Quantum Codes of Maximal Distance and Highly Entangled Subspaces

Felix Huber[1,2,3] and Markus Grassl[4,5]

[1]ICFO - The Institute of Photonic Sciences, 08860 Castelldefels (Barcelona), Spain

[2]Institut für Theoretische Physik, Universität zu Köln, 50937 Köln, Germany

[3]Naturwissenschaftlich-Technische Fakultät, Universität Siegen, 57068 Siegen, Germany

[4]International Centre for Theory of Quantum Technologies, University of Gdansk, 80-308 Gdańsk, Poland

[5]Max Planck Institute for the Science of Light, 91058 Erlangen, Germany

June 15, 2020

We present new bounds on the existence of general quantum maximum distance separable codes (QMDS): the length n of all QMDS codes with local dimension D and distance $d \geq 3$ is bounded by $n \leq D^2 + d - 2$. We obtain their weight distribution and present additional bounds that arise from Rains' shadow inequalities. Our main result can be seen as a generalization of bounds that are known for the two special cases of stabilizer QMDS codes and absolutely maximally entangled states, and confirms the quantum MDS conjecture in the special case of distance-three codes. As the existence of QMDS codes is linked to that of highly entangled subspaces (in which every vector has uniform r-body marginals) of maximal dimension, our methods directly carry over to address questions in multipartite entanglement.

1 Introduction

The processing of information with quantum particles is inevitably affected by disturbance from the environment. By distributing the information onto many particles, quantum error correcting codes (QECC) can safeguard quantum information from unwanted noise. In this way, a limited amount of corruption or even particle-loss can be tolerated. Since the discovery of quantum error correction [1, 2] and the establishment of its theoretical foundations [3–6], the search for "good" codes with desirable characteristics has been an ongoing endeavor. Both increasingly better-performing codes [7–12] as well as stricter bounds imposed upon their existence have been found [13, 14].

The *quantum Singleton bound* can be seen as having its origins in the no-cloning theorem [15, 16]. It states that the parameters of any quantum error correction code of distance d, encoding states from $\mathbb{C}^K$ into a subspace of n systems with local dimensions D each, are bounded by

$$K \leq D^{n-2(d-1)}. \qquad (1)$$

Codes achieving this bound are called quantum maximum distance separable (QMDS) [3, 17]. Hugging the fundamental limit of no-cloning, one can expect these codes to have particularly intriguing features.

The study of multipartite entanglement has led to the discovery of different types of entanglement that can be shared by three or more quantum particles [18–20]. In turn, subspaces whose vectors show interesting entanglement properties have been investigated, such as those showing a bounded Schmidt rank [21], having a negative partial transpose [22], and being completely [23, 24] or genuinely entangled [25–27].

Generalizing the concept of maximal bipartite entanglement, r-uniform states are a particular type of highly entangled pure quantum states: these states exhibit maximal entanglement between any r particles and the rest, in the sense that all of their r-sized marginals are maximally mixed (i.e. uniform).

It is reasonable to think that there are not too many states with this property, and one might be tempted to ask the following question: given a number n of D-level quantum systems, what is the largest possible subspace in which every state vector is r-uniform? In other words, what is the dimension of the largest possible *r-uniform subspace* (rUS), and by what methods can this subspace be characterized?

It can be established that the concepts of so-called *pure* QECC and rUS are in fact equivalent [28]. Consequently, the attainable dimensions of both objects are constrained by the quantum Singleton bound. In this article, we will focus on the case of QECC and rUS achieving this bound, that is, on general QMDS codes and their corresponding highly entangled subspaces. All of our results can thus be seen as results concerning both coding and entanglement theory, and we will use methods from quantum error correction to answer questions in multipartite entanglement, and vice versa.

Felix Huber: felix.huber@icfo.eu
Markus Grassl: markus.grassl@ug.edu.pl

Accepted in ⟨quantum⟩ 2020-06-09, click title to verify. Published under CC-BY 4.0.

1

While the quantum Singleton bound was one of the earliest bounds obtained on quantum codes, not much more about the structural properties of QMDS codes is known than what was already obtained by Rains in Ref. [17]. Explicit constructions for stabilizer QMDS codes from classical maximal distance separable codes followed [29–31], and QMDS codes were later understood to constitute optimal ramp secret sharing schemes [32].

It turns out that there are stronger constraints for the existence of QMDS codes than their parameters meeting the quantum Singleton bound, the full set of which are not yet known. Similarly, classical MDS codes have been studied for more than half a century, but despite of that, the exact conditions for their existence have not yet been entirely resolved [33, 34].

In this article, we obtain two new bounds: first, we prove that for *any* (both stabilizer and non-stabilizer) QMDS code [respectively $(d-1)$-uniform subspace satisfying the Singleton bound] to exist, the following condition has to be met,

$$n \leq D^2 + d - 2 \,. \qquad (2)$$

The result is obtained by a systematic investigation of certain families of QMDS codes. Second, we use Rains' shadow inequality to further restrict the allowed parameters in the case of small "alphabets". This can be seen as additional constraints that originate in the monogamy of entanglement [35].

Furthermore, we derive the weight distribution of QMDS codes, a useful tool for the analysis and characterization of codes; it is seen that the weights are solely determined by the parameters of the code, regardless how the code was constructed. Note that all quantum MDS codes found to date are constructed from classical MDS codes, in particular using the stabilizer theory. Yet, even if one would find a different construction for quantum MDS codes, their quantum weight distribution has to match that of their classical MDS counterpart. Hence it is an intriguing question whether or not there exist QMDS codes that do not arise from any classical construction.

The structure of this article is as follows: connections between quantum error correcting codes and highly entangled subspaces are drawn in Sections 2 and 3. Then, Sections 4 and 5 introduce methods that are needed for the proofs that follow: the machinery of quantum weight enumerators and descendance rules for pure codes are presented. Sections 6 and 7 introduce quantum maximum distance separable codes and the families formed thereof. The weights of QMDS codes are derived in Section 8. This results in bounds on the existence of QMDS codes (Sections 9 and 10). The QMDS conjecture is treated in Section 11, before concluding in Section 12. The appendices contain proofs of the quantum Singleton bound and an overview on previous bounds for stabilizer QMDS codes and AME states. This is followed by detailed tables on known QMDS constructions and bounds on their existence for small local dimensions.

2 Quantum error correcting codes

A quantum error correcting code $\mathcal{Q} = ((n, K, d))_D$ is a K-dimensional subspace of $(\mathbb{C}^D)^{\otimes n}$ such that every error affecting at most $d-1$ subsystems can either be detected or acts trivially on the code, i.e., introduces at most a global phase factor. Here, the parameter d is the distance and a code with $d \geq 2t + 1$ allows to correct any error that affects up to t subsystems, e.g. the complete depolarization of any t subsystems.

Let us gently introduce some notation to make this precise: denote by $\{e_a : a = 0, \ldots, D^2 - 1\}$ an orthogonal operator basis for $\mathbb{C}^D$ that includes the identity $e_0 = \mathbb{1}$, such that $\mathrm{tr}(e_a^\dagger e_b) = D\delta_{ab}$. By taking n-fold tensor products of elements in $\{e_a\}$ we obtain a so-called local error basis $\{E_{\boldsymbol{a}}\}$ on $(\mathbb{C}^D)^{\otimes n}$ satisfying $\mathrm{tr}(E_{\boldsymbol{a}}^\dagger E_{\boldsymbol{b}}) = D^n \delta_{\boldsymbol{ab}}$. The support of an error-operator $E_{\boldsymbol{a}}$, that is, the subsystems it acts non-trivially on, is denoted by $\mathrm{supp}(E_{\boldsymbol{a}})$. The weight of $E_{\boldsymbol{a}}$ is the size of its support, $\mathrm{wt}(E_{\boldsymbol{a}}) = |\mathrm{supp}(E_{\boldsymbol{a}})|$. Finally, let $\{|i_{\mathcal{Q}}\rangle : i = 1, \ldots, K\}$ be a set of orthogonal unit vectors spanning $\mathcal{Q}$. Then $\Pi_{\mathcal{Q}} = \sum |i_{\mathcal{Q}}\rangle\langle i_{\mathcal{Q}}|$ is the projector onto the code space.

For $\mathcal{Q}$ to be a QECC with minimum distance d, a necessary and sufficient criterion is for

$$\langle i_{\mathcal{Q}}| E_{\boldsymbol{a}} |j_{\mathcal{Q}}\rangle = C(E_{\boldsymbol{a}}) \, \delta_{ij} \qquad (3)$$

to hold for all pairs $|i_{\mathcal{Q}}\rangle, |j_{\mathcal{Q}}\rangle$ and errors $E_{\boldsymbol{a}}$ of weight strictly less than d [36]. Note that $C(E_{\boldsymbol{a}}) \in \mathbb{C}$ is a constant that depends only on the specific error $E_{\boldsymbol{a}}$, but not on the vectors $|i_{\mathcal{Q}}\rangle$ and $|j_{\mathcal{Q}}\rangle$. A code is called *pure* if $C(E_{\boldsymbol{a}}) = \mathrm{tr}(E_{\boldsymbol{a}})/D^n = 0$ for all $E_{\boldsymbol{a}}$ with $0 < \mathrm{wt}(E_{\boldsymbol{a}}) < d$. In other words, the constant $C(E_{\boldsymbol{a}})$ of pure codes vanishes for all non-trivial errors that the code is designed to detect.

