;\{\mathcal{Q}_1,\mathcal{Q}_i\}^c)=0, i\in[2:k+2]$. As $RQ_1\cdots Q_NQ_{N+1}$ is pure,

$$
\begin{aligned}
H(R)+H(\mathcal{Q}_3,\mathcal{Q}_4,\cdots,\mathcal{Q}_k,\mathcal{Q}_{k+1},\cdots,\mathcal{Q}_n,Q_{N+1}) &= H(\mathcal{Q}_1,\mathcal{Q}_2) \leq H(\mathcal{Q}_1)+H(\mathcal{Q}_2), && (85)\\
H(R)+H(\mathcal{Q}_2,\mathcal{Q}_4,\cdots,\mathcal{Q}_k,\mathcal{Q}_{k+1},\cdots,\mathcal{Q}_n,Q_{N+1}) &= H(\mathcal{Q}_1,\mathcal{Q}_3) \leq H(\mathcal{Q}_1)+H(\mathcal{Q}_3), && (86)\\
&\vdots\\
H(R)+H(\mathcal{Q}_2,\mathcal{Q}_3,\cdots,\mathcal{Q}_{k-1},\mathcal{Q}_{k+1},\cdots,\mathcal{Q}_n,Q_{N+1}) &= H(\mathcal{Q}_1,\mathcal{Q}_k) \leq H(\mathcal{Q}_1)+H(\mathcal{Q}_k), && (87)\\
H(R)+H(\mathcal{Q}_2,\mathcal{Q}_3,\cdots,\mathcal{Q}_k,\mathcal{Q}_{k+2},\cdots,\mathcal{Q}_n,Q_{N+1}) &= H(\mathcal{Q}_1,\mathcal{Q}_{k+1}) \leq H(\mathcal{Q}_1)+H(\mathcal{Q}_{k+1}), && (88)\\
H(R)+H(\mathcal{Q}_2,\mathcal{Q}_3,\cdots,\mathcal{Q}_k,\mathcal{Q}_{k+1},Q_{N+1}) &= H(\mathcal{Q}_1,\mathcal{Q}_{k+2},\cdots,\mathcal{Q}_n)\\
&\leq H(\mathcal{Q}_1)+H(\mathcal{Q}_{k+2},\cdots,\mathcal{Q}_n). && (89)
\end{aligned}
$$

Adding (85) - (88) and applying strong sub-additivity repeatedly, we obtain

$$
\begin{aligned}
& kH(R)+(k-1)\underbrace{H(\mathcal{Q}_2,\mathcal{Q}_3,\cdots,\mathcal{Q}_k,\mathcal{Q}_{k+1},\cdots,\mathcal{Q}_n,Q_{N+1})}_{=H(R,\mathcal{Q}_1)\overset{(73)}{=}H(R)+H(\mathcal{Q}_1)} + H(\mathcal{Q}_{k+2},\cdots,\mathcal{Q}_n,Q_{N+1})\\
\leq\ & kH(\mathcal{Q}_1)+H(\mathcal{Q}_2)+\cdots+H(\mathcal{Q}_k)+H(\mathcal{Q}_{k+1}) && (90)\\
\implies\ & (2k-1)H(R)+H(\mathcal{Q}_{k+2},\cdots,\mathcal{Q}_n)+H(Q_{N+1}\mid\mathcal{Q}_{k+2},\cdots,\mathcal{Q}_n)\\
\leq\ & H(\mathcal{Q}_1)+H(\mathcal{Q}_2)+\cdots+H(\mathcal{Q}_k)+H(\mathcal{Q}_{k+1}). && (91)
\end{aligned}
$$

Here (90) follows from the fact that $\mathcal{Q}_2 \cup \cdots \cup \mathcal{Q}_n$ contains a decoding set, so $I(R; \mathcal{Q}_1) = 0$ by (73). Adding (85) - (87), (89) and applying strong sub-additivity repeatedly, we have

$$\begin{aligned} & kH(R) + (k-1)\underbrace{H(\mathcal{Q}_2, \mathcal{Q}_3, \cdots, \mathcal{Q}_k, \mathcal{Q}_{k+1}, \cdots, \mathcal{Q}_n, Q_{N+1})}_{=H(R,\mathcal{Q}_1)\overset{(73)}{=}H(R)+H(\mathcal{Q}_1)} + H(\mathcal{Q}_{k+1}, Q_{N+1}) \\ \leq\ & kH(\mathcal{Q}_1) + H(\mathcal{Q}_2) + \cdots + H(\mathcal{Q}_k) + H(\mathcal{Q}_{k+2}, \cdots, \mathcal{Q}_n) \qquad (92) \\ \implies\ & (2k-1)H(R) + H(\mathcal{Q}_{k+1}) + H(Q_{N+1} \mid \mathcal{Q}_{k+1}) \\ \leq\ & H(\mathcal{Q}_1) + H(\mathcal{Q}_2) + \cdots + H(\mathcal{Q}_k) + H(\mathcal{Q}_{k+2}, \cdots, \mathcal{Q}_n). \qquad (93) \end{aligned}$$

Adding (91) and (93) and applying weak monotonicity, we have

$$\begin{aligned} 2(2k-1)H(R) &\leq 2(H(\mathcal{Q}_1) + H(\mathcal{Q}_2) + \cdots + H(\mathcal{Q}_k)) \qquad (94) \\ \implies \kappa\lambda_0 = H(R) &\leq \kappa\frac{\Lambda(\mathcal{Q}_1) + \Lambda(\mathcal{Q}_2) + \cdots + \Lambda(\mathcal{Q}_k)}{2k-1} \qquad (95) \\ \implies C(\mathcal{G}) = \sup\lambda_0 &\leq \frac{\Lambda(\mathcal{Q}_1) + \Lambda(\mathcal{Q}_2) + \cdots + \Lambda(\mathcal{Q}_k)}{2k-1}. \qquad (96) \end{aligned}$$

5.2 Proof of Theorem 2

We are given matrices $\mathbf{A}, \mathbf{B}$ with elements in finite field $\mathbb{F}_q$ that satisfy the conditions in Theorem 2. We show how to use them to design a quantum encoding and decoding scheme as follows.

Quantum Encoding: Set $\kappa\lambda_0 = k$ so that Q_0 has k qudits where each qudit is q-dimensional. Suppose Q_0 is in an arbitrary state with density matrix ω. Without loss of generality, suppose ω has a spectral decomposition $\omega = \sum_i p_i |i\rangle\langle i|$ and a purification $|\varphi\rangle_{RQ_0} = \sum_i \sqrt{p_i}\,|i\rangle\,|i\rangle$. The encoding proceeds as follows.

$$\begin{aligned} |\varphi\rangle_{RQ_0} &= \sum_i \sqrt{p_i}\,|i\rangle\,|i\rangle \qquad (97) \\ &= \sum_{a_1,\cdots,a_k \in \mathbb{F}_q} \sqrt{p_{a_1,\cdots,a_k}}\,|a_1, \cdots, a_k\rangle\,|a_1, \cdots, a_k\rangle \qquad (98) \\ &= \sum_{\boldsymbol{a} \in \mathbb{F}_q^{1\times k}} \sqrt{p_{\boldsymbol{a}}}\,|\boldsymbol{a}\rangle\,|\boldsymbol{a}\rangle \qquad (99) \\ &\rightsquigarrow \sum_{\boldsymbol{a}} \sqrt{p_{\boldsymbol{a}}}\,|\boldsymbol{a}\rangle\,|\boldsymbol{a}\mathbf{A}\rangle \qquad (100) \\ &\rightsquigarrow \sum_{\boldsymbol{a}} \sqrt{p_{\boldsymbol{a}}}\,|\boldsymbol{a}\rangle\,|\boldsymbol{a}\mathbf{A}\rangle\,\frac{1}{\sqrt{q^\delta}} \sum_{\boldsymbol{b} \in \mathbb{F}_q^{1\times\delta}} |\boldsymbol{b}\rangle \qquad (101) \\ &\rightsquigarrow \sum_{\boldsymbol{a}} \sqrt{p_{\boldsymbol{a}}}\,|\boldsymbol{a}\rangle_R\,\frac{1}{\sqrt{q^\delta}} \sum_{\boldsymbol{b}} |\boldsymbol{a}\mathbf{A} + \boldsymbol{b}\mathbf{B}\rangle_{Q_1\cdots Q_N} \qquad (102) \end{aligned}$$

where (100) is an isometric map (which can be extended to unitary) because $\text{rank}(\mathbf{A}) = k$, i.e., $\mathbf{A}$ has full rank; (102) is an isometric map because $\text{rank}(\mathbf{A}; \mathbf{B}) = k + \delta$ so that from $\boldsymbol{a}\mathbf{A} + \boldsymbol{b}\mathbf{B}$, one can recover $\boldsymbol{a}, \boldsymbol{b}$. Note that the encoding of Q_0 to $Q_1, \cdots Q_N$ does not touch R, i.e., R goes through an identity map and $RQ_1 \cdots Q_N$ ends up in a pure state. The encoding is now complete.

Quantum Decoding: Consider any decoding set $\mathcal{D}(e)$, $e \in \mathcal{E}$ (abbreviated as $\mathcal{D}$ in this section where e is fixed and omitted). For the quantum decoding procedure, we will perform a change of basis operation for $(\mathbf{A};\mathbf{B})$. To this end, suppose $\langle(\mathbf{A}_{\mathcal{D}};\mathbf{B}_{\mathcal{D}})\rangle \cap \langle(\mathbf{A}_{\mathcal{D}^c};\mathbf{B}_{\mathcal{D}^c})\rangle$ has dimension δ_1. Suppose $\text{rank}(\mathbf{A}_{\mathcal{D}};\mathbf{B}_{\mathcal{D}}) = k+\delta_1+\delta_2$ where $\delta_1 \geq 0, \delta_2 \geq 0$ as $\langle \mathbf{I}_{k\times k}; \mathbf{0}_{\delta\times k}\rangle$ is a subspace of $\langle \mathbf{A}_{\mathcal{D}};\mathbf{B}_{\mathcal{D}}\rangle$ (refer to (15)) and $\langle \mathbf{I}_{k\times k}; \mathbf{0}_{\delta\times k}\rangle$ has no intersection with $\langle \mathbf{A}_{\mathcal{D}^c};\mathbf{B}_{\mathcal{D}^c}\rangle$ (refer to (17)); and $\text{rank}(\mathbf{A}_{\mathcal{D}^c};\mathbf{B}_{\mathcal{D}^c}) = \delta_1+\delta_3$ where $\delta_1+\delta_2+\delta_3 = \delta$ as $\text{rank}(\mathbf{A};\mathbf{B}) = k+\delta$. We may now find matrices $\mathbf{A}_{\mathcal{D}_1}, \mathbf{A}_{\mathcal{D}_2}, \mathbf{A}_{\mathcal{D}_3}, \mathbf{B}_{\mathcal{D}_1}, \mathbf{B}_{\mathcal{D}_2}, \mathbf{B}_{\mathcal{D}_3}$ (where $\mathbf{A}_{\mathcal{D}_i}$ has k rows and $\mathbf{B}_{\mathcal{D}_i}$ has δ rows) such that

1. $(\mathbf{A}_{\mathcal{D}_1};\mathbf{B}_{\mathcal{D}_1}) \in \mathbb{F}_q^{(k+\delta)\times\delta_1}$ is a basis of $\langle(\mathbf{A}_{\mathcal{D}};\mathbf{B}_{\mathcal{D}})\rangle \cap \langle(\mathbf{A}_{\mathcal{D}^c};\mathbf{B}_{\mathcal{D}^c})\rangle$,
2. $(\mathbf{A}_{\mathcal{D}_2};\mathbf{B}_{\mathcal{D}_2}) \in \mathbb{F}_q^{(k+\delta)\times\delta_2}$ and $((\mathbf{I}_{k\times k};\mathbf{0}_{\delta\times k}),(\mathbf{A}_{\mathcal{D}_1};\mathbf{B}_{\mathcal{D}_1}),(\mathbf{A}_{\mathcal{D}_2};\mathbf{B}_{\mathcal{D}_2}))$ is a basis of $\langle \mathbf{A}_{\mathcal{D}};\mathbf{B}_{\mathcal{D}}\rangle$,
3. $(\mathbf{A}_{\mathcal{D}_3};\mathbf{B}_{\mathcal{D}_3}) \in \mathbb{F}_q^{(k+\delta)\times\delta_3}$ and $((\mathbf{A}_{\mathcal{D}_1};\mathbf{B}_{\mathcal{D}_1}),(\mathbf{A}_{\mathcal{D}_3};\mathbf{B}_{\mathcal{D}_3}))$ is a basis of $\langle \mathbf{A}_{\mathcal{D}^c};\mathbf{B}_{\mathcal{D}^c}\rangle$,
4. $\Big((\mathbf{I}_{k\times k};\mathbf{0}_{\delta\times k}),(\mathbf{A}_{\mathcal{D}_1};\mathbf{B}_{\mathcal{D}_1}),(\mathbf{A}_{\mathcal{D}_2};\mathbf{B}_{\mathcal{D}_2}),(\mathbf{A}_{\mathcal{D}_3};\mathbf{B}_{\mathcal{D}_3})\Big)$ is a basis of $\langle \mathbf{A};\mathbf{B}\rangle = \langle \mathbf{I}_{(k+\delta)\times(k+\delta)}\rangle$ and $(\mathbf{B}_{\mathcal{D}_1},\mathbf{B}_{\mathcal{D}_2},\mathbf{B}_{\mathcal{D}_3})$ is a basis of $\langle \mathbf{B}\rangle = \langle \mathbf{I}_{\delta\times\delta}\rangle$.