For one of the proofs that follow, we will also need an entropic condition on quantum error correction: consider the purification of $\varrho = \Pi_{\mathcal{Q}}/K$ with a reference system R of dimension K, $|\phi_{\mathcal{Q}}\rangle = \frac{1}{\sqrt{K}} \sum_{i=1}^{K} |i_R\rangle \otimes |i_{\mathcal{Q}}\rangle$. The von Neumann entropy of a subsystem I is given by $S(\varrho_I) = -\sum_i \lambda_i \log(\lambda_i)$, where λ_i are the eigenvalues of the reduced density matrix ϱ_I for the subsystem I. For the code to have distance d, a necessary and sufficient condition is that $S_{RA} = S_R + S_A$ holds for every subsystem A with $|A| < d$, that is, the reference system R and the subsystem A are uncorrelated. From the conditions on equality in the strong subadditivity, an equivalent formulation is that $\varrho_{RA} = \varrho_R \otimes \varrho_A$ must hold.

3 Highly entangled subspaces

A pure state $|\phi\rangle$, whose reductions onto r parties are all maximally mixed, is termed *r-uniform*. That is,

$\operatorname{tr}_{S^c}(|\phi\rangle\langle\phi|) \propto \mathbb{1}$ for every subset $S \subseteq \{1, \ldots, n\}$ of size $|S| \leq r$, where S^c denotes its complement. An r-*uniform subspace* (rUS) is a subspace of $(\mathbb{C}^D)^{\otimes n}$ in which every vector is at least r-uniform. In other words, every vector $|\phi\rangle$ lying in an rUS satisfies that for all error operators with $\operatorname{supp}(E_{\boldsymbol{a}}) \subseteq S$ where $|S| \leq r$

$$\langle\phi| E_{\boldsymbol{a}} |\phi\rangle = \operatorname{tr}[\underbrace{\operatorname{tr}_{S^c}(|\phi\rangle\langle\phi|)}_{\propto \mathbb{1}} \operatorname{tr}_{S^c}(E_{\boldsymbol{a}})] = \operatorname{tr}(E_{\boldsymbol{a}})/D^n .$$
(4)

Accordingly, $|\phi\rangle$ is maximally entangled across any bipartition of size r vs. $n-r$, having the largest possible von Neumann entropy on the smaller reduction.

From the definition of a QECC in Eq. (3), it is not hard to see that a pure code with parameters $((n, K, r+1))_D$ implies the existence of an r-uniform subspace of $(\mathbb{C}^D)^{\otimes n}$ with dimension K. In fact, the converse statement is also true: the existence of an r-uniform subspace implies that of a pure QECC of distance $r + 1$. The proof is based on an equivalent condition for a subspace $\mathcal{Q}$ to be a QECC, namely that the expectation value

$$\langle\phi| E |\phi\rangle = C(E)$$
(5)

is constant for all $|\phi\rangle$ ranging over the subspace $\mathcal{Q}$ and operators E with support on less than d parties. The claim then follows by considering pure codes for which $C(E) = 0$ when $0 < \operatorname{wt}(E) < d$.

The equivalence of Eq. (3) and Eq. (5) has already been established, and we sketch the proof [37, 38]: expanding $|\phi\rangle$ in the logical basis $\{|i_{\mathcal{Q}}\rangle\}$ and E in a Hermitean error basis $\{E_{\boldsymbol{a}}\}$, Eq. (3) implies Eq. (5). The converse can be established by defining the inner product $\langle v, w\rangle_{E_{\boldsymbol{a}}} := \langle v| (E_{\boldsymbol{a}} + \lambda\mathbb{1}) |w\rangle$, and its associated norm $||v||_{E_{\boldsymbol{a}}} = \sqrt{\langle v, v\rangle_{E_{\boldsymbol{a}}}}$, where $\lambda \geq 0$ is chosen such that $E_{\boldsymbol{a}} + \lambda\mathbb{1} \geq 0$. With the complex polarization identity

$$\langle v, w\rangle_{E_{\boldsymbol{a}}} = \frac{1}{4}\big(||v+w||^2_{E_{\boldsymbol{a}}} - ||v-w||^2_{E_{\boldsymbol{a}}} + i||v-iw||^2_{E_{\boldsymbol{a}}} - i||v+iw||^2_{E_{\boldsymbol{a}}} \big)$$
(6)

and the decomposition of $|i_{\mathcal{Q}}\rangle$ and $|j_{\mathcal{Q}}\rangle$ into sum and differences (with and without a complex phase i) of two vectors $|\psi\rangle, |\phi\rangle \in \mathcal{Q}$, it is seen that Eq. (5) implies Eq. (3). Therefore, the formulations of Eq. (3) and Eq. (5) are equivalent.

Considering these two definitions for the case of pure codes, one arrives at the following observation.

Observation 1 (Equivalence of pure QECC and rUS). *The following objects are equivalent:*
1. a pure $((n, K, d))_D$ quantum error correcting code;
2. a $(d-1)$-uniform subspace in $(\mathbb{C}^D)^{\otimes n}$ of dimension K.

Thus the question about the maximal dimension that an r-uniform subspace can attain is one-to-one related to the maximal dimension of pure codes. In what follows we will mostly focus on pure codes, as the corresponding results for uniform subspaces can simply be read off Observation 1.

4 Weight enumerators

We will make use of *weight enumerators* in the proofs that follow. Their knowledge is not required to understand the main result [Theorem 10] of this article (if Theorem 2 is accepted); in that case this section can be skipped.

For classical codes, the weight enumerator counts the number of codewords of a given Hamming weight. Although there is no such direct combinatorial interpretation of the quantum weight enumerator, it has been shown [39, 40] that quantum weight enumerators are a useful tool for the characterization of quantum codes and that they can, for example, be employed to determine their distance, as well as to derive other properties of putative codes or to show their non-existence.

Given a local error basis $\{E_{\boldsymbol{a}}\}$ with $\operatorname{tr}(E_{\boldsymbol{a}}^\dagger E_{\boldsymbol{b}}) = D^n \delta_{\boldsymbol{ab}}$, define the Shor-Laflamme weights of a code $\mathcal{Q}$ with associated projector $\Pi_{\mathcal{Q}}$ as [39, 40]

$$A_j(\Pi_{\mathcal{Q}}) = \sum_{\operatorname{wt}(E_{\boldsymbol{a}})=j} \operatorname{tr}[E_{\boldsymbol{a}}^\dagger \Pi_{\mathcal{Q}}] \operatorname{tr}[E_{\boldsymbol{a}} \Pi_{\mathcal{Q}}],$$
(7)

$$B_j(\Pi_{\mathcal{Q}}) = \sum_{\operatorname{wt}(E_{\boldsymbol{a}})=j} \operatorname{tr}[E_{\boldsymbol{a}}^\dagger \Pi_{\mathcal{Q}} E_{\boldsymbol{a}} \Pi_{\mathcal{Q}}].$$
(8)

The sum above is taken over all errors $E_{\boldsymbol{a}}$ of weight j in the basis. Note that $A_j = A_j(\Pi_{\mathcal{Q}})$ is simply the Hilbert-Schmidt norm of all correlations in the code that act on exactly j parties non-trivially. Both A_j and B_j are non-negative quantities that are invariant under the action of local unitaries $\mathcal{U}_1 \otimes \cdots \otimes \mathcal{U}_n$ [1], and thus do not depend on the specific orthonormal error basis chosen.

We will also need Rains' *unitary* weights [40], defined as

$$A'_j(\Pi_{\mathcal{Q}}) = \sum_{|S|=j} \operatorname{tr}[\operatorname{tr}_{S^c}(\Pi_{\mathcal{Q}}) \operatorname{tr}_{S^c}(\Pi_{\mathcal{Q}})],$$
(9)

$$B'_j(\Pi_{\mathcal{Q}}) = \sum_{|S|=j} \operatorname{tr}[\operatorname{tr}_S(\Pi_{\mathcal{Q}}) \operatorname{tr}_S(\Pi_{\mathcal{Q}})],$$
(10)

where the sum is over all subsets $S \subseteq \{1, \ldots, n\}$ of size j. For readers familiar with measures in quantum information, these quantities are proportional to the average purities of suitably normalized reductions of

---

[1] This can be seen from the fact that the purities $\operatorname{tr}[\operatorname{tr}_{S^c}(\Pi_{\mathcal{Q}})^2]$ of reductions can be expressed in terms of the weights A_j. In turn, the dual weights B_j can be expressed as linear combinations of A_j; this follows from the quantum MacWilliams identity [39–41]

size j and $n-j$, respectively.[2] From the definition, $A'_j = B'_{n-j}$.

A fine-graining of both types of weights will prove useful for later proofs:

$$\mathcal{A}_S(\Pi_{\mathcal{Q}}) = \sum_{\mathrm{supp}(E_{\boldsymbol{a}})=S} \mathrm{tr}[E_{\boldsymbol{a}}^\dagger \Pi_{\mathcal{Q}}]\,\mathrm{tr}[E_{\boldsymbol{a}}\Pi_{\mathcal{Q}}], \quad (11)$$

$$\mathcal{B}_S(\Pi_{\mathcal{Q}}) = \sum_{\mathrm{supp}(E_{\boldsymbol{a}})=S} \mathrm{tr}[E_{\boldsymbol{a}}^\dagger \Pi_{\mathcal{Q}} E_{\boldsymbol{a}} \Pi_{\mathcal{Q}}]. \quad (12)$$

$$\mathcal{A}'_S(\Pi_{\mathcal{Q}}) = \mathrm{tr}[\mathrm{tr}_{S^c}(\Pi_{\mathcal{Q}})\,\mathrm{tr}_{S^c}(\Pi_{\mathcal{Q}})], \quad (13)$$

$$\mathcal{B}'_S(\Pi_{\mathcal{Q}}) = \mathrm{tr}[\mathrm{tr}_{S}(\Pi_{\mathcal{Q}})\,\mathrm{tr}_{S}(\Pi_{\mathcal{Q}})]. \quad (14)$$

These are simply the non-symmetrized versions of Eqs. (7) to (10) for a fixed subset S.

The following facts about the weights of codes are known [40]: necessary and sufficient conditions for a projector Π of rank K to be a QECC of distance d are

$$KB_j(\Pi) = A_j(\Pi) \quad \text{for} \quad 0 \le j < d. \quad (15)$$

These conditions can be restated in terms of the unitary enumerators. The quantities A'_j and B'_j are linear functions of the quantities A_i and B_i with $i \le j$ respectively,[3]

$$A'_j(\Pi) = \sum_{i \le j} D^{-j} \binom{n-i}{n-j} A_i(\Pi), \quad (16)$$

$$B'_j(\Pi) = \sum_{i \le j} D^{-j} \binom{n-i}{n-j} B_i(\Pi). \quad (17)$$

(Note that this resembles the notion of binomial moments in [42].) Hence the relations of Eq. (15) are equivalent to

$$KB'_j(\Pi) = A'_j(\Pi) \quad \text{for} \quad 0 \le j < d. \quad (18)$$

Generally, one has that $KB_j \ge A_j$ and $KB'_j \ge A'_j$ for all j, while $KB_0 = A_0 = K^2$.

Analogous relations hold for subsets. Let T be a subset of size less than d. From the conditions for the image of a projector to be a code subspace [Eq. (15)] it follows that $K\mathcal{B}_T = \mathcal{A}_T$, while generally $K\mathcal{B}_S \ge \mathcal{A}_S$ holds.[4] Similarly, it can be seen that $K\mathcal{B}'_T = \mathcal{A}'_T$ holds, while $K\mathcal{B}'_S \ge \mathcal{A}'_S$ for arbitrary subsets S. (In terms of purities of the normalized projector $\varrho = \Pi_{\mathcal{Q}}/K$, this simply amounts to $K\,\mathrm{tr}[\mathrm{tr}_T(\varrho)^2] \ge \mathrm{tr}[\mathrm{tr}_{T^c}(\varrho)^2]$, with equality for all subsets $|T| < d$.)

From the definition in Eq. (3), it follows that *pure* codes are those with $A_j = 0$ [or correspondingly, $A'_j = \binom{n}{j}K^2 D^{-j}$] for all $0 < j < d$. These are codes whose spanning vectors have maximally mixed $(d-1)$-body marginals, and correspond to r-uniform subspaces.

[2] If $\Pi_{\mathcal{Q}}$ is normalized to a quantum state $\varrho = \Pi_{\mathcal{Q}}/K$, $A'_j(\varrho)$ is the sum over the purities of all j-body reductions.

[3] This can be established by writing the partial trace as a channel. See Refs. [40, 41] for more details.

[4] For a detailed derivation of this fact, see Appendix B in Ref. [41]

5 New codes from old

To develop our main results, we need a method with which new codes can be constructed from old ones. This is done by taking partial traces of $\Pi_{\mathcal{Q}}$.

Theorem 2 (Rains [40]). *Let* $((n, K, d))_D$ *be a pure code with* $n, d \ge 2$. *Then there exists a pure code* $((n-1, DK, d-1))_D$.

Proof. Let the code space be spanned by an orthogonal set of vectors, $\Pi_{\mathcal{Q}} = \sum_{i=1}^K |i_{\mathcal{Q}}\rangle\langle i_{\mathcal{Q}}|$. For simplicity, we normalize the projector onto the code space to a density matrix, $\varrho = \Pi_{\mathcal{Q}}/K$, such that $\mathrm{tr}(\varrho) = 1$. (This is motivated by the fact that ϱ stays normalized after application of the partial trace). The code being pure, it follows from Eq. (3) that all marginals of the spanning vectors $|i_{\mathcal{Q}}\rangle$ on less than d parties must be maximally mixed. Accordingly, the above vectors can for any subset of parties $S \subseteq \{1, \dots, n\}$ with $|S| < d$ be Schmidt-decomposed as

$$|i_{\mathcal{Q}}\rangle = \frac{1}{\sqrt{D^{|S|}}} \sum_{\ell=1}^{D^{|S|}} |v_i^{(\ell)}\rangle_S \otimes |w_i^{(\ell)}\rangle_{S^c}. \quad (19)$$

We will now show that after performing a partial trace over parties of some subset V with $|V| < d$, the operator $\mathrm{tr}_V(\varrho)$ forms again (a projector onto) a pure code of distance $d - |V|$ and dimension $KD^{|V|}$. First, note that the rank of $\mathrm{tr}_V(\varrho)$ can be at most $KD^{|V|}$, while the complementary operator $\mathrm{tr}_{V^c}(\varrho)$ is proportional to the identity. Because the reduction onto V is maximally mixed, $\mathcal{A}'_V(\varrho) = 1/D^{|V|}$. From the condition in Eq. (18), the complementary reduction must have $\mathcal{B}'_V(\varrho) = \mathrm{tr}[\mathrm{tr}_V(\varrho)^2] = 1/(KD^{|V|})$. As the operator $\mathrm{tr}_V(\varrho)$ can have a rank of at most $D^{|V|}K$, it must indeed be proportional to a projector onto a subspace of dimension $D^{|V|}K$.

In similar manner, we can establish that the code $\mathrm{tr}_V(\Pi_{\mathcal{Q}})$ has a distance of $d - |V|$. For this we must check the condition in Eq. (18), namely $KB'_j[\mathrm{tr}_S(\Pi_{\mathcal{Q}})] = A'_j[\mathrm{tr}_S(\Pi_{\mathcal{Q}})]$ for $0 \le j < d - |V|$. Respectively, it suffices to show that $K\mathcal{B}'_S(\varrho') = \mathcal{A}'_S(\varrho')$ for all $|S| < d - |V|$, with $\varrho' = \mathrm{tr}_V(\varrho)$. Let T be a subset of size smaller than $d - |V|$ with $T^c \cap V = \varnothing$. Then $\mathrm{tr}[\mathrm{tr}_{T\setminus V}(\varrho')^2] = \mathrm{tr}[\mathrm{tr}_T(\varrho)^2] = 1/(KD^{|T|})$. On the other hand, $\mathrm{tr}[\mathrm{tr}_{T^c}(\varrho')^2] = 1/D^{|T|}$, where T^c is now the complement of T in $\{1, \dots, n\}\setminus V$. We conclude that $K\mathcal{B}'_T(\varrho') = \mathcal{A}'_T(\varrho') = 1/D^{|T|}$ for all $|T| < d - |V|$, and $\mathrm{tr}_V \Pi_{\mathcal{Q}}$ indeed spans a pure code of distance $d - |V|$. The claim follows by setting $|V|$ to a single party. $\square$

As established in the above proof, a pure $((n, D^k, d))_D$ code spawns a family of new pure codes having parameters $((n-s, D^{k+s}, d-s))_D$ for all integers s in $0 \le s < d$. In the case of stabilizer codes, the same result can be obtained more straightforwardly [43, 44].

Remark. Naturally, this implies that if the existence of a pure $((n, D^k, d))_D$ can be ruled out, then any pure $((n+s, D^{k-s}, d+s))_D$ for $0 \leq s \leq k$ cannot exist either.

Does this method of creating new codes from old by partial trace also work for codes that are not pure? It is tempting to think that any given impure code $((n, K, d))_D$ may yield a $((n - 1, K', d - 1))_D$ with $K < K' \leq DK$. However, this does not seem to be straightforward: consider Shor's code, which is an impure code with parameters $((9, 2, 3))_2$. A partial trace on the last qubit yields a projector of rank 4, yet it does not form an $((8, 4, 2))_2$ code (such that $K' = DK$), as an analysis of its weight distribution shows.[5]

6 Quantum MDS codes

Let us recall the bound from which the concept of QMDS codes originates, the quantum Singleton bound.

Theorem 3 (Rains [17]). *Let* $\mathcal{Q} = [\![n, k, d]\!]_D$ *be a QECC. Its parameters are bounded by*

$$k + 2d \leq n + 2. \qquad (20)$$

For a code $\mathcal{Q} = ((n, K, d))_D$ with K not necessarily a power of D, the quantum singleton bound reads

$$K \leq D^{n-2(d-1)}. \qquad (21)$$

Two proofs of the quantum Singleton bound are presented in Appendix A.

A code that achieves equality in Eqs. (20) and (21), respectively, [i.e., having parameters $((n, D^{n-2d+2}, d))_D$] is called a *quantum maximum distance separable* code (QMDS). The length n of QMDS codes is unbounded for $d \leq 2$; these codes are called *trivial* [45]. From now on, we restrict ourselves to non-trivial QMDS codes, and can make use of $n+2 = k+2d$ in all derivations that follow.