Then define

$$\boldsymbol{b}'_1 = \boldsymbol{a}\mathbf{A}_{\mathcal{D}_1} + \boldsymbol{b}\mathbf{B}_{\mathcal{D}_1} \in \mathbb{F}_q^{1\times\delta_1}, \tag{103}$$
$$\boldsymbol{b}'_2 = \boldsymbol{a}\mathbf{A}_{\mathcal{D}_2} + \boldsymbol{b}\mathbf{B}_{\mathcal{D}_2} \in \mathbb{F}_q^{1\times\delta_2}, \tag{104}$$
$$\boldsymbol{b}'_3 = \boldsymbol{a}\mathbf{A}_{\mathcal{D}_3} + \boldsymbol{b}\mathbf{B}_{\mathcal{D}_3} \in \mathbb{F}_q^{1\times\delta_3}. \tag{105}$$

As $(\mathbf{B}_{\mathcal{D}_1},\mathbf{B}_{\mathcal{D}_2},\mathbf{B}_{\mathcal{D}_3})$ is a basis of $\langle \mathbf{I}_{\delta\times\delta}\rangle$, the product $\boldsymbol{b}(\mathbf{B}_{\mathcal{D}_1},\mathbf{B}_{\mathcal{D}_2},\mathbf{B}_{\mathcal{D}_3})$ is invertible to $\boldsymbol{b} \in \mathbb{F}_q^{1\times\delta}$, and then

$$\boldsymbol{b}' \triangleq (\boldsymbol{b}'_1,\boldsymbol{b}'_2,\boldsymbol{b}'_3) \text{ is invertible to } \boldsymbol{b} \in \mathbb{F}_q^{1\times\delta} \text{ for any fixed } \boldsymbol{a}. \tag{106}$$

We are now ready to proceed to decoding. The state for $RQ_1\cdots Q_N = R\mathcal{D}\mathcal{D}^c$ is expressed as follows.

$$\sum_{\boldsymbol{a}} \sqrt{p_{\boldsymbol{a}}}\,|\boldsymbol{a}\rangle \frac{1}{\sqrt{q^\delta}} \sum_{\boldsymbol{b}} |\boldsymbol{a}\mathbf{A}+\boldsymbol{b}\mathbf{B}\rangle \tag{107}$$
$$= \sum_{\boldsymbol{a}} \sqrt{p_{\boldsymbol{a}}}\,|\boldsymbol{a}\rangle \frac{1}{\sqrt{q^\delta}} \sum_{\boldsymbol{b}} |\boldsymbol{a}\mathbf{A}_{\mathcal{D}}+\boldsymbol{b}\mathbf{B}_{\mathcal{D}}\rangle\,|\boldsymbol{a}\mathbf{A}_{\mathcal{D}^c}+\boldsymbol{b}\mathbf{B}_{\mathcal{D}^c}\rangle \tag{108}$$
$$\rightsquigarrow \sum_{\boldsymbol{a}} \sqrt{p_{\boldsymbol{a}}}\,|\boldsymbol{a}\rangle \frac{1}{\sqrt{q^\delta}} \sum_{\boldsymbol{b}} |\boldsymbol{a}\rangle\,|\boldsymbol{b}'_1\rangle\,|\boldsymbol{b}'_2\rangle\,|l(\boldsymbol{b}'_1,\boldsymbol{b}'_2)\rangle\,|l(\boldsymbol{b}'_1,\boldsymbol{b}'_3)\rangle \tag{109}$$
$$= \sum_{\boldsymbol{a}} \sqrt{p_{\boldsymbol{a}}}\,|\boldsymbol{a}\rangle \frac{1}{\sqrt{q^\delta}} \sum_{\boldsymbol{b}'} |\boldsymbol{a}\rangle\,|\boldsymbol{b}'_1\rangle\,|\boldsymbol{b}'_2\rangle\,|l(\boldsymbol{b}'_1,\boldsymbol{b}'_2)\rangle\,|l(\boldsymbol{b}'_1,\boldsymbol{b}'_3)\rangle \tag{110}$$
$$= \sum_{\boldsymbol{a}} \sqrt{p_{\boldsymbol{a}}}\,|\boldsymbol{a}\rangle\,|\boldsymbol{a}\rangle \frac{1}{\sqrt{q^\delta}} \sum_{\boldsymbol{b}'} |\boldsymbol{b}'_1\rangle\,|\boldsymbol{b}'_2\rangle\,|l(\boldsymbol{b}'_1,\boldsymbol{b}'_2)\rangle\,|l(\boldsymbol{b}'_1,\boldsymbol{b}'_3)\rangle \tag{111}$$
$$= |\varphi\rangle_{R\widehat{Q}_0} \otimes \left(\frac{1}{\sqrt{q^\delta}} \sum_{\boldsymbol{b}'} |\boldsymbol{b}'_1\rangle\,|\boldsymbol{b}'_2\rangle\,|l(\boldsymbol{b}'_1,\boldsymbol{b}'_2)\rangle\,|l(\boldsymbol{b}'_1,\boldsymbol{b}'_3)\rangle\right), \tag{112}$$

where (109) involves a change of basis operation following space decomposition using $\mathbf{A}_{\mathcal{D}_i}, \mathbf{B}_{\mathcal{D}_i}$ presented above and change of basis is unitary; $l(\boldsymbol{b}'_1, \boldsymbol{b}'_2)$ represents the remaining $\kappa\Lambda(\mathcal{D}) - (k + \delta_1 + \delta_2)$ columns of $\boldsymbol{a}\mathbf{A}_{\mathcal{D}} + \boldsymbol{b}\mathbf{B}_{\mathcal{D}}$ that can be written as linear combinations of $\boldsymbol{b}'_1, \boldsymbol{b}'_2$; and $\boldsymbol{a}\mathbf{A}_{\mathcal{D}^c} + \boldsymbol{b}\mathbf{B}_{\mathcal{D}^c}$ is written as $l(\boldsymbol{b}'_1, \boldsymbol{b}'_3)$ (so nothing is changed and this is required for decoding as $\mathcal{D}^c$ is not in the decoding set). (110) follows from the observation that for any fixed $\boldsymbol{a}$, as we sum over all possible values of $\boldsymbol{b}$ over $\mathbb{F}_q^{1\times\delta}$, $\boldsymbol{b}'$ also takes all values over $\mathbb{F}_q^{1\times\delta}$ (because of the invertible map in (106)). In the last step, we have unentangled $R\widehat{Q}_0$ from the remaining qudits and $|\varphi\rangle_{R\widehat{Q}_0} = |\varphi\rangle_{RQ_0}$, so decoding is successful.

Rate Achieved: $\lambda_0 = k/\kappa$ so the proof of the lower bound on capacity in Theorem 2 is complete.

5.3 Proof of Corollary 1

Noting that $\boldsymbol{a}, \boldsymbol{b}$ consist of i.i.d. uniform elements in $\mathbb{F}_q$, we may express the entropy and mutual information terms in (6), (7) as rank conditions of the associated matrices and then Corollary 1 will follow.

First, consider (14).

$$\begin{aligned}
0 &\overset{(6)}{=} H(\boldsymbol{a} \mid \mathcal{Y}_{\mathcal{D}(e)}) && (113)\\
&= H(\boldsymbol{a}, \mathcal{Y}_{\mathcal{D}(e)}) - H(\mathcal{Y}_{\mathcal{D}(e)}) && (114)\\
&= H(\boldsymbol{a}) + H(\mathcal{Y}_{\mathcal{D}(e)} \mid \boldsymbol{a}) - H((\boldsymbol{a}, \boldsymbol{b})(\mathbf{A}_{\mathcal{D}(e)}; \mathbf{B}_{\mathcal{D}(e)})) && (115)\\
&= H(\boldsymbol{a}) + H(\boldsymbol{b}\mathbf{B}_{\mathcal{D}(e)} \mid \boldsymbol{a}) - H((\boldsymbol{a}, \boldsymbol{b})(\mathbf{A}_{\mathcal{D}(e)}; \mathbf{B}_{\mathcal{D}(e)})) && (116)\\
&= k + \text{rank}(\mathbf{B}_{\mathcal{D}(e)}) - \text{rank}(\mathbf{A}_{\mathcal{D}(e)}; \mathbf{B}_{\mathcal{D}(e)}), && (117)
\end{aligned}$$

where the last step follows from the fact that $\boldsymbol{a}, \boldsymbol{b}$ are i.i.d. uniform and (14) is proved.

(15) follows from (14) because the rank of $\mathbf{A}_{\mathcal{D}(e)}$ is at most k and $\text{rank}(\mathbf{A}_{\mathcal{D}(e)}; \mathbf{B}_{\mathcal{D}(e)}) - \text{rank}(\mathbf{0}; \mathbf{B}_{\mathcal{D}(e)}) = k$ so that $\langle \mathbf{I}_{k\times k}; \mathbf{0}_{\delta\times k} \rangle$ must be a subspace of $\langle \mathbf{A}_{\mathcal{D}(e)}; \mathbf{B}_{\mathcal{D}(e)} \rangle$.

Second, consider (16).

$$\begin{aligned}
0 &\overset{(7)}{=} I(\boldsymbol{a}; \mathcal{Y}_{\mathcal{D}^c(e)}) && (118)\\
&= H(\mathcal{Y}_{\mathcal{D}^c(e)}) - H(\mathcal{Y}_{\mathcal{D}^c(e)} \mid \boldsymbol{a}) && (119)\\
&= H((\boldsymbol{a}, \boldsymbol{b})(\mathbf{A}_{\mathcal{D}^c(e)}; \mathbf{B}_{\mathcal{D}^c(e)})) - H(\boldsymbol{b}\mathbf{B}_{\mathcal{D}^c(e)} \mid \boldsymbol{a}) && (120)\\
&= \text{rank}(\mathbf{A}_{\mathcal{D}^c(e)}; \mathbf{B}_{\mathcal{D}^c(e)}) - \text{rank}(\mathbf{B}_{\mathcal{D}^c(e)}) && (121)
\end{aligned}$$

and (16) is proved.

(17) follows from (16) because $\text{rank}(\mathbf{A}_{\mathcal{D}^c(e)}; \mathbf{B}_{\mathcal{D}^c(e)}) = \text{rank}(\mathbf{0}; \mathbf{B}_{\mathcal{D}^c(e)})$ so that $\langle \mathbf{I}_{k\times k}; \mathbf{0}_{\delta\times k} \rangle$ must have no intersection with $\langle \mathbf{A}_{\mathcal{D}^c(e)}; \mathbf{B}_{\mathcal{D}^c(e)} \rangle$.

5.4 Proof of Corollary 2

5.4.1 If and only if condition for $C(\mathcal{G}) = 0$

The 'if' direction is immediate, i.e., when $e_i \cap e_j = \emptyset$, by the intersection bound (4), we have $C(\mathcal{G}) \leq 0$.

We then consider the 'only if' direction, i.e., we show that as long as for any $\mathcal{D}(e_i), \mathcal{D}(e_j), e_i, e_j \in \mathcal{E}$, $e_i \cap e_j \neq \emptyset$, then there exists a feasible quantum storage code such that $C(\mathcal{G}) > 0$. We now present

such a (simple) code. We devote no effort to improving the efficiency but note that this is possible, e.g., by following existing work in related topics such as (quantum) secret sharing [35].

For the quantum code, we resort to the classical code in Theorem 2 whose performance translates into the quantum case.

For the classical secure storage problem with constraints (6) and (7), we consider $k = 1$ uniform binary classical secret symbol $a \in \mathbb{F}_2$. Then consider each decoding set $\mathcal{D}(e_1), \cdots, \mathcal{D}(e_{|\mathcal{E}|}), e_i \in \mathcal{E}$ sequentially. For decoding set $\mathcal{D}(e_i) = \{Q_{i_1}, \cdots, Q_{i_{|e_i|}}\}, i \in [|\mathcal{E}|]$, we set

$$\begin{aligned} &Y_{Q_{i_1}} \overset{\text{include}}{\longleftarrow} b_{i_1}, Y_{Q_{i_2}} \overset{\text{include}}{\longleftarrow} b_{i_2}, \cdots, Y_{Q_{i_{|e_i|}-1}} \overset{\text{include}}{\longleftarrow} b_{i_{|e_i|-1}}, \\ &Y_{Q_{i_{|e_i|}}} \overset{\text{include}}{\longleftarrow} a - b_{i_1} - \cdots - b_{i_{|e_i|-1}}, \end{aligned} \tag{122}$$

where the b symbols are all i.i.d. and uniform over $\mathbb{F}_2$ and in total $\sum_{i\in[|\mathcal{E}|]}(|e_i| - 1)$ uniform bits b are used; the notation $Y \overset{\text{include}}{\longleftarrow} b$ means b is appended as the last element in vector Y, i.e., for any $\mathcal{D}(e_i), i \in [|\mathcal{E}|]$, one more bit is included in $Y_Q, Q \in \mathcal{D}(e_i)$.