It happens that all QMDS codes are pure [17, 45]. For this fact we will present a new information theoretic proof which was kindly communicated to us by Andreas Winter [46]. The following lemma on the von Neumann entropy $S(J) = S(\varrho_J) = -\sum_i \lambda_i \log(\lambda_i)$ of a subsystem $J \subseteq \{1, \ldots, n\}$, where λ_i are the eigenvalues of ϱ_J, is needed.

Lemma 4 (Winter [46]). *Let* $n \geq m > \ell$. *Then*

$$\frac{1}{\binom{n}{m}} \sum_{\substack{I \subseteq \{1,\ldots,n\} \\ |I|=m}} S(I) \leq \frac{m}{\ell} \frac{1}{\binom{n}{\ell}} \sum_{\substack{J \subset \{1,\ldots,n\} \\ |J|=\ell}} S(J). \qquad (22)$$

[5] The Shor code is spanned by the vectors $(|000\rangle + |111\rangle)^{\otimes 3}$ and $(|000\rangle - |111\rangle)^{\otimes 3}$. It has the weights $A = [4, 0, 36, 0, 108, 0, 300, 0, 576, 0]$ and $B = [2, 0, 18, 78, 54, 414, 150, 666, 288, 378]$ giving it a minimum distance $d = 3$. After a partial trace over a single particle, one obtains $A' = [16, 0, 112, 0, 240, 0, 400, 0, 256]$ and $B' = [4, 8, 80, 152, 520, 568, 1136, 808, 820]$, a trivial code with distance $d = 1$ and $K = 4$.

The proof can be found in Appendix B.

Theorem 5 (Rains [17]). *Let* $\mathcal{Q}$ *be a QMDS code. Then* $\mathcal{Q}$ *is pure.*

Proof. (Winter [46]) Purify the projector $\Pi_\mathcal{Q}$ onto the code space with a reference system R of dimension D^k. For any bipartition $A|B$ of $\{1, \ldots, n\}$ with sizes $|A| = d - 1$ and $|B| = n - d + 1$, respectively,

$$S(B) = S(RA) = S(R) + S(A) \qquad (23)$$

must hold for $\Pi_\mathcal{Q}$ to be a code of distance d [cf. Section 2]. Naturally, also

$$S(\overline{B}) = S(R) + S(\overline{A}), \qquad (24)$$

where $S(\overline{A})$ and $S(\overline{B})$ denote the average entropy of subsystems in $\{1, \ldots, n\}$ of sizes $d - 1$ and $n - d + 1$, respectively. Making use of Lemma 4, one has that

$$S(R) = S(\overline{B}) - S(\overline{A}) \leq \frac{n - 2(d-1)}{d-1} S(\overline{A}). \qquad (25)$$

For a quantum MDS code, $S(R) = k = n - 2(d-1)$. Thus to satisfy Eq. (25), $S(A) = (d-1)\log(D)$ for all A of size $(d-1)$ must hold. This proofs the claim. $\square$

It is interesting to note that Eq. (25) presents a trade-off, where large values of d/n and k/n go hand in hand with a highly entangled code space.

Quantum maximum distance separable codes being pure, we can extend Observation 1 to the case of subspaces that meet the quantum Singleton bound:

Observation 6 (QMDS codes and maximal rUS). *The following objects are equivalent:*
1. an $((n, D^{n-2d+2}, d))_D$ *QMDS code;*
2. a $(d-1)$-*uniform subspace in* $(\mathbb{C}^D)^{\otimes n}$ *of dimension* $n - 2d + 2$.

These objects—quantum MDS codes and r-uniform subspaces of maximal dimension—are now the main focus of our attention. All results in the following sections apply to both objects.

7 QMDS families

By Theorem 2, the existence of a QMDS code with distance d leads to a family of QMDS codes with distances $d' \leq d$ (see Fig. 1). As an example, the existence of a code having the parameters $((6, 2^0, 4))_2$ yields the chain $((6, 2^0, 4))_2 \Rightarrow ((5, 2^1, 3))_2 \Rightarrow ((4, 2^2, 3))_2 \Rightarrow ((3, 2^3, 1))_2$, where we refer to $((6, 2^0, 4))_2$ as the parent code. Such a *QMDS family* is solely determined by the parameter $n + k$ with $k = \log_D K$ ($n+k = 6$ in the above example), and we are interested in the highest achievable distance $\tilde{d} = (\tilde{n} - \tilde{k})/2 + 1$ within any given family.

Note that the reversal of such a chain of codes might not always be possible: for example, the existence of

$$n+k = 6, \; D = 2 \qquad n+k = 12, \; D = 3$$

$$
\begin{array}{cc}
((6, 2^0, 4))_2 & \exists \\
((5, 2^1, 3))_2 & \exists \\
((4, 2^2, 2))_2 & \exists \\
((3, 2^3, 1))_2 & \exists
\end{array}
\qquad
\begin{array}{cc}
((12, 3^0, 7))_3 & \nexists \\
((11, 3^1, 6))_3 & \nexists \\
((10, 3^2, 5))_3 & \nexists \\
((9, 3^3, 4))_3 & \nexists \\
((8, 3^4, 3))_3 & \exists \\
((7, 3^5, 2))_3 & \exists \\
((6, 3^6, 1))_3 & \exists
\end{array}
$$

Figure 1: Two examples of QMDS families. Left: a qubit QMDS family with $n + k = 6$. All its members, up to the parent code $((6, 2^0, 4))_2$, exist. Right: a trutrit QMDS family with $n + k = 12$. Its members are known for $d \leq 3$ [29], while it follows from the shadow inequalities that no corresponding codes can exist for $d > 3$. See also Tables 1 and 2 in Appendix D.

a code $((8, 3^4, 3))_3$ does not imply the existence of a code $((9, 3^3, 4))_3$. Indeed, a construction for the former is known, whereas the existence of the latter can be excluded (see Section 10 and Tables 1 and 2 in Appendix D). Nevertheless, any QMDS code $\mathcal{Q}$ has the characteristics of same-sized reductions of any of its hypothetical parent codes $\tilde{\mathcal{Q}}$: the reductions of $\mathcal{Q}$ are proportional to projectors, whose ranks match those of hypothetical reductions of $\tilde{\mathcal{Q}}$, while forming QECC themselves. This structure of nested projectors makes QMDS codes both attractive from the perspective of coding and entanglement theory, but also non-trivial to construct.

A certain part of the chain of the QMDS codes, consisting of the two top-most codes in any family, can always be reversed.

Proposition 7. *The existence of the following two QMDS codes is equivalent:*

$$((n, 1, n/2 + 1))_D \quad \Longleftrightarrow \quad ((n-1, D, n/2))_D. \quad (26)$$

(Note that for these to be QMDS codes, n must necessarily be even).

Proof. $\Rightarrow$: This direction was established in Theorem 2.
$\Leftarrow$: Let us purify $((n-1, D, n/2))_D$ with the associated projector $\Pi_{\mathcal{Q}} = \sum_{i=1}^{D} |i_{\mathcal{Q}}\rangle \langle i_{\mathcal{Q}}|$ to a state on n parties,

$$|\phi\rangle = \frac{1}{\sqrt{D}} \sum_{i=1}^{D} |i_{\mathcal{Q}}\rangle \otimes |i_R\rangle, \quad (27)$$

where $\{|i_R\rangle\}$ is a basis for the nth particle. From the conditions in Eq. (18) it follows that for $|\phi\rangle\langle\phi|$ to be a pure code of distance $n/2 + 1$ it suffices to check that $B'_j(|\phi\rangle\langle\phi|) = A'_j(|\phi\rangle\langle\phi|) = \binom{n}{j} D^{-j}$ (as $K = 1$) for all $j < n/2 + 1$. By partially tracing over any $(n/2 - 1)$ parties of $\Pi_{\mathcal{Q}}$, we see that this is indeed

the case. With Theorem 2, any code $\mathcal{Q}$ with parameters $((n-1, D^1, n/2))_D$ can be reduced to a pure $((n/2, D^{n/2}, 1))_D$, the latter corresponding to the identity matrix on $n/2$ particles. Thus every reduction of $\Pi_{\mathcal{Q}} = \sum_{i=1}^{D} |v_i\rangle\langle v_i|_{\mathcal{Q}}$ onto $n/2$ particles is maximally mixed. Correspondingly, any reduction of $|\phi\rangle$ of size $n/2$ that does not include the last particle is maximally mixed. From the Schmidt decomposition for pure states, it follows that any $n/2$-sized reduction that includes the last particle must then be maximally mixed, too. Thus $|\phi\rangle\langle\phi|$ forms a pure code of dimension 1 and distance $n/2 + 1$. This completes the proof. $\square$

Hence, not only can an $((n-1, D, n/2))_D$ code be obtained by partial trace from an $((n, 1, n/2+1))_D$, but the latter can always be constructed by purification from the former. As a consequence, all QMDS codes with $k = 0, 1$ come in pairs, such as, e.g., the codes $((6, 1, 4))_D$ and $((5, D, 3))_D$, which exist for all local dimensions D [17].

While it was previously known that every pure code of dimension D can with the addition of a single D-dimensional system be purified to a rank-one quantum state [40], the increase in distance for the case of QMDS codes [Proposition 7] appears to be new.

It is natural to ask under what conditions other steps in the hierarchy can be reversed. While we leave this question open for now, note that for some cases

$$((n-2, D^2, n/2-1))_D \quad \nRightarrow \quad ((n-1, D, n/2))_D. \quad (28)$$

For example, there exists a $((6, 3^2, 3))_3$ code, yet a $((7, 3^1, 4))_3$ can be excluded with the methods of Section 10 (also see Table 2 in Appendix D).

Let us make a small detour to propagation rules for classical codes. From a linear code $[n, k, d]_q$, one can obtain a code $[n-1, k, d-1]_q$ by an operation called *puncturing* (deleting one coordinate), and a code $[n-1, k-1, d]_q$ by *shortening* (taking an appropriate subcode after deleting one coordinate) [47]. Both operations yield MDS codes when starting with an MDS code. On the other hand, puncturing (i.e. projectively measuring a single subsystem) a quantum code $((n, K, d))_D$ yields a code $((n-1, K, d-1))_D$ [6]. But even when starting from a QMDS code, the resulting code is, in general, no longer QMDS. The analogue of shortening of quantum codes preserves the property of being a QMDS code, but it is more involved and not always possible. Rains [17] has given a criterion when a stabilizer code $[\![n-s, k-s, d]\!]_q$ can be derived from a stabilizer code $[\![n, k, d]\!]_q$ by shortening.

8 The weights of quantum MDS codes

The weights of classical MDS codes are fixed by their parameters [48], and it is natural to ask if a similar result might also hold for their quantum analogue. This is indeed the case.

Theorem 8. *The* unitary *weights A'_j of a general QMDS code $\mathcal{Q} = (\!(n, D^k, d)\!)_D$ are given by*

$$A'_j(\Pi_{\mathcal{Q}}) = \binom{n}{j} D^{2k - \min(2\alpha - j, j)}, \qquad (29)$$

where $\alpha = (n + k)/2$.

Proof. From the repeated application of Theorem 2, all reductions of size smaller than or equal to α are proportional to identity. On the other hand, all reductions of size $j > \alpha$, being pure codes with parameters $(\!(j, D^{2\alpha - j}, j - \alpha + 1)\!)_D$, are also proportional to projectors. These, however, have a non-full rank of $2\alpha - j$, namely the dimension of their code space. Summing over all reductions of size j and taking into account the normalization $\mathrm{tr}(\Pi_{\mathcal{Q}}) = D^k$ yields the claim. $\square$

To obtain the Shor-Laflamme weights A_j, we make use of the combinatorial version of the Möbius inversion formula (see p. 267 in Ref. [49]). Denote by $2^{[n]}$ the set of subsets of $\{1, \dots, n\}$. Given the functions $f \colon 2^{[n]} \to \mathbb{R}$ and $g \colon 2^{[n]} \to \mathbb{R}$ with $g(S) = \sum_{T \subseteq S} f(T)$, then

$$f(S) = \sum_{T \subseteq S} (-1)^{|S - T|} g(T). \qquad (30)$$

Using Möbius inversion, one can determine the weight distribution of QMDS codes.

Theorem 9. *The* Shor-Laflamme *weights A_j of a general QMDS code $\mathcal{Q} = (\!(n, D^k, d)\!)_D$ are given by*

$$A_j(\Pi_{\mathcal{Q}}) = \binom{n}{j} \sum_{i=0}^{j} \binom{j}{i} (-1)^{j-i} D^{2k + i - \min(2\alpha - i, i)}, \qquad (31)$$

where $\alpha = (n + k)/2$.

Proof. In Eq. (11) and (13), we defined the fine-grained weights

$$\mathcal{A}_S(\Pi_{\mathcal{Q}}) = \sum_{\mathrm{supp}(E_{\boldsymbol{a}}) = S} \mathrm{tr}[E_{\boldsymbol{a}}^\dagger \Pi_{\mathcal{Q}}] \, \mathrm{tr}[E_{\boldsymbol{a}} \Pi_{\mathcal{Q}}], \qquad (32)$$

$$\mathcal{A}'_S(\Pi_{\mathcal{Q}}) = \mathrm{tr}[\mathrm{tr}_{S^c}(\Pi_{\mathcal{Q}}) \, \mathrm{tr}_{S^c}(\Pi_{\mathcal{Q}})]. \qquad (33)$$

As shown in [41], they are related via

$$\mathcal{A}'_S(\Pi_{\mathcal{Q}}) = D^{-|S|} \sum_{T \subseteq S} \mathcal{A}_T(\Pi_{\mathcal{Q}}). \qquad (34)$$

We can accordingly make use of the Möbius inversion [Eq. (30)] to obtain [40],

$$\mathcal{A}_S(\Pi_{\mathcal{Q}}) = \sum_{T \subseteq S} (-1)^{|S| - |T|} D^{|T|} \mathcal{A}'_T(\Pi_{\mathcal{Q}}). \qquad (35)$$

With $A_j(\Pi_{\mathcal{Q}}) = \sum_{|S| = j} \mathcal{A}_S(\Pi_{\mathcal{Q}})$, one obtains the Shor-Laflamme weights for QMDS codes

$$A_j(\Pi_{\mathcal{Q}}) = \sum_{|S| = j} \sum_{T \subseteq S} (-1)^{|S| - |T|} D^{|T|} \mathcal{A}'_T(\Pi_{\mathcal{Q}})$$

$$= \binom{n}{j} \sum_{i=0}^{j} \binom{j}{i} (-1)^{j-i} D^{2k + i - \min(2\alpha - i, i)}. \qquad (36)$$

This ends the proof. $\square$

Remark. The same result could be obtained by the polynomial transform [40, 41]

$$A(x, y) = A'(x - y, Dy) \qquad (37)$$

where

$$A(x, y) = \sum_{j=0}^{n} A_j x^{n-j} y^j, \quad A'(x, y) = \sum_{j=0}^{n} A'_j x^{n-j} y^j.$$

Let us point out that the weights of an $(\!(n, D^k, d)\!)_D$ QMDS code are proportional to those of any n-sized reduction of a *hypothetical* QMDS parent code $(\!(n + k, 1, \frac{n+k}{2} + 1)\!)_D$ [6] (cf. the next section): this hypothetical parent code is represented by a pure state $|\phi\rangle\langle\phi|$ that has all its $(n + k)/2$-body marginals maximally mixed. Accordingly, its j-sized reductions $\varrho_{(j)}$ have purity $\mathrm{tr}[\varrho_{(j)}^2] = D^{-\min(j, n+k-j)}$. Indeed, let $\Pi_{\mathcal{Q}'} = D^k \, \mathrm{tr}_V(|\phi\rangle\langle\phi|)$ with $|V| = k$ be proportional to an n-sized reduction of $|\phi\rangle$. Summing over the purities of all its marginals of size j, we obtain the weights of Theorem 8. We conclude that the unitary weights of a QMDS code $(\!(n, D^k, d)\!)_D$ are proportional to those of any n-sized reduction $\mathrm{tr}_V |\phi\rangle\langle\phi|$ with $(|V| = k)$ of a hypothetical $(\!(n + k, 1, \frac{n+k}{2})\!)_D$ code.

This observation motivates the bound on QMDS codes that follows in Section 9. It is of the same type as the one obtained by Scott in Ref. [50] (see Proposition 17 in Appendix C) for the existence of absolutely maximally entangled states.

9 The maximal length of QMDS codes

In this section we derive a new bound for the existence of QMDS codes. Our bound generalizes a result by Ketkar et al. [51] on QMDS *stabilizer* or *additive* codes to QMDS codes of any type. It can equally be seen as a generalization of a bound by Scott [50] on the existence of codes with parameters $(\!(n, 1, \lfloor \frac{n}{2} \rfloor + 1)\!)$ that are known as *absolutely maximally entangled* states or *perfect tensors* [52, 53]. Thus our main result extends Props. 16 and 17 in Appendix C to *all* QMDS codes.

Theorem 10 (Maximal length of QMDS codes)**.** *Let $\mathcal{Q} = (\!(n, D^k, d)\!)_D$ be a (stabilizer or non-stabilizer) QMDS code with $d \geq 3$. Then*

$$n \leq D^2 + d - 2, \qquad \text{or equivalently} \qquad (38)$$

$$n + k \leq 2(D^2 - 1). \qquad (39)$$

Proof. Denote by $\Pi_{\mathcal{Q}}$ the projector onto the code space. For convenience we normalize the code to a quantum state $\varrho = \Pi_{\mathcal{Q}}/D^k$, such that $\mathrm{tr}[\varrho] = 1$. Define $\alpha = (n + k)/2$, and denote by ϱ' the reduced density matrix of ϱ corresponding to the code

---

[6] This argument could be refined: the weights of any $(\!(n, D^k, d)\!)_D$ QMDS code are proportional to a reduction of any of its hypothetical QMDS parents $(\!(n + k - s, D^s, \frac{n+k}{2} + 1 - s)\!)_D$ for all $1 \leq s \leq k$.