The classical decoding constraint (6) is satisfied as from (122), $a = \sum_{j\in[|e_i|]} Y_{Q_{i_j}}$ for decoding set $\mathcal{D}(e_i)$. The classical security constraint (7) is satisfied because any two decoding sets are intersecting such that for any decoding set $\mathcal{D}(e_k), k \in [|\mathcal{E}|]$, its complement $\mathcal{D}^c(e_k)$ is missing at least one b_i noise bit from any other decoding set $\mathcal{D}(e_i), i \neq k, i \in [|\mathcal{E}|]$ (note that in (122), any $|e_i| - 1$ Y_Q see independent b_i noise bits) and thus nothing about a is revealed. $C(\mathcal{G}) \geq k/\kappa > 0$, where κ is chosen so that the size constraint of each storage node is not exceeded, so the proof of the only if direction (and the overall proof) is now complete.

5.4.2 Capacity of small graphs

The graphs where $C(\mathcal{G}) = 0$ have been covered and we only need to consider graphs where $C(\mathcal{G}) > 0$. Note that we assume $\mathcal{G}$ has no redundant storage nodes (every storage node appears in some decoding set) and no redundant decoding sets (only minimal decoding sets are considered).

Let us start from the case when $|\mathcal{E}| \leq 3$. The case $|\mathcal{E}| = 1$ is trivial. When $|\mathcal{E}| = 2$, say $\mathcal{E} = \{e_1, e_2\}$, we have $C(\mathcal{G}) = \Lambda(\mathcal{D}(e_1) \cap \mathcal{D}(e_2))$; converse follows from the intersection bound (4) and achievability follows from storing the qudits directly in the storage nodes that are in both $\mathcal{D}(e_1)$ and $\mathcal{D}(e_2)$. When $|\mathcal{E}| = 3$, say $\mathcal{E} = \{e_1, e_2, e_3\}$, we may partition $\mathcal{Q}(\mathcal{G})$ into the following 7 disjoint sets.

$$\mathcal{Q}_{123} \triangleq \mathcal{D}(e_1) \cap \mathcal{D}(e_2) \cap \mathcal{D}(e_3), \tag{123}$$

$$\begin{aligned} &\mathcal{Q}_{123^c} \triangleq \mathcal{D}(e_1) \cap \mathcal{D}(e_2) \cap \mathcal{D}^c(e_3),\ \mathcal{Q}_{12^c3} \triangleq \mathcal{D}(e_1) \cap \mathcal{D}^c(e_2) \cap \mathcal{D}(e_3), \\ &\quad \mathcal{Q}_{1^c23} \triangleq \mathcal{D}^c(e_1) \cap \mathcal{D}(e_2) \cap \mathcal{D}(e_3), \end{aligned} \tag{124}$$

$$\begin{aligned} &\mathcal{Q}_{12^c3^c} \triangleq \mathcal{D}(e_1) \cap \mathcal{D}^c(e_2) \cap \mathcal{D}^c(e_3),\ \mathcal{Q}_{1^c23^c} \triangleq \mathcal{D}^c(e_1) \cap \mathcal{D}(e_2) \cap \mathcal{D}^c(e_3), \\ &\quad \mathcal{Q}_{1^c2^c3} \triangleq \mathcal{D}^c(e_1) \cap \mathcal{D}^c(e_2) \cap \mathcal{D}(e_3). \end{aligned} \tag{125}$$

From the intersection bound (4), we have

$$C(\mathcal{G}) \leq \min\Big(\Lambda\big(\mathcal{D}(e_1) \cap \mathcal{D}(e_2)\big), \Lambda\big(\mathcal{D}(e_1) \cap \mathcal{D}(e_3)\big), \Lambda\big(\mathcal{D}(e_2) \cap \mathcal{D}(e_3)\big)\Big) \tag{126}$$

$$= \Lambda(\mathcal{Q}_{123}) + \min\Big(\Lambda(\mathcal{Q}_{123^c}), \Lambda(\mathcal{Q}_{12^c3}), \Lambda(\mathcal{Q}_{1^c23})\Big), \tag{127}$$

which can be achieved by dividing the quantum message Q_0 into two parts - the first part has $\Lambda(\mathcal{Q}_{123})$ qudits and is directly stored in $\mathcal{Q}_{123}$; the second part has $\min(\Lambda(\mathcal{Q}_{123^c}), \Lambda(\mathcal{Q}_{12^c3}), \Lambda(\mathcal{Q}_{1^c23}))$ qudits and is stored over the MDS storage graph with three node sets $\mathcal{Q}_{123^c}, \mathcal{Q}_{12^c3}, \mathcal{Q}_{1^c23}$ and any two node sets form a decoding set (invoking the MDS storage graph $\mathcal{M}_{3,2}$ result from Theorem 3).

Next we consider $N \leq 4$ settings, among which $|\mathcal{E}| \leq 3$ cases have been covered above and the only remaining cases are

1. the wheel graph $\mathcal{W}_4$ that is covered by Theorem 4,
2. the MDS storage graph $\mathcal{M}_{4,3}$ that is covered by Theorem 3.

So all small graph cases are settled.

5.5 Proof of Theorem 3

The converse $C(\mathcal{M}_{N,K}) \leq \lambda_1 + \cdots + \lambda_{2K-N}$ follows from the intersection bound (4) by setting $e_1 = [K], e_2 = \{1, 2, \cdots, 2K-N, K+1, \cdots, N\}$ so that $e_1 \cap e_2 = [2K-N]$ and $\Lambda(\mathcal{D}(e_1) \cap \mathcal{D}(e_2)) = \lambda_1 + \cdots + \lambda_{2K-N}$, leading to $C_u(\mathcal{M}_{N,K}) \leq 2K - N$ in the uniform storage case where $\lambda_1 = \cdots = \lambda_N = 1$.

We now prove the achievability and start from the uniform storage case. We show that $C_u(\mathcal{M}_{N,K}) = 2K - N$ is achievable. Set q as a prime power where $q \geq N$, and

$$k = 2K - N,\ \boldsymbol{a} = (a_1, \cdots, a_k), \tag{128}$$

$$\delta = N - K,\ \boldsymbol{b} = (b_1, \cdots, b_\delta), \tag{129}$$

$$\kappa = 1, n = N, (\mathbf{A}; \mathbf{B}) = [(\alpha_j)^{k+\delta-i}]_{i,j} \in \mathbb{F}_q^{(k+\delta)\times n}, \tag{130}$$

$$(Y_{Q_1}, \cdots, Y_{Q_N}) = \boldsymbol{a}\mathbf{A} + \boldsymbol{b}\mathbf{B}, \tag{131}$$

where $(\mathbf{A}; \mathbf{B})$ is a Vandermonde matrix with the element in the i^{th} row and j^{th} column being $\alpha_j^{k+\delta-i}, i \in [k+\delta], j \in [n]$ and $\alpha_1, \cdots, \alpha_n$ are distinct elements in $\mathbb{F}_q$. Then the classical decoding constraint (6) is satisfied as we may verify the equivalent rank constraint (14) as follows. For any $e \in \mathcal{E} = \binom{[N]}{K}$,

$$\text{rank}(\mathbf{A}_{\mathcal{D}(e)}; \mathbf{B}_{\mathcal{D}(e)}) - \text{rank}(\mathbf{B}_{\mathcal{D}(e)}) = (k+\delta) - \delta = k, \tag{132}$$

where $(\mathbf{A}_{\mathcal{D}(e)}; \mathbf{B}_{\mathcal{D}(e)})$ is a sub-matrix of the Vandermonde matrix $(\mathbf{A}; \mathbf{B})$ with $|\mathcal{D}(e)| = K = k + \delta$ columns and is also square Vandermonde thus has full rank; $(\mathbf{B}_{\mathcal{D}(e)})$ is a sub-matrix of the Vandermonde matrix $(\mathbf{A}_{\mathcal{D}(e)}; \mathbf{B}_{\mathcal{D}(e)})$ with the last δ rows and is also Vandermonde and has full rank (note that in $(\mathbf{A}; \mathbf{B})$, we order the exponents of α_j increasingly from the bottom to the top). The classical security constraint (7) is satisfied as we may verify the equivalent rank constraint (16) as follows. For any $e \in \mathcal{E}$,

$$\text{rank}(\mathbf{A}_{\mathcal{D}^c(e)}; \mathbf{B}_{\mathcal{D}^c(e)}) - \text{rank}(\mathbf{B}_{\mathcal{D}^c(e)}) = \delta - \delta = 0, \tag{133}$$

where $(\mathbf{A}_{\mathcal{D}^c(e)}; \mathbf{B}_{\mathcal{D}^c(e)})$ is a sub-matrix of $(\mathbf{A}; \mathbf{B})$ with $|\mathcal{D}^c(e)| = N - K = \delta$ columns and is Vandermonde and has full rank; $(\mathbf{B}_{\mathcal{D}^c(e)})$ is a sub-matrix of $(\mathbf{A}_{\mathcal{D}^c(e)}; \mathbf{B}_{\mathcal{D}^c(e)})$ with last δ rows and is square Vandermonde and has full rank. Thus we may apply Theorem 2 to obtain a quantum code and $C_u(\mathcal{M}_{N,K}) \geq k/\kappa = 2K - N$.

Next consider the non-uniform storage case and we show that $C(\mathcal{M}_{N,K}) = \lambda_1 + \lambda_2 + \cdots + \lambda_{2K-N}$ is achievable. We will combine (space-share over) uniform storage MDS graphs as follows. Set $q \geq N$ as a prime power. For any $\epsilon > 0$, there exist rational λ'_i such that $\lambda'_i \leq \lambda_i, |\lambda'_i - \lambda_i| < \epsilon$ for all $i \in [N]$ as rationals are dense over the reals. For rationals $\lambda'_1, \cdots, \lambda'_N$, one can choose an integer scaling factor κ so that $\kappa\lambda'_1, \cdots, \kappa\lambda'_N$ are integers.

$$\text{Store } \lambda_0(1) = (2K-N)\kappa\lambda'_1 \text{ qudits of } Q_0 \text{ in } \mathcal{M}_{N,K}$$
$$\text{by utilizing } \lambda_i(1) = \kappa\lambda'_1 \text{ qudits of storage for } Q_i, i \in [1:N]. \tag{134}$$
$$\text{Store } \lambda_0(2) = (2K-N-1)\kappa(\lambda'_2 - \lambda'_1) \text{ qudits of } Q_0 \text{ in } \mathcal{M}_{N-1,K-1}$$
$$\text{by utilizing } \lambda_i(2) = \kappa(\lambda'_2 - \lambda'_1) \text{ qudits of storage for } Q_i, i \in [2:N]. \tag{135}$$
$$\text{Store } \lambda_0(3) = (2K-N-2)\kappa(\lambda'_3 - \lambda'_2) \text{ qudits of } Q_0 \text{ in } \mathcal{M}_{N-2,K-2}$$
$$\text{by utilizing } \lambda_i(3) = \kappa(\lambda'_3 - \lambda'_2) \text{ qudits of storage for } Q_i, i \in [3:N]. \tag{136}$$
$$\vdots$$
$$\text{Store } \lambda_0(j) = (2K-N-j+1)\kappa(\lambda'_j - \lambda'_{j-1}) \text{ qudits of } Q_0 \text{ in } \mathcal{M}_{N-j+1,K-j+1}$$
$$\text{by utilizing } \lambda_i(j) = \kappa(\lambda'_j - \lambda'_{j-1}) \text{ qudits of storage for } Q_i, i \in [j:N]. \tag{137}$$
$$\vdots$$
$$\text{Store } \lambda_0(2K-N) = 1 \times \kappa(\lambda'_{2K-N} - \lambda'_{2K-N-1}) \text{ qudits of } Q_0 \text{ in } \mathcal{M}_{2N-2K+1,N-K+1}$$
$$\text{by utilizing } \lambda_i(2K-N) = \kappa(\lambda'_{2K-N} - \lambda'_{2K-N-1}) \text{ qudits of storage for } Q_i, i \in [2K-N:N]. \tag{138}$$

For each $j \in [2K-N]$, we are using the capacity achieving code for uniform storage MDS graph $\mathcal{M}_{N-j+1,K-j+1}$ where $C \geq 2K-N-j+1 > 0$. Further the component code for each $j \in [2K-N]$ satisfies the original K out of N MDS constraint because

$$\underbrace{(j-1)}_{\text{unused } Q_i} + (K-j+1) = K. \tag{139}$$

In total the number of qudits from the quantum message stored and the number of qudits used in the storage nodes are

$$\lambda_0(1) + \cdots + \lambda_0(2K-N) = \kappa(\lambda'_1 + \cdots + \lambda'_{2K-N}) \triangleq \kappa\lambda_0, \tag{140}$$
$$\lambda_1(1) = \kappa\lambda'_1 \leq \kappa\lambda_1, \tag{141}$$
$$\lambda_2(1) + \lambda_2(2) = \kappa\lambda'_2 \leq \kappa\lambda_2, \tag{142}$$
$$\vdots \tag{143}$$
$$\lambda_{2K-N}(1) + \cdots + \lambda_{2K-N}(2K-N) = \kappa\lambda'_{2K-N} \leq \kappa\lambda_{2K-N}, \tag{144}$$
$$\kappa\lambda'_{2K-N} \leq \kappa\lambda_i, i \in [2K-N+1:N]. \tag{145}$$

Thus, $C(\mathcal{M}_{N,K}) \geq \sup \lambda_0 = \sup \lambda'_1 + \cdots + \lambda'_{2K-N} \overset{\epsilon \to 0}{=} \lambda_1 + \cdots + \lambda_{2K-N}$, as desired.