$\mathcal{Q}' = ((a+1, D^{\alpha-1}, 2))_D$ on the first $\alpha+1$ parties. Likewise, denote by ϱ'' a reduced density matrix of ϱ corresponding to $\mathcal{Q}'' = ((\alpha+2, D^{\alpha-2}, 3))_D$ on the first $\alpha+2$ parties. By Theorem 2 both $\mathcal{Q}'$ and $\mathcal{Q}''$ must be pure, being derived from a pure code $\mathcal{Q}$. Then $\text{tr}[\varrho'^2] = D^{-(\alpha-1)}$ and $\text{tr}[\varrho''^2] = D^{-(\alpha-2)}$. Since $A_j = 0$ for all $0 < j < \alpha+1$, we can decompose ϱ' and ϱ'' in the Bloch representation in the following way,

$$\varrho' = \frac{1}{D^{\alpha+1}}(\mathbb{1} + P_{\alpha+1}), \tag{40}$$

$$\varrho'' = \frac{1}{D^{\alpha+2}}(\mathbb{1} + \sum_{i=1}^{\alpha+2} P_{\alpha+1}^{(i)} \otimes \mathbb{1}_i + P_{\alpha+2}), \tag{41}$$

where $P_{\alpha+1}$, $P_{\alpha+1}^{(i)}$, and $P_{\alpha+2}$ only contain terms of weight $\alpha+1$, $\alpha+1$, and $\alpha+2$ respectively. Note that there are $\alpha+2$ different terms $P_{\alpha+1}^{(i)}$ with support on different subsystems in ϱ''. Also, our normalization is chosen such that

$$A_{\alpha+1}(\varrho') = D^{-(\alpha+1)} \text{tr}[P_{\alpha+1}^2], \tag{42}$$

$$A_{\alpha+1}(\varrho'') = D^{-(\alpha+2)} \text{tr}[(\sum_{i=1}^{\alpha+2} P_{\alpha+1}^{(i)} \otimes \mathbb{1}_i)^2], \tag{43}$$

$$A_{\alpha+2}(\varrho'') = D^{-(\alpha+2)} \text{tr}[P_{\alpha+2}^2], \tag{44}$$

Making use of $\text{tr}[\varrho'^2] = D^{-(\alpha-1)}$ leads to

$$A_{\alpha+1}(\varrho') = D^2 - 1. \tag{45}$$

Similarly, making use of $\text{tr}[\varrho''^2] = D^{-(\alpha-2)}$ yields,

$$A_{\alpha+2}(\varrho'') = D^4 - (\alpha+2)(D^2-1) - 1 \ge 0, \tag{46}$$

which must be non-negative. Division by (D^2-1) leads to $D^2 - 1 - \alpha \ge 0$, which can be recast to the bound above. This proofs the claim. $\quad\square$

10 Shadow bounds

Considering absolutely maximally entangled states, stronger bounds on their existence can be made than what is achieved by the bound from Scott [see Proposition 17 in Appendix C] in case their local dimension is small [41, 54]. In a similar spirit, it is possible to constrain the existence of low-dimensional QMDS codes further.

The *shadow inequalities* state that for any positive semi-definite operators $M_1, M_2 \ge 0$ and any subset $T \subseteq \{1, \dots, n\}$, the following family of inequalities hold [40, 55].

$$\sum_{S \subseteq \{1,\dots,n\}} (-1)^{|S \cap T|} \text{tr}[\text{tr}_{S^c}(M_1) \text{tr}_{S^c}(M_2)] \ge 0. \tag{47}$$

The shadow inequalities can be seen as a family of monogamy of entanglement relations that constrain the entanglement appearing in the code sub-

space [35].[7] In order to use the shadow inequalities to determine the existence of codes, one sets $M_1 = M_2 = \Pi_{\mathcal{Q}}$ and checks the non-negativity of Eq. (47) for all subsets $T \subseteq \{1, \dots, n\}$.

Let $\mathcal{Q} = ((n, D^k, d))_D$ be a QMDS code. Then $\text{tr}_{S^c}(\Pi_{\mathcal{Q}})^2 = D^{2k+\min(n+k-|S|,|S|)}$, in line with the arguments of the proof of Theorem 8. Thus their structure in terms of their unitary invariants is symmetric under permutation of the subsystems. We thus do not forgo by considering a symmetrized version of Eq. (47) only, the coefficients of the so-called shadow enumerator [40, 55]

$$S_j(\Pi_{\mathcal{Q}}) = \sum_{|T^c|=j} \sum_{S \subseteq \{1,\dots,n\}} (-1)^{|S \cap T|} \text{tr}[\text{tr}_{S^c}(\Pi_{\mathcal{Q}})^2]$$

$$= \sum_{\ell=0}^{n} K_{n-j}(\ell, n) A_\ell'(\Pi_{\mathcal{Q}}) \ge 0. \tag{48}$$

Above, $K_m(\ell, n)$ is the Krawtchouk polynomial defined as

$$K_m(\ell, n) = \sum_{\beta=0}^{m} (-1)^\beta \binom{n-\ell}{m-\beta} \binom{\ell}{\beta}. \tag{49}$$

Remark. The same result can be obtained by the polynomial transform [40, 41]

$$S(x, y) = A'(x+y, y-x) \tag{50}$$

where

$$S(x, y) = \sum_{j=0}^{n} S_j x^{n-j} y^j, \quad A'(x, y) = \sum_{j=0}^{n} A_j' x^{n-j} y^j.$$

We now can state the following corollary for the special case of QMDS codes.

Corollary 11. *Let* $((n, D^k, d))_D$ *be a QMDS code. The following expression must be non-negative for all j in $0 \le j \le n$,*

$$S_j = D^{2k} \sum_{\ell=0}^{n} K_{n-j}(\ell, n) \binom{n}{\ell} D^{-\min(n+k-\ell,\ell)} \ge 0. \tag{51}$$

Generally, the constraints imposed by Eqs. (47) and (48) do not seem to give rise to simple closed-form expressions on the existence or minimum distance of codes. In the case of a binary alphabet however, the constraints yield the following bounds (cf. Theorem 15 in Ref. [56] and Theorem 13.4.1 in Ref. [57]): the minimum distance of pure codes $((n, 1, d))_2$ is bounded by

$$d \le \begin{cases} 2\lfloor \frac{n}{6} \rfloor + 3 & \text{if } n = 5 \bmod 6; \\ 2\lfloor \frac{n}{6} \rfloor + 2 & \text{otherwise}, \end{cases} \tag{52}$$

---

[7] The shadow inequalities are also connected to a family of positive maps that generalize the reduction map $\varrho \mapsto \mathbb{1} - \varrho$. Consequently, Eq. (47) also holds in operator form: for all $M \ge 0$ and all subsets $T \subseteq \{1, \dots, n\}$, $\sum_{S \subseteq \{1,\dots,n\}} (-1)^{|S \cap T|} M_S \otimes \mathbb{1}_{S^c} \ge 0$, where $M_S = \text{tr}_{S^c} M$ [35].

whereas the minimum distance of codes $((n, K, d))_2$ with $K > 1$ is bounded by

$$d \leq \begin{cases} 2\lfloor \frac{n+1}{6} \rfloor + 2 & \text{if } n = 4 \bmod 6; \\ 2\lfloor \frac{n+1}{6} \rfloor + 1 & \text{otherwise}. \end{cases} \qquad (53)$$

As done for the case of AME states in Ref. [41], it is possible to evaluate Corollary 11 numerically for any QMDS code having small enough parameters. This leads to new bounds on the existence of QMDS codes in dimensions $D \leq 5$, see Appendix D.

11 QMDS conjecture

The following conjecture relating the maximal length of QMDS codes and the local dimension D is of interest. It follows from the classical MDS conjecture, and thus concerns itself with QMDS codes of stabilizer type only. The MDS conjecture for classical codes states that the length of a non-trivial linear MDS code over the field $GF(q)$ is bounded by $n \leq q + 1$, with the exception of $q = 2^m$ where additionally codes with parameters $[q+2, 3, q]_q$ and $[q+2, q-1, 4]_q$ exist. [48, Research Problem (11.4)]. Applying this conjecture to the classical codes over the field $GF(q^2)$ corresponding to stabilizer codes, one obtains the following conjecture.

Conjecture 12 (QMDS Conjecture, Cor. 65 in Ref. [51]). *With exception of $[\![D^2 + 2, D^2 - 4, 4]\!]_D$ with $D = 2^m$ where $n \leq D^2 + 2$ (cf. Thm. 14 in Ref. [30]), the length of all stabilizer QMDS codes with $d \geq 3$ is bounded by $n \leq D^2 + 1$.*[8]

The strongest confirmation of the classical MDS conjecture was proven in a seminal work by Ball, which showed that the conjecture is true for linear q-ary codes when q is prime [34]. Even when the classical MDS conjecture turns out to be true, Conjecture 12 could be violated by non-stabilizer QMDS codes.

On the other hand, our bound (Theorem 10) constrains the length of QMDS codes for distance $d = 3$ to $n \leq D^2 + 1$, confirming the QMDS Conjecture for this choice of distance. For $d = 4$, our bound can be met when $D = 2^m$ (Thm. 14 in Ref. [30]). In general, however, Conjecture 12 is still unresolved for $d > 3$.

From the bound in Theorem 10 it is seen that QMDS codes with distance $d \geq 3$ can only exist if $n + k \leq 6$ for qubits, $n + k \leq 16$ for qutrits, $n + k \leq 30$ for ququarts, and $n + k \leq 48$ in the case of local dimension $D = 5$. Thus for qubits, no other non-trivial QMDS codes exist apart from those with the parameters of the known stabilizer codes $[\![6, 0, 4]\!]_2$ and $[\![5, 1, 3]\!]_2$. In the case of qutrits, only seven QMDS families exist; for five of these, the optimal parent code has already been found (see Table 2).