5.6 Proof of Theorem 4

Consider the upper bound $C(\mathcal{W}_N) \leq \min\left(\lambda_1, \lambda_2, \frac{\lambda_1+\lambda_2}{3}, \frac{\lambda_1+\lambda_2+\lambda_3}{5}, \cdots, \frac{\lambda_1+\lambda_2+\cdots+\lambda_{N-2}}{2N-5}\right)$. The first two terms follow from the intersection bound (4),

$$e_1 = \{1,2\}, e_2 = \{1,3\} \quad \stackrel{(4)}{\Longrightarrow} \quad C(\mathcal{W}_N) \leq \Lambda\Big(\mathcal{D}(e_1) \cap \mathcal{D}(e_2)\Big) = \lambda_1, \tag{146}$$

$$e_1 = \{1,2\}, e_N = \{2,3,\cdots,N\} \quad \stackrel{(4)}{\Longrightarrow} \quad C(\mathcal{W}_N) \leq \Lambda\Big(\mathcal{D}(e_1) \cap \mathcal{D}(e_N)\Big) = \lambda_2. \tag{147}$$

The remaining terms follow from the wheel bound (5) by setting $n = N$, $\mathcal{Q}_i = \{Q_i\}$ for all $i \in [n]$. Next, we prove the achievability of the upper bound for the following two cases.

With a similar proof as that for the MDS graph in Section 5.5, we assume without loss of generality that $\lambda_i, i \in [N]$ and the number of qudits used in the schemes (i.e., $\frac{2\lambda_1-\lambda_2}{2N-5}$ in (152), $\frac{(N-2)\lambda_2-\lambda_1}{2N-5}$ in (153), $\frac{2\lambda_2-\lambda_1}{3}$ in (161), $\frac{2\lambda_1-\lambda_2}{3}$ in (162), $\frac{2(\lambda_1+\lambda_2)-3\lambda_3}{5}$ in (170), $\frac{4\lambda_2-(\lambda_1+\lambda_3)}{5}$ in (171)) are integers (through approximating reals by rationals and scaling rationals to integers).

5.6.1 $\lambda_2 = \lambda_3 = \cdots = \lambda_N$

We show that $C(\mathcal{W}_N) = \min(\lambda_1, \lambda_2, \frac{\lambda_1+(N-3)\lambda_2}{2N-5})$. Note that the uniform storage case, where $\lambda_1 = \lambda_2 = \cdots = \lambda_N = 1$ and $C_u(\mathcal{W}_N) = \frac{N-2}{2N-5}$, is covered and thus needs no proof. The proof in this section is a generalization of the proof of $C(\mathcal{W}_4)$ presented in Section 4.2.

We first present two component codes.

1. $\lambda_0 = 1$ code for storage graph $\mathcal{W}_N$ with $(\lambda_1, \lambda_2, \cdots, \lambda_N) = (N-2, 1, \cdots, 1)$.

   Set $\kappa = 1$ and $q \geq N-1$ is a prime power. Use the following classical (generic linear) secure storage code,

   $$Y_{Q_1} = (b_1, b_2, \cdots, b_{N-2}), \tag{148}$$
   $$(Y_{Q_2}, Y_{Q_3}, \cdots, Y_{Q_N}) = (a, b_1, \cdots, b_{N-2}) \times [\alpha_j^{N-1-i}]_{i,j}, \tag{149}$$

   where $a, b_1, \cdots, b_{N-2}$ are i.i.d. uniform elements in $\mathbb{F}_q$, $[\alpha_j^{N-1-i}]_{i,j} \in \mathbb{F}_q^{(N-1)\times(N-1)}, i, j \in [N-1]$ is a Vandermonde matrix and α_j are distinct elements in $\mathbb{F}_q$. The classical constraints (6), (7) are satisfied and Theorem 2 produces the desired quantum code.

2. $\lambda_0 = 1$ code for storage graph $\mathcal{W}_N$ with $(\lambda_1, \lambda_2, \cdots, \lambda_N) = (1, 2, \cdots, 2)$.

   Set $\kappa = 1$ and $q \geq N-1$ is a prime power. Use the following classical (structured) secure storage code. $Y_{Q_i}, i \in [2:N]$ contains two symbols $Y_{Q_i} = (Y_{Q_i}(1), Y_{Q_i}(2))$.

   $$Y_{Q_1} = b_1, Y_{Q_i}(1) = a + b_1, i \in [2:N], \tag{150}$$
   $$(Y_{Q_2}(2), Y_{Q_3}(2), \cdots, Y_{Q_N}(2)) = (a, b_2, \cdots, b_{N-1}) \times [\alpha_j^{N-1-i}]_{i,j}, \tag{151}$$

   where $a, b_1, \cdots, b_{N-1}$ are i.i.d. uniform elements in $\mathbb{F}_q$, $[\alpha_j^{N-1-i}]_{i,j} \in \mathbb{F}_q^{(N-1)\times(N-1)}, i, j \in [N-1]$ is Vandermonde and α_j are distinct in $\mathbb{F}_q$. The classical constraints (6), (7) are satisfied and Theorem 2 produces the desired quantum code.

Next we use the above two component codes to achieve $C(\mathcal{W}_N) = \min\left(\lambda_1, \lambda_2, \frac{\lambda_1+(N-3)\lambda_2}{2N-5}\right)$. There are three cases. Choose a prime power $q \geq N-1$.

1. When $\lambda_1 \leq \lambda_2/2$, $\min\left(\lambda_1, \lambda_2, \frac{\lambda_1+(N-3)\lambda_2}{2N-5}\right) = \lambda_1$. Use the second component code to store $\lambda_0 = \lambda_1$ qudits of Q_0 in $(Q_1, Q_2, \cdots, Q_N)$ while utilizing storage in the amounts $(\lambda_1, 2\lambda_1, \cdots, 2\lambda_1)$ qudits, respectively. The scheme works as $\lambda_1 \leq \lambda_2/2$ and $Q_2, \cdots, Q_N$ might have extra unused qudits.

2. When $\lambda_2/2 \leq \lambda_1 \leq (N-2)\lambda_2$, $\min\left(\lambda_1, \lambda_2, \frac{\lambda_1+(N-3)\lambda_2}{2N-5}\right) = \frac{\lambda_1+(N-3)\lambda_2}{2N-5}$.

   Use the first component code to store $\lambda_0(1) = \frac{2\lambda_1-\lambda_2}{2N-5} \geq 0$ qudits of Q_0 in $(Q_1, Q_2, \cdots, Q_N)$ by utilizing $((N-2)\lambda_0(1), \lambda_0(1), \cdots, \lambda_0(1))$ qudits of storage. (152)

   Use the second component code to store $\lambda_0(2) = \frac{(N-2)\lambda_2-\lambda_1}{2N-5} \geq 0$ qudits of Q_0 in $(Q_1, Q_2, \cdots, Q_N)$ by utilizing $(\lambda_0(2), 2\lambda_0(2), \cdots, 2\lambda_0(2))$ qudits of storage. (153)

   The scheme works because we have stored the desired number of qudits of Q_0, $\lambda_0(1) + \lambda_0(2) = \frac{\lambda_1+(N-3)\lambda_2}{2N-5}$, in $Q_1, Q_2, \cdots, Q_N$ and all storage qudits are fully used, $\lambda_1 = (N-2)\lambda_0(1) + \lambda_0(2), \lambda_2 = \lambda_0(1) + 2\lambda_0(2)$.

3. When $(N-2)\lambda_2 \leq \lambda_1$, $\min\left(\lambda_1, \lambda_2, \frac{\lambda_1+(N-3)\lambda_2}{2N-5}\right) = \lambda_2$. Use the first component code to store $\lambda_0 = \lambda_2$ qudits of Q_0 in $(Q_1, Q_2, \cdots, Q_N)$ by utilizing storage in the amounts $((N-2)\lambda_2, \lambda_2, \cdots, \lambda_2)$ qudits, respectively. The scheme works as $(N-2)\lambda_2 \leq \lambda_1$ and Q_1 might have extra unused qudits.

The results of this section generalize (slightly) to cases where λ_{N-1}, λ_N are unconstrained (so not necessarily equal to λ_2 and $\lambda_2 \leq \lambda_{N-1} \leq \lambda_N$) as they do not influence the upper bound (20) and the above code construction.

5.6.2 $N = 5$

Note that the $N = 4$ case is covered in Section 4.2 and we only need to consider $N = 5$. We show that $C(\mathcal{W}_5) = \min(\lambda_1, \lambda_2, \frac{\lambda_1+\lambda_2}{3}, \frac{\lambda_1+\lambda_2+\lambda_3}{5})$ is achievable. The idea is similar to that in the above section, i.e., carefully combining component codes, so repetitive details are omitted and only differences are highlighted.

We first present three component codes, where the first two are identical to above.

1. $\lambda_0 = 1$ code for storage graph $\mathcal{W}_5$ with $(\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5) = (3, 1, 1, 1, 1)$.

2. $\lambda_0 = 1$ code for storage graph $\mathcal{W}_5$ with $(\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5) = (1, 2, 2, 2, 2)$.

3. $\lambda_0 = 1$ code for storage graph $\mathcal{W}_5$ with $(\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5) = (2, 1, 2, 2, 2)$.

   Set $\kappa = 1$ and q is any prime power. Use the following classical (structured) secure storage code.

$$Y_{Q_1} = (b_1, b_4), Y_{Q_2} = (a + b_1), Y_{Q_3} = (b_2, a + b_4), \tag{154}$$

$$Y_{Q_4} = (b_3, a + b_4), Y_{Q_5} = (a + b_2 + b_3, a + b_4), \tag{155}$$

   where a, b_1, b_2, b_3, b_4 are i.i.d. uniform elements in $\mathbb{F}_q$. Interestingly, a different alignment structure is applied here. The classical constraints (6), (7) are satisfied and Theorem 2 produces the desired quantum code.

Next we combine the above three component codes to achieve $C(\mathcal{W}_5) = \min(\lambda_1, \lambda_2, \frac{\lambda_1+\lambda_2}{3}, \frac{\lambda_1+\lambda_2+\lambda_3}{5})$. Depending on which term is the minimum, we have four cases. Choose a prime power $q \geq 4$. Note that $\lambda_2 \leq \lambda_3 \leq \lambda_4 \leq \lambda_5$.

1. When $\min(\lambda_1, \lambda_2, \frac{\lambda_1+\lambda_2}{3}, \frac{\lambda_1+\lambda_2+\lambda_3}{5}) = \lambda_1$, we have $\lambda_1 \leq \lambda_2/2 \leq (\lambda_2+\lambda_3)/4$. Use the second component code to store $\lambda_0 = \lambda_1$ qudits of Q_0 in $(Q_1, Q_2, Q_3, Q_4, Q_5)$ by utilizing storage in the amounts $(\lambda_1, 2\lambda_1, 2\lambda_1, 2\lambda_1, 2\lambda_1)$ qudits, respectively.

2. When $\min(\lambda_1, \lambda_2, \frac{\lambda_1+\lambda_2}{3}, \frac{\lambda_1+\lambda_2+\lambda_3}{5}) = \lambda_2$, we have $\lambda_2 \leq \lambda_1/2$ and $\lambda_2 \leq (\lambda_1+\lambda_3)/4$. There are two sub-cases here.

   (a) $\lambda_1 \leq \lambda_3$ or $2\lambda_2 \leq \lambda_3 \leq \lambda_1$: Use the third component code to store $\lambda_0 = \lambda_2$ qudits of Q_0 in $(Q_1, Q_2, Q_3, Q_4, Q_5)$ by utilizing storage in the amounts $(2\lambda_2, \lambda_2, 2\lambda_2, 2\lambda_2, 2\lambda_2)$ qudits, respectively, where $2\lambda_2 \leq \lambda_1$ and $2\lambda_2 \leq \lambda_3 \leq \lambda_4 \leq \lambda_5$.