---

[8] Note that while in Corollary 65 of Ref. [51] the case $d = q^2$ and $n \leq q^2 + 2$ is listed as well, this is already excluded by the quantum Singleton bound if $q > 2$.

12 Conclusions

It is readily seen that quantum maximum distance separable (QMDS) codes must correspond to subspaces in which every unit vector shows maximal entanglement across all bipartitions where the smaller partition has size $(d - 1)$. The question under what conditions such codes exist is thus not only relevant in coding theory, but also for the study of multipartite entanglement.

Interestingly, all QMDS codes can be grouped into QMDS families whose members can be regarded as being obtained by partial trace from a (possibly hypothetical) parent code of larger length and distance. Since all descendants within a QMDS family form codes of smaller distance themselves, their spectra are completely determined by the parameters of their parent code. This insight completely determines the weight enumerator of QMDS codes. It also leads to a bound applicable to all (stabilizer and non-stabilizer) QMDS codes, extending results known for the special cases of stabilizer QMDS codes and absolutely maximally entangled states. Moreover, the application of Rains' shadow inequalities yields additional non-existence results.

The quantum Singleton bound is independent of the local dimension D and one thus cannot expect it to be particularly strong. However, if the Singleton bound can be met, classical codes are in all known cases origin of these optimal quantum codes and highly entangled subspaces. More precisely, the majority of non-trivial QMDS codes in the literature are of stabilizer type and hence based on classical additive or linear MDS codes. There are also some examples of non-stabilizer (also called *non-additive*) QMDS codes, in particular codes of distance two [58, Thm. 7]. However, putting these non-additive codes into the framework of so-called union stabilizer codes or CWS codes (see [45, Chapter 10]), one finds a connection to classical non-additive MDS codes as well.

It is an open question if this must generally be the case and we state the problem more formally:

Research Problem. Is every quantum maximum distance separable code related to a classical MDS code?

It is indeed intriguing that hitherto no genuine "quantum" constructions have been found that surpass their classical counterparts for these types of codes. We note that an affirmative answer to this question would also reduce the question of the existence of absolutely maximally entangled states for some given even number of parties and local dimension to merely a finite computational problem (also see Problem 3. in Ref. [59]).

An interesting aspect seen here is that "optimal" codes that have the largest possible distance must necessarily also exhibit the highest possible bipartite entanglement amongst the constituent particles. One can readily expect a trade-off to be present, where

large values of k/n and d/n necessarily go hand in hand with a highly entangled code space, whereas lowly entangled subspaces can only yield low values. Indeed, such a trade-off can be seen in Eq. (25), quantified by the average entropy of entanglement. A precise understanding of this trade-off might pave the way to derive stronger bounds on the performance of quantum codes, and could possibly help to explain the distance scalings found in low-density parity check codes [9].

To conclude, QMDS codes present themselves as a rich playground: they form nested subspaces that are highly entangled and prove to be a testing ground for our understanding of multipartite entanglement. The discovery of further monogamy relations as well as entropic and rank inequalities would likely find an immediate application in stronger bounds on the existence of these ideal quantum objects.

A Proofs of the quantum Singleton bound

We present two known proofs for the quantum Singleton bound below.

Theorem 13 (Quantum Singleton bound [15, 17, 60, 61]). *Let $((n, K, d))_D$ be a QECC. Its parameters are bounded by*

$$K \leq D^{n-2(d-1)} \,. \tag{54}$$

Proof 1: (Rains, Thm. 2 in Ref. [17]). Let us first show that $2(d-1) \leq n$. Assume that $2(d-1) > n$ and consider $K = 1$: by convention, codes with $K = 1$ are only considered codes if they are pure, and thus must have $\mathrm{tr}_{S^c} |\phi\rangle\langle\phi| \propto \mathbb{1}$ for all $|S| < d$. From the Schmidt decomposition however it is seen that it is impossible that marginals of size $\lfloor \frac{n}{2} \rfloor + 1$ are of full rank, and thus $2(d-1) \leq n$. Consider now $K > 1$: in terms of the unitary weight enumerators, the conditions for a projector $\Pi_{\mathcal{Q}}$ to be a QECC subspace read $KB'_j(\Pi_{\mathcal{Q}}) = A'_j(\Pi_{\mathcal{Q}})$ for all $j < d$ [Eq. (18)]. Also recall that by definition $A'_j = B'_{n-j}$. If $2(d-1) > n$, one thus requires that

$$A'_{d-1} = KB'_{d-1} = KA'_{n-(d-1)} \,, \tag{55}$$

and, due to $n - (d-1) < (d-1)$, also that

$$A'_{n-(d-1)} = KB'_{n-(d-1)} = KA'_{d-1} \,, \tag{56}$$

leading to a contradiction also for $K > 1$.

Consequently, $2(d-1) \leq n$. With the decompositions from Eq. (16), one has that

$$A'_{d-1} = D^{-d+1} \sum_{i=0}^{d-1} \binom{n-i}{n-d+1} A_i \,, \tag{57}$$

but also[9]

$$A'_{d-1} = KB'_{d-1} = KA'_{n-d+1}$$
$$= KD^{-n+d-1} \sum_{i=0}^{n-d+1} \binom{n-i}{d-1} A_i \,. \tag{58}$$

With $\binom{n-i}{n-d+1} = \binom{n-i}{d-1-i}$, the quantum Singleton bound follows from the analysis of

$$0 = A'_{d-1} - A'_{d-1} = KD^{-n+d-1} \sum_{i=0}^{n-d+1} \binom{n-i}{d-1} A_i$$
$$- D^{-d+1} \sum_{i=0}^{d-1} \binom{n-i}{d-1-i} A_i \,. \tag{59}$$

Consider the coefficient A_i for $0 \leq i < d$.

$$KD^{-n+d-1} \binom{n-i}{d-1} - D^{-d+1} \binom{n-i}{d-1-i} \,. \tag{60}$$

Note that

$$\frac{\binom{n-i}{d-1}}{\binom{n-i}{d-1-i}} = \frac{(d-1-i)!(n-d+1)!}{(d-1)!(n-i-d+1)!}$$

---

[9]The arXiv version (quant-ph/9703048) of Ref. [17] contains in the corresponding formulae erroneous factors of $(D-1)^i$.

$$= \frac{(n-d+1)(n-d)\cdots(n-d+2-i)}{(d-1)(d-2)\cdots(d-i)} \geq 1, \quad (61)$$

because $n - d + 1 \geq d - 1$ as established previously. If $K > D^{n-2(d-1)} > 1$, the expression (60) must be non-negative due to $A_i \geq 0$, and it is furthermore strictly positive in the case of $i = 0$ due to $A_0 = K$. Consequently Eq. (60) can only vanish if at least $K \leq D^{n-2(d-1)}$. This proofs the claim. $\quad\square$

Proof 2: (Cerf & Cleve [15]). For this proof we only consider the case $K > 1$. Then the distance must be bounded by $2(d-1) \leq n$, for if not, two copies of the encoded state could be recovered each from reductions of size $n - (d-1) < d - 1$, violating the no-cloning theorem.

Let $\Pi_{\mathcal{Q}} = \sum_{i=1}^{K} |i_{\mathcal{Q}}\rangle\langle i_{\mathcal{Q}}|$ be the projector onto the code space. The purification with a reference system R leads to,

$$|\psi_{QR}\rangle = \frac{1}{\sqrt{K}} \sum_{i=1}^{K} |i_{\mathcal{Q}}\rangle \otimes |i_R\rangle, \quad (62)$$

where $|i_R\rangle$ is any orthonormal basis for R. Recall that the von Neumann entropy is defined as $S(\varrho) = -\operatorname{tr} \varrho \log \varrho$. Let us partition the code into the three subsystems A, B, C, such that $|A| = |B| = d - 1$ and $|C| = n - 2(d-1)$. Then $S_R = S(\operatorname{tr}_{ABC}[\varrho]) = \log(K)$. As the code has distance d, any subsystem of size strictly smaller than d cannot reveal anything about the reference system R: indeed the condition of $\varrho_{RA} = \varrho_R \otimes \varrho_A$ is known to be a necessary and sufficient condition for the subsystem A to be correctable [62]; this is also equivalent to $S_{RA} = S_R + S_A$. With the subadditivity of the von Neumann entropy, namely $S_{12} \leq S_1 + S_2$, this leads to

$$S_R + S_A = S_{RA} = S_{BC} \leq S_B + S_C, \quad (63)$$
$$S_R + S_B = S_{RB} = S_{AC} \leq S_A + S_C, \quad (64)$$

where we used that the entropies of complementary subsystems are equal for a pure state. The combination of the above two inequalities yields $\log(K) = S_R \leq S_C \leq \log \dim(\mathcal{H}_C) = \log D^{n-2(d-1)}$. This proofs the claim. $\quad\square$

A third proof of the quantum Singleton bound using linear programming can be found in Refs. [60, 61].