   (b) $\lambda_3 \leq \lambda_1$ and $\lambda_3 \leq 2\lambda_2$:

   Use the first component code to store $\lambda_0(1) = 2\lambda_2 - \lambda_3 \geq 0$ qudits of Q_0 in Q_1, Q_2, Q_3, Q_4, Q_5 by utilizing $(3\lambda_0(1), \lambda_0(1), \lambda_0(1), \lambda_0(1), \lambda_0(1))$ qudits of storage. (156)

   Use the third component code to store $\lambda_0(2) = \lambda_3 - \lambda_2 \geq 0$ qudits of Q_0 in Q_1, Q_2, Q_3, Q_4, Q_5 by utilizing $(2\lambda_0(2), \lambda_0(2), 2\lambda_0(2), 2\lambda_0(2), 2\lambda_0(2))$ qudits of storage. (157)

   The scheme works because the number of stored qudits of Q_0 is $\lambda_0 = \lambda_0(1)+\lambda_0(2) = \lambda_2$, and the number of used storage qudits are

$$Q_1: \quad 3\lambda_0(1) + 2\lambda_0(2) = 4\lambda_2 - \lambda_3 \leq \lambda_1, \tag{158}$$
$$Q_2: \quad \lambda_0(1) + \lambda_0(2) = \lambda_2, \tag{159}$$
$$Q_3, Q_4, Q_5: \quad \lambda_0(1) + 2\lambda_0(2) = \lambda_3 \leq \lambda_4 \leq \lambda_5. \tag{160}$$

3. When $\min(\lambda_1, \lambda_2, \frac{\lambda_1+\lambda_2}{3}, \frac{\lambda_1+\lambda_2+\lambda_3}{5}) = \frac{\lambda_1+\lambda_2}{3}$, we have $2\lambda_1 \geq \lambda_2, 2\lambda_2 \geq \lambda_1, 3\lambda_3 \geq 2(\lambda_1+\lambda_2)$ and use[6]

$$\text{second component code } (1,2,2,2,2) \times \frac{2\lambda_2 - \lambda_1}{3} \ (\geq 0), \tag{161}$$
$$\text{third component code } (2,1,2,2,2) \times \frac{2\lambda_1 - \lambda_2}{3} \ (\geq 0). \tag{162}$$

   The scheme works because

$$Q_0: \quad \lambda_0 = \frac{2\lambda_2 - \lambda_1}{3} + \frac{2\lambda_1 - \lambda_2}{3} = \frac{\lambda_1 + \lambda_2}{3}, \tag{163}$$
$$Q_1: \quad 1 \times \frac{2\lambda_2 - \lambda_1}{3} + 2 \times \frac{2\lambda_1 - \lambda_2}{3} = \lambda_1, \tag{164}$$
$$Q_2: \quad 2 \times \frac{2\lambda_2 - \lambda_1}{3} + 1 \times \frac{2\lambda_1 - \lambda_2}{3} = \lambda_2, \tag{165}$$
$$Q_3, Q_4, Q_5: \quad 2 \times \frac{2\lambda_2 - \lambda_1}{3} + 2 \times \frac{2\lambda_1 - \lambda_2}{3} = \frac{2(\lambda_1+\lambda_2)}{3} \leq \lambda_3 \leq \lambda_4 \leq \lambda_5. \tag{166}$$

[6] $(\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5) \times \lambda_0$ denotes the coding scheme that stores λ_0 qudits of Q_0 in $(Q_1, Q_2, Q_3, Q_4, Q_5)$ by utilizing storage in the amounts $(\lambda_0\lambda_1, \lambda_0\lambda_2, \lambda_0\lambda_3, \lambda_0\lambda_4, \lambda_0\lambda_5)$ qudits, respectively.

4. When $\min(\lambda_1, \lambda_2, \frac{\lambda_1+\lambda_2}{3}, \frac{\lambda_1+\lambda_2+\lambda_3}{5}) = \frac{\lambda_1+\lambda_2+\lambda_3}{5}$, we have

$$\begin{aligned} 4\lambda_1 &\geq \lambda_2 + \lambda_3, && (167)\\ 4\lambda_2 &\geq \lambda_1 + \lambda_3, && (168)\\ 2(\lambda_1+\lambda_2) &\geq 3\lambda_3 && (169) \end{aligned}$$

and use

$$\text{first component code } (3,1,1,1,1) \times \beta_1, \text{ where } \beta_1 = \frac{2(\lambda_1+\lambda_2)-3\lambda_3}{5} \geq 0 \text{ due to (169)}, \quad (170)$$

$$\text{second component code } (1,2,2,2,2) \times \beta_2, \text{ where } \beta_2 = \frac{4\lambda_2-(\lambda_1+\lambda_3)}{5} \geq 0 \text{ due to (168)}, \quad (171)$$

$$\text{third component code } (2,1,2,2,2) \times \beta_3, \text{ where } \beta_3 = (\lambda_3-\lambda_2) \geq 0. \quad (172)$$

The scheme works because

$$\begin{aligned} Q_0: &\quad \lambda_0 = \beta_1+\beta_2+\beta_3, = \frac{\lambda_1+\lambda_2+\lambda_3}{5}, && (173)\\ Q_1: &\quad 3\beta_1+\beta_2+2\beta_3 = \lambda_1, && (174)\\ Q_2: &\quad \beta_1+2\beta_2+\beta_3 = \lambda_2, && (175)\\ Q_3, Q_4, Q_5: &\quad \beta_1+2\beta_2+2\beta_3 = \lambda_3 \leq \lambda_4 \leq \lambda_5. && (176) \end{aligned}$$

5.7 Proof of Theorem 6

For uniform storage, $\lambda_i = 1, \forall i$. The intersection bound (4) gives the converse as follows.

$$\begin{aligned} C_u(\sqcap_{\Delta,m}) &\leq \Lambda(\mathcal{D}(e_1) \cap \mathcal{D}(e_2)) = \Lambda\left(\left\{Q_{\overline{\mathcal{S}}} : 1 \in \mathcal{S}, 2 \in \mathcal{S}, \mathcal{S} \in \binom{[\Delta]}{m}\right\}\right) && (177)\\ &= \binom{\Delta-2}{m-2}. && (178) \end{aligned}$$

For the achievability, we use Theorem 2 and translate from the following classical (structured) secure storage code. Set $\kappa = 1$ and q as a prime power such that $q > \binom{\Delta-1}{m-1} + \Delta\binom{\Delta-2}{m-2}$, and $k = \binom{\Delta-2}{m-2}$, $\delta = \binom{\Delta-2}{m-1}$ so that $\boldsymbol{a} \in \mathbb{F}_q^{1\times k}$ and $\boldsymbol{b} \in \mathbb{F}_q^{1\times\delta}$ (with i.i.d. elements in $\mathbb{F}_q$). Note that $k+\delta = \binom{\Delta-1}{m-1}$. For the design of Y_Q, consider first $\mathcal{D}(e_1)$.

$$\left(Y_{Q_{\overline{\mathcal{S}}}} : 1 \in \mathcal{S}, \mathcal{S} \in \binom{[\Delta]}{m}\right) = (\boldsymbol{a}, \boldsymbol{b}) \times \left(\mathbf{A}_{\mathcal{D}(e_1)}; \mathbf{B}_{\mathcal{D}(e_1)}\right) \in \mathbb{F}_q^{1\times(k+\delta)}, \quad (179)$$

where $(\mathbf{A}_{\mathcal{D}(e_1)}; \mathbf{B}_{\mathcal{D}(e_1)}) \in \mathbb{F}_q^{(k+\delta)\times(k+\delta)}$ is a square matrix that needs to satisfy some rank constraints so as to guarantee (6), (7) (refer to Lemma 3). For now, it suffices to imagine it as a sufficiently generic matrix. In particular, if we randomly generate each of its element over a large field, then it will work with high probability.

Consider next $\mathcal{D}^c(e_1)$. For any $Q_{\overline{\mathcal{S}}}, 1 \notin \mathcal{S}$, denote

$$\mathcal{S} = \{i_1, i_2, \cdots, i_m\}, 1 < i_1 < i_2 < \cdots < i_m \quad (180)$$

and define the set where $i_j, j \in [m]$ in $\mathcal{S}$ is replaced by 1 as $\mathcal{S}_j$,

$$\mathcal{S}_j \triangleq \{i_1, \cdots, i_{j-1}, 1, i_{j+1}, \cdots, i_m\}, j \in [m]. \tag{181}$$

Then for any $\mathcal{S}$ such that $1 \notin \mathcal{S}, \mathcal{S} \in \binom{[\Delta]}{m}$, set

$$Y_{Q_{\overline{\mathcal{S}}}} = \sum_{j \in [m]} (-1)^j Y_{Q_{\overline{\mathcal{S}_j}}}. \tag{182}$$

The encoding is now complete. Next we show that this encoding satisfies some useful properties in the following lemma and the proof is deferred to Section 5.7.1.

Lemma 2. *For the encoding in (182), the following three properties hold.*

1. *For any $i \in [2:\Delta]$,*

$$\left(Y_{Q_{\overline{\mathcal{S}}}} : i \in \mathcal{S}, \mathcal{S} \in \binom{[\Delta]}{m}\right) \overset{\textit{invertible}}{\longleftrightarrow} \left(Y_{Q_{\overline{\mathcal{S}}}} : 1 \in \mathcal{S}, \mathcal{S} \in \binom{[\Delta]}{m}\right). \tag{183}$$

2. *For any $i \in [2:\Delta]$,*

$$\left(Y_{Q_{\overline{\mathcal{S}}}} : i \notin \mathcal{S}, \mathcal{S} \in \binom{[\Delta]}{m}\right) \textit{ is a function of } \left(Y_{Q_{\overline{\mathcal{S}}}} : 1 \in \mathcal{S}, i \notin \mathcal{S}, \mathcal{S} \in \binom{[\Delta]}{m}\right). \tag{184}$$

3.

$$\left(Y_{Q_{\overline{\mathcal{S}}}} : 1 \notin \mathcal{S}, \mathcal{S} \in \binom{[\Delta]}{m}\right) \textit{ is a function of } \left(Y_{Q_{\overline{\mathcal{S}}}} : 1 \notin \mathcal{S}, 2 \in \mathcal{S}, \mathcal{S} \in \binom{[\Delta]}{m}\right). \tag{185}$$

Remark 3. *Lemma 2 is intuitively described as follows. In (183), the LHS is all classical shares in $\mathcal{D}(e_i), i \neq 1$ and the RHS is all classical shares in $\mathcal{D}(e_1)$; their invertibility means that if $\mathcal{D}(e_1)$ can decode the classical secret, then so can all $\mathcal{D}(e_i)$ (see (186) below). Referring to $\sqcap_{5,3}$ in Figure 6 for an example, $\mathcal{D}(e_2)$ contains classical shares $(z_1, z_4, z_5, z_4 - z_1 + z_2, z_5 - z_1 + z_3, z_5 - z_4 + z_6)$, which are invertible to $(z_1, z_2, z_3, z_4, z_5, z_6)$, all classical shares in $\mathcal{D}(e_1)$. In (184), the LHS is all classical shares in $\mathcal{D}^c(e_i), i \neq 1$ and the RHS is a subset where 1 belongs to the label. The property that LHS is a function of the RHS means that for security, we need to show the noise (b_i terms) in the RHS spans the full space thus leaking no information (see (189) below). Referring to $\sqcap_{5,3}$ in Figure 6, $\mathcal{D}^c(e_2)$ contains classical shares $(z_2, z_3, z_6, z_6 - z_3 + z_2)$ where $z_6 + z_3 + z_2$ is a function of the remaining three (RHS). Regarding alignment, $z_6 - z_3 + z_2$ is aligned in the space spanned by z_2, z_3, z_6 so that it cannot contribute additional information. In (185), the LHS is all classical shares in $\mathcal{D}^c(e_1)$, which are a function of the RHS, a subset of LHS. Thus for security, it suffices to show the noise in the RHS has full rank (see (191) below). Referring to $\sqcap_{5,3}$ in Figure 6, $\mathcal{D}^c(e_1)$ contains $(z_4 - z_1 + z_2, z_5 - z_1 + z_3, z_5 - z_4 + z_6, z_6 - z_3 + z_2)$ where the last element $z_6 - z_3 + z_2$ is a function of the first three elements (alignment), i.e., $(z_4 - z_1 + z_2) - (z_5 - z_1 + z_3) + (z_5 - z_4 + z_6)$. Thanks to such alignment, the dimension in the complement of a decoding set, $\binom{\Delta-1}{m}$ is reduced to the dimension of noise, $\binom{\Delta-2}{m-1}$.*

Equipped with the above properties, we proceed to consider the decoding constraint (6) and the security constraint (7).

First, consider (6). For any decoding set $\mathcal{D}(e_i), i \in [\Delta]$, from (179) and (183), (6) is equivalent to that

$$\text{square matrix } \left(\mathbf{A}_{\mathcal{D}(e_1)}; \mathbf{B}_{\mathcal{D}(e_1)}\right) \text{ has full rank } k+\delta \tag{186}$$

because for $\mathcal{D}(e_1)$, if the square matrix $(\mathbf{A}_{\mathcal{D}(e_1)}; \mathbf{B}_{\mathcal{D}(e_1)})$ has full rank, then by (179), we can decode all $\boldsymbol{a}, \boldsymbol{b}$ from $\mathcal{Y}_{\mathcal{D}(e_1)}$ and for $\mathcal{D}(e_i), i \in [2:\Delta]$, by (183), $\mathcal{Y}_{\mathcal{D}(e_i)}$ is invertible to $\mathcal{Y}_{\mathcal{D}(e_1)}$ so that the full rank of $(\mathbf{A}_{\mathcal{D}(e_1)}; \mathbf{B}_{\mathcal{D}(e_1)})$ also suffices.

Second, consider (7) for $\mathcal{D}(e_i), i \in [2:\Delta]$. From (184), we know that $\mathcal{Y}_{\mathcal{D}^c(e_i)}$ is a function of $\left(Y_{Q_{\overline{\mathcal{S}}}} : 1 \in \mathcal{S}, i \notin \mathcal{S}, \mathcal{S} \in \binom{\Delta}{m}\right)$ and denote

$$\left(Y_{Q_{\overline{\mathcal{S}}}} : 1 \in \mathcal{S}, i \notin \mathcal{S}, \mathcal{S} \in \binom{[\Delta]}{m}\right) \triangleq (\boldsymbol{a}, \boldsymbol{b}) \times (\mathbf{A}_{\mathcal{D}_i^c}; \mathbf{B}_{\mathcal{D}_i^c}), \tag{187}$$

where $(\mathbf{A}_{\mathcal{D}_i^c}; \mathbf{B}_{\mathcal{D}_i^c}) \in \mathbb{F}_q^{(k+\delta)\times\delta}$ is a sub-matrix of $(\mathbf{A}_{\mathcal{D}(e_1)}; \mathbf{B}_{\mathcal{D}(e_1)})$ (with corresponding columns that produce the above $Y_{Q_{\overline{\mathcal{S}}}}$). Then (7) and equivalently (16) hold if

$$\text{rank}\left(\mathbf{A}_{\mathcal{D}_i^c}; \mathbf{B}_{\mathcal{D}_i^c}\right) = \text{rank}\left(\mathbf{B}_{\mathcal{D}_i^c}\right), \tag{188}$$

which is further equivalent to

$$\text{square matrix } \mathbf{B}_{\mathcal{D}_i^c} \in \mathbb{F}_q^{\delta\times\delta} \text{ has full rank}, i \in [2:\Delta], \tag{189}$$

as $(\mathbf{A}_{\mathcal{D}_i^c}; \mathbf{B}_{\mathcal{D}_i^c})$ has δ columns and its rank is no smaller than the rank of $\mathbf{B}_{\mathcal{D}_i^c}$.

Third, consider (7) for $\mathcal{D}(e_1)$. From (185), we know that $\mathcal{Y}_{\mathcal{D}^c(e_1)}$ is a function of

$$\left(Y_{Q_{\overline{\mathcal{S}}}} : 1 \notin \mathcal{S}, 2 \in \mathcal{S}, \mathcal{S} \in \binom{[\Delta]}{m}\right) \triangleq (\boldsymbol{a}, \boldsymbol{b}) \times \left(\mathbf{A}_{\mathcal{D}_1^c}; \mathbf{B}_{\mathcal{D}_1^c}\right), \tag{190}$$

where $(\mathbf{A}_{\mathcal{D}_1^c}; \mathbf{B}_{\mathcal{D}_1^c}) \in \mathbb{F}_q^{(k+\delta)\times\delta}$ can be written as linear combinations of the columns of $(\mathbf{A}_{\mathcal{D}(e_1)}; \mathbf{B}_{\mathcal{D}(e_1)})$ because from (182), $Y_{Q_{\overline{\mathcal{S}}}}, 1 \notin \mathcal{S}$ is coded through $Y_{Q_{\overline{\mathcal{S}}}}, 1 \in \mathcal{S}$, i.e., $(\mathbf{A}_{\mathcal{D}(e_1)}; \mathbf{B}_{\mathcal{D}(e_1)})$. Then (7) and equivalently (16) hold if

$$\text{square matrix } \mathbf{B}_{\mathcal{D}_1^c} \in \mathbb{F}_q^{\delta\times\delta} \text{ has full rank}. \tag{191}$$

We have now established that (6), (7) hold if (186), (189), (191) hold, which can be guaranteed according to the following lemma. So the proof is complete.

Lemma 3. *When the field size $q > (k+\delta) + \Delta\delta = \binom{\Delta-1}{m-1} + \Delta\binom{\Delta-2}{m-2}$, there exists an assignment of matrix $(\mathbf{A}_{\mathcal{D}(e_1)}; \mathbf{B}_{\mathcal{D}(e_1)})$ such that (186), (189), (191) are satisfied.*

Proof: Take the product of the determinants of the square matrices in (186), (189), (191) and view it as a polynomial, denoted as Π, whose variables are the $(k+\delta)^2$ elements of the square matrix $(\mathbf{A}_{\mathcal{D}(e_1)}; \mathbf{B}_{\mathcal{D}(e_1)})$. Π has degree $(k+\delta) + \Delta\delta = \binom{\Delta-1}{m-1} + \Delta\binom{\Delta-2}{m-2} < q$.

The polynomial Π is not the zero polynomial because there exists a realization of the $(k+\delta)^2$ variables such that any single matrix in (186), (189), (191) has full rank (for (191), note that each $Y_{Q_{\overline{\mathcal{S}}}}$ where $1 \in \mathcal{S}, 2 \notin \mathcal{S}$ appears in one distinct $Y_{Q_{\overline{\mathcal{S}'}}}$ where $1 \notin \mathcal{S}', 2 \in \mathcal{S}'$). Sample the $(k+\delta)^2$ variables independently and uniformly from $\mathbb{F}_q$ so that by the Schwartz–Zippel lemma, the probability of Π being zero is no greater than the degree of Π over q, which is strictly smaller than 1. Therefore there exists an assignment of $(\mathbf{A}_{\mathcal{D}(e_1)}; \mathbf{B}_{\mathcal{D}(e_1)})$ such that the matrices in (186), (189), (191) all have full rank.

□

5.7.1 Proof of Lemma 2

First, we prove (183). Consider any $i \in [2:\Delta]$.

$$\begin{aligned} & \left(Y_{Q_{\overline{\mathcal{S}}}} : i \in \mathcal{S}, \mathcal{S} \in \binom{[\Delta]}{m}\right) \\ \overset{\text{invertible}}{\longleftrightarrow} \quad & \left(Y_{Q_{\overline{\mathcal{S}}}} : 1 \in \mathcal{S}, i \in \mathcal{S}, \mathcal{S} \in \binom{[\Delta]}{m}, Y_{Q_{\overline{\mathcal{S}}}} : 1 \notin \mathcal{S}, i \in \mathcal{S}, \mathcal{S} \in \binom{[\Delta]}{m}\right). \end{aligned} \tag{192}$$

Note that from (182), for any $\mathcal{S} = \{i_1, \cdots, i_m\}$ such that $1 \notin \mathcal{S}, i \in \mathcal{S}$,

$$Y_{Q_{\overline{\mathcal{S}}}} = \sum_{j \in [m], i_j \neq i} (-1)^j Y_{Q_{\overline{\mathcal{S}_j}}} + \sum_{j \in [m], i_j = i} (-1)^j Y_{Q_{\overline{\mathcal{S}_j}}}, \tag{193}$$

where the first sum term contains $m-1$ terms and each term, $(-1)^j Y_{Q_{\overline{\mathcal{S}_j}}}$ satisfies that $1 \in \mathcal{S}_j, i \in \mathcal{S}_j$; and the second sum term contains only 1 term, $(-1)^j Y_{Q_{\overline{\mathcal{S}_j}}}, i_j = i$ so that $\mathcal{S}_j = \{i_1, i_2, \cdots, i_{j-1}, 1, i_{j+1}, \cdots, i_m\}$ and $1 \in \mathcal{S}_j, i \notin \mathcal{S}_j$. Plugging this property in the second term of the right-hand-side (RHS) of (192), we eliminate the contribution of the first term of RHS of (192) in the second term,

$$\begin{aligned} & \left(Y_{Q_{\overline{\mathcal{S}}}} : i \in \mathcal{S}, \mathcal{S} \in \binom{[\Delta]}{m}\right) \\ \overset{\text{invertible}}{\longleftrightarrow} \quad & \left(Y_{Q_{\overline{\mathcal{S}}}} : 1 \in \mathcal{S}, i \in \mathcal{S}, \mathcal{S} \in \binom{[\Delta]}{m}, Y_{Q_{\overline{\mathcal{S}_j}}} : 1 \in \mathcal{S}_j, i \notin \mathcal{S}_j, \mathcal{S} \in \binom{[\Delta]}{m}\right) && (194) \\ = \quad & \left(Y_{Q_{\overline{\mathcal{S}}}} : 1 \in \mathcal{S}, i \in \mathcal{S}, \mathcal{S} \in \binom{[\Delta]}{m}, Y_{Q_{\overline{\mathcal{S}_j}}} : 1 \in \mathcal{S}_j, i \notin \mathcal{S}_j, \mathcal{S}_j \in \binom{[\Delta]}{m}\right) && (195) \\ \overset{\text{invertible}}{\longleftrightarrow} \quad & \left(Y_{Q_{\overline{\mathcal{S}}}} : 1 \in \mathcal{S}, \mathcal{S} \in \binom{[\Delta]}{m}\right), && (196) \end{aligned}$$

where (195) follows from the fact that for distinct $\mathcal{S}$, $\mathcal{S}_j$ are also distinct, i.e., if $\mathcal{S}' \neq \mathcal{S}$, then $\mathcal{S}'_j$ is obtained from $\mathcal{S}'$ by replacing i by 1 and is not equal to $\mathcal{S}_j$ which is obtained from $\mathcal{S}$ by replacing i by 1.

Second, we prove (184) as a simple consequence of (182). Consider any $i \in [2:\Delta]$.

$$\begin{aligned} & \left(Y_{Q_{\overline{\mathcal{S}}}} : i \notin \mathcal{S}, \mathcal{S} \in \binom{[\Delta]}{m}\right) \\ \overset{\text{invertible}}{\longleftrightarrow} \quad & \left(Y_{Q_{\overline{\mathcal{S}}}} : 1 \in \mathcal{S}, i \notin \mathcal{S}, \mathcal{S} \in \binom{[\Delta]}{m}, Y_{Q_{\overline{\mathcal{S}}}} : 1 \notin \mathcal{S}, i \notin \mathcal{S}, \mathcal{S} \in \binom{[\Delta]}{m}\right), \end{aligned} \tag{197}$$

where the second term of RHS of (197) is a function of the first term due to the encoding (182), so $\left(Y_{Q_{\overline{\mathcal{S}}}} : i \notin \mathcal{S}, \mathcal{S} \in \binom{\Delta}{m}\right)$ is a function of the first term of RHS of (197) and this is our desired claim.

Third, we prove (185). It suffices to show that

$$\left(Y_{Q_{\overline{\mathcal{S}}}} : 1 \notin \mathcal{S}, 2 \notin \mathcal{S}, \mathcal{S} \in \binom{[\Delta]}{m}\right) \text{ is a function of } \left(Y_{Q_{\overline{\mathcal{S}}}} : 1 \notin \mathcal{S}, 2 \in \mathcal{S}, \mathcal{S} \in \binom{[\Delta]}{m}\right). \tag{198}$$

To this end, consider any $\mathcal{S} = \{i_1, \cdots, i_m\}$ such that $1 \notin \mathcal{S}, 2 \notin \mathcal{S}, \mathcal{S} \in \binom{[\Delta]}{m}$. From (182), we have

$$Y_{Q_{\overline{\mathcal{S}}}} = \sum_{j \in [m]} (-1)^j Y_{Q_{\overline{\mathcal{S}_j}}}, \tag{199}$$

where $\mathcal{S}_j = \{i_1, \cdots, i_{j-1}, 1, i_{j+1}, \cdots, i_m\}$. Define $\mathcal{S}'_j = \{i_1, \cdots, i_{j-1}, 2, i_{j+1}, \cdots, i_m\}$ and it turns out that

$$\sum_{j\in[m]} (-1)^j Y_{Q_{\overline{\mathcal{S}_j}}} = -\sum_{j\in[m]} (-1)^j Y_{Q_{\overline{\mathcal{S}'_j}}} \tag{200}$$

and the desired claim follows. So it remains to prove (200). We plug in the encoding function (182) to $Y_{Q_{\overline{\mathcal{S}'_j}}}$, where $\mathcal{S}'_j = \{2, i_1, \cdots, i_{j-1}, i_{j+1}, \cdots, i_m\}$ (note that $2 < i_1 < \cdots < i_{j-1} < i_{j+1} < \cdots i_m$).

$$\begin{aligned} Y_{Q_{\overline{\mathcal{S}'_j}}} &= -Y_{Q_{\overline{\{1,i_1,\cdots,i_{j-1},i_{j+1},\cdots,i_m\}}}} + Y_{Q_{\overline{\{2,1,\cdots,i_{j-1},i_{j+1},\cdots,i_m\}}}} - \cdots \\ &\quad +(-1)^j Y_{Q_{\overline{\{2,i_1,\cdots,1,i_{j+1},\cdots,i_m\}}}} + (-1)^{j+1} Y_{Q_{\overline{\{2,i_1,\cdots,i_j,1,\cdots,i_m\}}}} + \cdots \\ &\quad +(-1)^m Y_{Q_{\overline{\{2,i_1,\cdots,i_{j-1},i_{j+1},\cdots,1\}}}} \end{aligned} \tag{201}$$

and we show that the left-hand-side (LHS) of (200) is equal to RHS of (200). After expanding through (201), RHS of (200) contains more $Y_{Q_{\overline{\mathcal{S}}}}, 1 \in \mathcal{S}$ terms than those in LHS of (200). So we show that for the $Y_{Q_{\overline{\mathcal{S}}}}, 1 \in \mathcal{S}$ terms that exist in LHS, RHS has the same term and for the remaining $Y_{Q_{\overline{\mathcal{S}}}}, 1 \in \mathcal{S}$ terms that do not exist in LHS, they will cancel in RHS.

Consider any $Y_{Q_{\overline{\mathcal{T}}}}$ that is in LHS of (200), i.e., $\mathcal{T} = \{i_1, \cdots, i_{j-1}, 1, i_{j+1}, \cdots, i_m\}$ and it is equal to $(-1)^j Y_{Q_{\mathcal{T}}}$ in LHS. In RHS, we have the same term because it appears as the first term in (201), i.e., $-(-1)^j \times (-Y_{Q_{\overline{\mathcal{T}}}})$.

Consider any remaining $Y_{Q_{\overline{\mathcal{T}}}}$, i.e., $1 \in \mathcal{T}, 2 \in \mathcal{T}$ and $m-2$ elements from $i_1, \cdots, i_{j-1}, i_{j+1}, \cdots, i_m$ are in $\mathcal{T}$. For any $m-2$ such elements, $Y_{Q_{\overline{\mathcal{T}}}}$ will cancel in RHS of (200). We have two cases.

1. The $m-2$ elements are $i_1, \cdots, i_{t-1}, i_{t+1}, \cdots, i_{j-1}, i_{j+1}, \cdots, i_m$, i.e., i_t is missing and $1 \le t \le j-1$. $Y_{Q_{\overline{\mathcal{T}}}}, \mathcal{T} = \{1, 2, i_1, \cdots, i_{t-1}, i_{t+1}, \cdots, i_{j-1}, i_{j+1}, \cdots, i_m\}$ will cancel in RHS of (200) because it appears twice - for the first time $\mathcal{S}'_j = \{i_1, \cdots, i_t, \cdots i_{j-1}, 2, i_{j+1}, \cdots, i_m\}$ and i_t is replaced by 1 to become $\mathcal{T}$ in (201), i.e., $(-1)^j \times (-1)^{t+1} Y_{Q_{\overline{\mathcal{T}}}}$; for the second time, $\mathcal{S}'_t = \{i_1, \cdots, i_{t-1}, 2, i_{t+1}, \cdots, i_{j-1}, i_j, i_{j+1}, \cdots, i_m\}$ and i_j is replaced by 1 to become $\mathcal{T}$ in (201), i.e., $(-1)^t \times (-1)^j Y_{Q_{\overline{\mathcal{T}}}}$; thus the two $Y_{Q_{\overline{\mathcal{T}}}}$ terms have different signs and cancel.

2. The $m-2$ elements are $i_1, \cdots, i_{j-1}, i_{j+1}, \cdots, i_{t-1}, i_{t+1}, \cdots, i_m$, i.e., i_t is missing and $j+1 \le t \le m$. $Y_{Q_{\overline{\mathcal{T}}}}, \mathcal{T} = \{1, 2, i_1, \cdots, i_{j-1}, i_{j+1}, \cdots, i_{t-1}, i_{t+1}, \cdots, i_m\}$ will cancel in RHS of (200) because it appears twice - for the first time $\mathcal{S}'_j = \{i_1, \cdots i_{j-1}, 2, i_{j+1}, \cdots, i_t, \cdots, i_m\}$ and i_t is replaced by 1 to become $\mathcal{T}$ in (201), i.e., $(-1)^j \times (-1)^t Y_{Q_{\overline{\mathcal{T}}}}$; for the second time, $\mathcal{S}'_t = \{i_1, \cdots, i_{j-1}, i_j, i_{j+1}, \cdots, i_{t-1}, 2, i_{t+1}, \cdots, i_m\}$ and i_j is replaced by 1 to become $\mathcal{T}$ in (201), i.e., $(-1)^t \times (-1)^{j+1} Y_{Q_{\overline{\mathcal{T}}}}$; thus the two $Y_{Q_{\overline{\mathcal{T}}}}$ terms have different signs and cancel.

5.8 Proof of Theorem 7

First, consider the 'if' direction. We show that if the condition in Theorem 7 is satisfied for $C(\mathcal{G})$, $\mathcal{G} = ((\lambda_1, \cdots, \lambda_N), \mathcal{E})$, then for any $\mathcal{G}' = ((\lambda'_1, \cdots, \lambda'_{N'}), \mathcal{E}')$ such that $\mathcal{G}$ is a proper subgraph of $\mathcal{G}'$ we have $C(\mathcal{G}') = 0$. We have two cases for the proper subgraph.

1. $N = N'$ and $\mathcal{E}'$ contains at least one more hyperedge that is not in $\mathcal{E}$, denoted as e'. Then by the condition in Theorem 7, there exists one $e \in \mathcal{E}$ such that $\mathcal{D}(e') \cap \mathcal{D}(e) \in \{\emptyset, \mathcal{D}(e)\}$.

   (a) $\mathcal{D}(e') \cap \mathcal{D}(e) = \emptyset$. By the intersection bound (4), we have $C(\mathcal{G}') \le \Lambda(\mathcal{D}(e') \cap \mathcal{D}(e)) = 0$, as desired.

(b) $\mathcal{D}(e') \cap \mathcal{D}(e) = \mathcal{D}(e)$. Then $\mathcal{D}(e')$ is redundant for $\mathcal{G}'$ as a strict subset of $\mathcal{D}(e')$, $\mathcal{D}(e)$ is also a decoding set. Note that in our definition of storage graphs, we do not include redundant decoding sets so that this case violates the assumption that $\mathcal{G}$ is a proper subgraph of $\mathcal{G}'$ and cannot happen.

2. $N' > N$, i.e., $\mathcal{G}'$ contains at least one more storage node that is not in $\mathcal{G}$, say Q_{N+1}. As we do not include redundant storage nodes in our definition of storage graphs, $\mathcal{G}'$ must contain one decoding set that includes Q_{N+1}, denoted as $\mathcal{D}(e') = \{\mathcal{S}, Q_{N+1}\}$ where $\mathcal{S} \subset \{Q_1, \cdots, Q_N\}$. Then by the condition in Theorem 7, there exists one $e \in \mathcal{E}$ such that $\mathcal{S} \cap \mathcal{D}(e) \in \{\emptyset, \mathcal{D}(e)\}$.

   (a) $\mathcal{S} \cap \mathcal{D}(e) = \emptyset$. By the intersection bound (4), we have $C(\mathcal{G}') \leq \Lambda(\mathcal{D}(e') \cap \mathcal{D}(e)) = 0$.

   (b) $\mathcal{S} \cap \mathcal{D}(e) = \mathcal{D}(e)$. Then $\mathcal{D}(e')$ is a redundant decoding set for $\mathcal{G}'$ and $\mathcal{G}$ is not a proper subgraph of $\mathcal{G}'$.

Second, consider the 'only if' direction. We show that if the condition in Theorem 7 is not satisfied for $C(\mathcal{G})$, then there exists $\mathcal{G}'$ such that $\mathcal{G}$ is a proper subgraph of $\mathcal{G}'$ and $C(\mathcal{G}') > 0$.

When the condition in Theorem 7 is not satisfied, there exists a set of storage nodes, denoted as $\mathcal{S} \subset \{Q_1, \cdots, Q_N\}$ so that for any decoding set $\mathcal{D}(e), e \in \mathcal{E}$, we have $\mathcal{S} \cap \mathcal{D}(e) \notin \{\emptyset, \mathcal{D}(e)\}$, i.e., $\mathcal{S}$ intersects with every decoding set $\mathcal{D}(e)$ and is not equal to any $\mathcal{D}(e)$. As a result, we can include $\mathcal{S}$ as an additional non-redundant decoding set for $\mathcal{G}'$ and $C(\mathcal{G}') > 0$ as $\mathcal{G}'$ satisfies the condition for $C > 0$ in Corollary 2 (i.e., any two distinct decoding sets are intersecting).

5.9 Proof of Corollary 3

1. MDS graph $\mathcal{M}_{N,K}$. First, consider strong maximality. Suppose $2K - N = 1$ and consider any $\mathcal{S} \subset \{Q_1, \cdots, Q_N\}$. When $|\mathcal{S}| < K$, $\mathcal{S}^c$ must contain a decoding set as a subset, thus $\mathcal{S}$ is completely excluded by this decoding set; when $|\mathcal{S}| \geq K$, $\mathcal{S}$ must include a decoding set as a subset, i.e., this decoding set is completely included by $\mathcal{S}$. So the condition of Theorem 7 is satisfied and $\mathcal{M}_{2K-1,K}$ is strongly maximal. Suppose $2K - N > 1$ and consider $\mathcal{S} = \{Q_1, \cdots, Q_{K-1}\}$. Note that $\mathcal{S}$ intersects with any decoding set $\mathcal{D}(e)$, where $|\mathcal{D}(e)| = K$ as $K - 1 + K - N > 0$, so there is no decoding set that is completely included or excluded by $\mathcal{S}$, i.e., the condition in Theorem 7 is not satisfied and $\mathcal{M}_{N,K}, 2K - N > 1$ is not strongly maximal. To summarize, we have proved that $\mathcal{M}_{N,K}$ is strongly maximal if and only if $2K - N = 1$.

   Second, consider weak maximality. By definition, strongly maximal storage graphs are weakly maximal, so we only need to consider the cases not covered above, i.e., when $2K - N > 1$. For all $\mathcal{G}' = ((\lambda'_1, \cdots, \lambda'_N), \mathcal{E}')$ such that $\mathcal{G} = (\{\lambda_1, \cdots, \lambda_N\}, \mathcal{E}) = \mathcal{M}_{N,K}$ is a proper subgraph of $\mathcal{G}'$, there must exist (non-redundant) $e' \in \mathcal{E}'$ such that for all $e \in \mathcal{E}$, $\mathcal{D}(e') \cap \mathcal{D}(e) \notin \{\emptyset, \mathcal{D}(e)\}$.

   (a) $\mathcal{D}(e') \subset \{Q_1, \cdots, Q_N\}$. Then $|\mathcal{D}(e')| < K$ and $\mathcal{D}(e')$ intersects with every $\mathcal{D}(e), e \in \mathcal{E}$. Consider $\mathcal{D}(e)$ such that $|\mathcal{D}(e') \cap \mathcal{D}(e)|$ is the smallest among all $e \in \mathcal{E}$. By the intersection bound (4), $C(\mathcal{G}') \leq |\mathcal{D}(e') \cap \mathcal{D}(e)| < 2K - N = C(\mathcal{G}) = C(\mathcal{M}_{N,K})$.

   (b) $\mathcal{D}(e') \not\subset \{Q_1, \cdots, Q_N\}$. Then $\mathcal{D}(e')$ contains a subset $\mathcal{S}$ such that $\mathcal{S} \subset \{Q_1, \cdots, Q_N\}$, $\mathcal{S} \cap \mathcal{D}(e) \notin \{\emptyset, \mathcal{D}(e)\}$ and then $|\mathcal{S}| < K$. The same argument as above shows that $C(\mathcal{G}') < C(\mathcal{G})$.

So the definition of weak maximality is satisfied.

2. Wheel graph $\mathcal{W}_N$. We show that $\mathcal{W}_N, N \geq 4$ is strongly maximal by verifying the condition in Theorem 7. Consider any $\mathcal{S} \subset \mathcal{Q} = \{Q_1, \cdots, Q_N\}$.

   (a) When $Q_1 \in \mathcal{S}$, then $\mathcal{S}$ must be decoding set $\{Q_1, Q_i\}$ for some $i \in [2:N]$ or must include decoding set $\{Q_1, Q_i\}$ for some $i \in [2:N]$. Thus there exists a decoding set that is completely included by $\mathcal{S}$.

   (b) When $Q_1 \notin \mathcal{S}$, then $\mathcal{S}$ is either equal to decoding set $\{Q_2, \cdots, Q_N\}$ or is completely excluded by decoding set $\{Q_1, Q_i\}$ for some $i \in [2:N]$.

3. Fano graph $\mathcal{F}_7$. We show that $\mathcal{F}_7$ is strongly maximal by verifying the condition in Theorem 7. As $\mathcal{F}_7$ only contains 7 storage nodes, we may verify through checking all $\mathcal{S} \subset \mathcal{Q} = \{Q_1, \cdots, Q_7\}$. When $|\mathcal{S}| \geq 4$, $\mathcal{S}$ either contains a decoding set or is equal to the complement of a decoding set. When $|\mathcal{S}| \leq 3$, $\mathcal{S}$ is either a decoding set or is a subset of the complement of some decoding set.

4. Intersection graph $\sqcap_{\Delta,m}$. As strongly maximal storage graphs are by definition also weakly maximal storage graphs, we only need to prove the if direction for strong maximality (when $\Delta = 3, m = 2$, $\sqcap_{3,2}$ is isomorphic to MDS graph $\mathcal{M}_{3,2}$, so this has been proved above) and the only if direction for weak maximality, presented next. We show that we may include a non-redundant decoding set to $\sqcap_{\Delta,m}$ that intersects with every existing decoding sets while the capacity remains the same so $\sqcap_{\Delta,m}, (\Delta, m) \neq (3,2), \Delta > m$ is not weakly maximal. Specifically, for $\mathcal{G} = ((\lambda_1, \cdots, \lambda_N), \mathcal{E}) = \sqcap_{\Delta,m}$, we set $\mathcal{G}' = ((\lambda_1, \cdots, \lambda_N), \mathcal{E}')$ where $\mathcal{E}' = \mathcal{E} \cup e^*$ and

$$\mathcal{D}(e^*) = \{\mathcal{D}(e_2) \setminus Q_{\overline{\{2,\Delta-m+2,\cdots,\Delta-1,\Delta\}}}\} \cup \left\{Q_{\overline{\{i,\Delta-m+2,\cdots,\Delta-1,\Delta\}}} : i \in \{1,3,\cdots,\Delta-m+1\}\right\}, \tag{202}$$

   i.e., the additional decoding set is chosen as deleting one element in $\mathcal{D}(e_2)$ and including $\Delta - m$ elements (specifically, deleting the last one in lexicographic order and including through replacing 2 by each of $\{1,3,\cdots,\Delta-m+1\}$ in the label). $\mathcal{D}(e^*) \cap \mathcal{D}(e) \notin \{\emptyset, \mathcal{D}(e)\}$ for all $e \in \mathcal{E}$ and $C(\mathcal{G}') = C(\mathcal{G})$ because the same code for $\sqcap_{\Delta,m}$ in Section 5.7 continues to work. The decoding and security constraint of the corresponding classical code for decoding set $\mathcal{D}(e^*)$ is guaranteed by proving similar arguments to (183), (184).

6 Discussion and Open Problems

In this work, we have explored the capacity of storing a quantum message over a number of storage nodes of certain specified relative sizes such that from certain specified subsets of the storage nodes, the message must be perfectly recovered. The problem is surprisingly rich as it is intimately related to a corresponding classical secure storage problem. This stands in sharp contrast to the problem of storing a *classical* message (over either classical or quantum storage nodes) where the cut-set bound (Holevo bound for quantum storage nodes) is tight; such a significant difference stems from the distinct properties of quantum systems, in particular the no-cloning theorem that introduces additional security constraints. The quantum storage problem turns out to be quite challenging as the related (via CSS codes) classical secure storage problem can be equivalently

formulated as a secure network coding problem, which is known to be hard [36]. In light of this connection, we have applied an interference alignment perspective to obtain various code constructions and provided tight converse bounds through quantum information inequalities. As an initial step towards an important capacity problem that has not been considered in the literature, there are many interesting future research avenues and open problems and we list a few in the following.

1. Is the achievable scheme in Theorem 2 always tight? Equivalently, we may view the classical secure storage problem (6), (7) as a stand-alone problem and ask if the capacity of this stand-alone classical secure storage problem is always equal to the capacity of the quantum storage problem, $C(\mathcal{G})$? For the cases settled in this work, the answer is yes while the general case is open and interesting, because if the general answer is yes, then the quantum storage problem fully reduces to a classical secure storage problem.

2. What is the capacity of the wheel graph $C(\mathcal{W}_N)$ in general, particularly $N \geq 6$? What is the capacity of the intersection graph $C(\sqcap_{\Delta,m})$ in general?

3. Extremal rate values for uniform storage: if $C(\mathcal{G}) \neq 0$, then what is the smallest (across all feasible storage graphs $\mathcal{G}$ with N storage nodes) capacity value $C_u(\mathcal{G})$ as a function of N? In other words, what is the worst storage graph in terms of storage capacity for a fixed number of storage nodes N? Generalizing Csirmaz's lower bound [37] from classical secret sharing to quantum storage, we can find a graph with polynomially small (in N) storage capacity, but can the capacity be exponentially small?

4. Additivity of combined storage: given storage graphs $\mathcal{G}_1 = ((\alpha_1, \cdots, \alpha_{N_1}), \mathcal{E}_1)$ and $\mathcal{G}_2 = ((\beta_1, \cdots, \beta_{N_2}), \mathcal{E}_2)$, for distinct storage systems (the storage nodes are disjoint), the combined storage graph can be defined as $\mathcal{G}_{12} \triangleq ((\alpha_1, \cdots, \alpha_{N_1}, \beta_1, \cdots, \beta_{N_2}), \mathcal{E}_{12})$ where

$$\mathcal{G}_{12} \text{ has } N_1 + N_2 \text{ storage nodes,} \tag{203}$$

$$\mathcal{E}_{12} = \{e_1 \cup e_2 \mid e_1 \in \mathcal{E}_1, e_2 \in \mathcal{E}_2\}. \tag{204}$$

   Clearly $C(\mathcal{G}_{12}) \geq C(\mathcal{G}_1) + C(\mathcal{G}_2)$ since quantum information can be divided into two parts with the parts stored separately in $\mathcal{G}_1, \mathcal{G}_2$. The question is, can the combined capacity ever be strictly larger than the sum of capacities? In other words, is storage capacity always *additive* or can it be *super-additive*? A special case worth considering is the combination of a zero storage capacity system with any other system, i.e., if $C(\mathcal{G}_1) = 0$, then is $C(\mathcal{G}_{12}) = C(\mathcal{G}_2)$? Or even more specifically, what if $\mathcal{G}_1 = ((1, 1), \{\{1\}, \{2\}\})$?

References

[1] M. Grassl, "Bounds on the minimum distance of linear codes and quantum codes," *available online at http://www.codetables.de*, 2007 (recently updated in 2024).

[2] J. S. Gundersen, R. B. Christensen, M. Grassl, P. Popovski, and R. Wisniewski, "Puncturing quantum stabilizer codes," *IEEE Journal on Selected Areas in Information Theory*, vol. 6, p. 74–84, 2025.

[3] M. Grassl, F. Huber, and A. Winter, "Entropic proofs of singleton bounds for quantum error-correcting codes," *IEEE Transactions on Information Theory*, vol. 68, no. 6, pp. 3942–3950, 2022.

[4] M. Mamindlapally and A. Winter, "Singleton bounds for entanglement-assisted classical and quantum error correcting codes," *IEEE Trans. Inf. Theory*, vol. 69, pp. 5857–5868, Sept. 2023.

[5] E. Knill and R. Laflamme, "Theory of quantum error-correcting codes," *Physical Review A*, vol. 55, no. 2, p. 900, 1997.

[6] E. M. Rains, "Nonbinary quantum codes," *IEEE Transactions on Information Theory*, vol. 45, no. 6, pp. 1827–1832, 1999.

[7] N. J. Cerf and R. Cleve, "Information-theoretic interpretation of quantum error-correcting codes," *Physical Review A*, vol. 56, no. 3, p. 1721, 1997.

[8] F. Huber and M. Grassl, "Quantum codes of maximal distance and highly entangled subspaces," *Quantum*, vol. 4, p. 284, 2020.

[9] M. Grassl, T. Beth, and T. Pellizzari, "Codes for the quantum erasure channel," *Phys. Rev. A*, vol. 56, pp. 33–38, Jul 1997.

[10] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, "Nonbinary stabilizer codes over finite fields," *IEEE Transactions on Information Theory*, vol. 52, no. 11, pp. 4892–4914, 2006.

[11] M. Grassl and M. Rötteler, "Quantum MDS codes over small fields," in *2015 IEEE International Symposium on Information Theory (ISIT)*, pp. 1104–1108, IEEE, 2015.

[12] K. Tiurev, P.-J. H. S. Derks, J. Roffe, J. Eisert, and J.-M. Reiner, "Correcting non-independent and non-identically distributed errors with surface codes," *Quantum*, vol. 7, p. 1123, Sept. 2023.

[13] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Physical Review A*, vol. 54, no. 2, p. 1098, 1996.

[14] A. Steane, "Multiple-particle interference and quantum error correction," *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, vol. 452, no. 1954, pp. 2551–2577, 1996.

[15] A. D. Smith, "Quantum secret sharing for general access structures," *arXiv preprint quant-ph/0001087*, 2000.

[16] M. Hayashi and S. Song, "Unified approach to secret sharing and symmetric private information retrieval with colluding servers in quantum systems," *IEEE Transactions on Information Theory*, vol. 69, no. 10, pp. 6537–6563, 2023.

[17] M. Hayashi, *Quantum information: an introduction*. Springer, 2006.

[18] M. M. Wilde, *Quantum information theory*. Cambridge university press, 2013.

[19] J. Cannons, R. Dougherty, C. Freiling, and K. Zeger, "Network routing capacity," *IEEE Transactions on Information Theory*, vol. 52, no. 3, pp. 777–788, 2006.

[20] S. Loyka and C. D. Charalambous, "A general formula for compound channel capacity," *IEEE Transactions on Information Theory*, vol. 62, no. 7, pp. 3971–3991, 2016.

[21] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, 1982.

[22] D. Dieks, "Communication by EPR devices," *Physics Letters A*, vol. 92, no. 6, pp. 271–272, 1982.

[23] E. H. Lieb and M. B. Ruskai, "Proof of the strong subadditivity of quantum-mechanical entropy," *J. Math. Phys*, vol. 14, no. 12, 1973.

[24] N. Pippenger, "The inequalities of quantum information theory," *IEEE Transactions on Information Theory*, vol. 49, no. 4, pp. 773–789, 2003.

[25] K. Senthoor and P. K. Sarvepalli, "Concatenating extended CSS codes for communication efficient quantum secret sharing," in *2023 12th International Symposium on Topics in Coding (ISTC)*, pp. 1–5, IEEE, 2023.

[26] Z. Li and H. Sun, "Conditional disclosure of secrets: A noise and signal alignment approach," *IEEE Transactions on Communications*, vol. 70, no. 6, pp. 4052–4062, 2022.

[27] Z. Li and H. Sun, "On the linear capacity of conditional disclosure of secrets," *IEEE Transactions on Communications*, vol. 71, no. 12, pp. 7218–7227, 2023.

[28] Z. Li and H. Sun, "On extremal rates of storage over graphs," *IEEE Transactions on Information Theory*, vol. 70, no. 4, pp. 2464–2478, 2023.

[29] Z. Li and H. Sun, "On extremal rates of secure storage over graphs," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 4721–4731, 2023.

[30] H. Sun and S. A. Jafar, "The capacity of private computation," *IEEE Transactions on Information Theory*, vol. 65, no. 6, pp. 3880–3897, 2018.

[31] K. Wan, H. Sun, M. Ji, D. Tuninetti, and G. Caire, "On the optimal load-memory tradeoff of cache-aided scalar linear function retrieval," *IEEE Transactions on Information Theory*, vol. 67, no. 6, pp. 4001–4018, 2021.

[32] K. Wan, X. Yao, H. Sun, M. Ji, and G. Caire, "On the information theoretic secure aggregation with uncoded groupwise keys," *IEEE Transactions on Information Theory*, vol. 70, no. 9, pp. 6596–6619, 2024.

[33] K. Wan, H. Sun, M. Ji, T. Mi, and G. Caire, "The capacity region of information theoretic secure aggregation with uncoded groupwise keys," *IEEE Transactions on Information Theory*, vol. 70, no. 10, pp. 6932–6949, 2024.

[34] B. Schumacher and M. A. Nielsen, "Quantum data processing and error correction," *Physical Review A*, vol. 54, no. 4, p. 2629, 1996.

[35] A. Beimel, "Secret-sharing schemes for general access structures: An introduction," *Cryptology ePrint Archive*, 2025.

[36] W. Huang, T. Ho, M. Langberg, and J. Kliewer, "Single-unicast secure network coding and network error correction are as hard as multiple-unicast network coding," *IEEE Transactions on Information Theory*, vol. 64, no. 6, pp. 4496–4512, 2018.

[37] L. Csirmaz, "The size of a share must be large," *Journal of cryptology*, vol. 10, no. 4, pp. 223–231, 1997.