B Entropy lemma

Lemma 14 (Winter [46]). *Let $n \geq m > \ell$. Then*

$$\frac{1}{\binom{n}{m}} \sum_{\substack{I \subseteq \{1,\ldots,n\} \\ |I|=m}} S(I) \leq \frac{m}{\ell} \frac{1}{\binom{n}{\ell}} \sum_{\substack{J \subset \{1,\ldots,n\} \\ |J|=\ell}} S(J). \quad (65)$$

Proof. For any subset $T \subseteq \{1,\ldots,n\}$, denote by X_T the combination of the subsystems $\{X_i : i \in T\}$. We first aim to show that

$$S(X_{\{1,\ldots,n\}}) \leq \frac{1}{n-1} \sum_{i=1}^{n} S(X_{\{1,\ldots,n\}\setminus\{i\}}). \quad (66)$$

For this, we purify the state with a reference system R. Then Eq. (66) is equivalent to

$$(n-1)S(R) \leq \sum_{i=1}^{n} S(X_i R). \quad (67)$$

Rewritten in terms of the conditional von Neumann entropy $S(A|B) = S(AB) - S(B)$ yields

$$-S(R) \leq \sum_{i=1}^{n} S(X_i|R). \quad (68)$$

To see that this holds, note that

$$-S(R) = S(X_{\{1,\ldots,n\}}|R) \leq \sum_{i=1}^{n} S(X_i|R), \quad (69)$$

where the equality follows from the fact that the state on the entire system $X_1 \ldots X_n R$ is pure, and the inequality follows from strong subadditivity. The repeated application of Eq. (66) yields

$$\frac{1}{m} \frac{1}{\binom{n}{m}} \sum_{|I|=m} S(I) \leq \frac{1}{\ell} \frac{1}{\binom{n}{\ell}} \sum_{|J|=\ell} S(J). \quad (70)$$

This completes the proof. $\quad\square$

A slightly more general form of above Lemma, the "quantum Shearer's inequality", and its history can be found in Ref. [63].

C QMDS stabilizer codes and AME states

In order to set the bound appearing in Section 9, Theorem 10 into context, we shortly state the previously known bounds on stabilizer and largest-distance QMDS codes.

Stabilizer codes are constructed from Abelian subgroups of *nice error bases* not containing a non-trivial multiple of the identity.[10] When the local dimension $D = q = p^m$ is a power of a prime, such Abelian subgroups correspond to additive codes $\mathcal{C}$ over the finite field $\mathbb{F}_{q^2}$ with q^2 elements. Additionally, the code $\mathcal{C}$ is contained in its dual, $\mathcal{C} \subseteq \mathcal{C}^{\perp_a}$, with respect to the trace-alternating form on $\mathbb{F}_{q^2}^n$, given by

$$\langle x, y \rangle_a = \operatorname{tr}_{\mathbb{F}_q/\mathbb{F}_p} \left(\frac{x \cdot y^q - x^q \cdot y}{\beta^{2q} - \beta^q} \right). \quad (71)$$

---

[10] A nice error basis is a set of unitary matrices $\{E_g\}$ corresponding to a group G such that $E_1 = \mathbb{1}$ and $E_g E_h = \omega_{g,h} E_{gh}$ [64].

Some QMDS constructions

short (Gilbert-Varshamov) [51, Cor. 32]:	$[\![n, n-2d+2, d]\!]_q$	$2 \le d \le \lceil \frac{n}{2} \rceil$, $\binom{n}{d} \le q^2 - 1$
Euclidean (CSS) [65, Cor. 1]:[a]	$[\![n, n-2d+2, d]\!]_q$	$1 \le d \le \lfloor \frac{n}{2} \rfloor + 1$, $3 \le n \le q+1$ for $2 < q$
punctured GRM [66, Thm. 5 & Cor. 6]:	$[\![q^2 - q\alpha, q^2 - q\alpha - 2d + 2, d]\!]_q$	$2 \le d \le q$, $0 \le \alpha \le q - d + 1$
Hermitean [29, Thm. 14]:[b]	$[\![q^2 - s, q^2 - s - 2d + 2, d]\!]_q$	$2 \le d \le q$, for some $0 \le s < q$, incl. $s = 0, 1$
single-error [67, Cor. 3.6]:[c]	$[\![n, n-4, 3]\!]_q$	$4 \le n \le q^2 + 1$ except $q = 2$ with $n = 4$
Grassl/Rötteler I [30, Thm. 13]:	$[\![q^2 + 1, q^2 - 2d + 3, d]\!]_q$	$2 \le d \le q + 1$, for q odd or (q even and d odd)
Ball [69, Thm. 4]:	$[\![q^2 + 1, q^2 - 2d + 3, d]\!]_q$	$2 \le d \le q + 1$, for $d \neq q$
Grassl/Rötteler II [30, Thm. 14]:	$[\![q^2 + 2, q^2 - 4, 4]\!]_q$	$q = 2^m$
trivial [30, Thm. 12]:	$[\![n, n-2, 2]\!]_D$	n even and (D odd or a multiple of 4)

[a]In Theorem 14 of Ref. [29], and subsequently also in the overview table of Ketkar et al. [51], only the upper bound $n \le q$ is given. The bound $n \le q + 1$ follows from Corollary 1 of Ref. [65] (note that there, the condition $q > 2$ for $n = q + 1$ is missing).
[b]Further details on what values s can take can be found in Refs. [29, 30].
[c]The case where q is odd also appears in Theorem 1.1 of Ref. [68].

Table 1: Some known QMDS constructions when $q = p^\beta$ is a power of prime (except for the trivial QMDS). The table is partially adopted from Ref. [51]. Apart from the trival QMDS codes with $d = 2$, all codes are stabilizer codes.

Here (β, β^q) is a normal basis of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$ and the trace function for $q = p^m$ is defined as $\mathrm{tr}_{\mathbb{F}_q / \mathbb{F}_p}(a) = \sum_{i=0}^{m-1} a^{q^i}$.

Thus, in the context of quantum MDS codes of stabilizer type, their correspondence to classical MDS codes is of relevance.

Proposition 15 (Thm. 15 and Lemma 61 in [51]).
The existence of the following is equivalent:
1. an $[\![n, n-2d+2, d]\!]_q$ QMDS stabilizer code;
2. an $[n, d-1, n-d+2]_{q^2}$ additive MDS code $\mathcal{C} \subset \mathbb{F}_{q^2}^n$ that is contained in its dual, $\mathcal{C} \subset \mathcal{C}^{\perp_a}$.

Note that the dual code $\mathcal{C}^{\perp_a}$ is also an MDS code with parameters $[n, n-d+1, d]_{q^2}$.

The following is known on the maximal length of stabilizer QMDS codes.

Proposition 16 (Maximal length of QMDS *stabilizer* codes, Thm. 63 in Ref. [51]). *Let $\mathcal{Q} = [\![n, k, d]\!]_D$ be a QMDS stabilizer code with $d \ge 3$ and where D is a prime-power. Then*

$$n \le D^2 + d - 2. \tag{72}$$

A pure state $|\phi_{n,D}\rangle$ of n parties with local dimension D each is called *absolutely maximally entangled* (AME), if maximal entanglement is present across every bipartition. Consequently, all its reductions to half of its parties are maximally mixed. AME states are pure codes with parameters $((n, 1, \lfloor \frac{n}{2} \rfloor + 1))_D$. If n is even, these states are the top-most member of a QMDS family, reaching the largest distance allowed by the quantum Singleton bound. They are also known as *perfect tensors*. Scott obtained the following bound on the existence of absolutely maximally entangled states.

Proposition 17 (Maximal length of AME states, Eq. 44 in Ref. [50]). *Let $|\phi_{n,D}\rangle$ be an absolutely maximally entangled state of $n \ge 4$ parties of local dimension D each. Then*

$$n \le \begin{cases} 2(D^2 - 1) & \text{if } n \text{ is even;} \\ 2D(D+1) - 1 & \text{if } n \text{ is odd.} \end{cases} \tag{73}$$

Thus for n even, Proposition 17 is indeed a bound on the existence of QMDS codes that have $k = 0$.

D Known constructions and tables

We list parameters of some known QMDS constructions in Table 1. Tables 2 to 4 report on the highest distances within a QMDS family that are not excluded by our bounds, as well as on the parameters that can be reached by known constructions. All upper bounds listed arise from the shadow inequalities (Corollary 11). For local dimensions $D > 5$, these constraints do not seem to be stronger than those of Theorem 10 and thus our tables only include codes up to $D = 5$.

Should the upper and lower bound meet, the corresponding code is *optimal* and specifies its QMDS family completely; these entries are marked by $*$. Since all currently known non-trivial constructions are stabilizer codes, we use the notation $[\![n, k, d]\!]_q$ for both the lower and upper bound. The upper bound is valid for general codes $((n, D^k, d))_q$ as well.

n + k	upper	lower		
4	$[\![4,0,3]\!]_3$	$[\![4,0,3]\!]_3$	$*$	Hermitean
6	$[\![6,0,4]\!]_3$	$[\![6,0,4]\!]_3$	$*$	Rains [17]
8	$[\![6,2,3]\!]_3$	$[\![6,2,3]\!]_3$	$*$	single-error
10	$[\![10,0,6]\!]_3$	$[\![10,0,6]\!]_3$	$*$	Glynn code [70]
12	$[\![8,4,3]\!]_3$	$[\![8,4,3]\!]_3$	$*$	single-error
14	$[\![11,3,5]\!]_3$	$[\![10,4,4]\!]_3$		Grassl/Rötteler I
16	$[\![11,5,4]\!]_3$	$[\![10,6,3]\!]_3$		single-error

Table 2: Upper and lower bounds for the highest distance in QMDS families of local dimension $D = 3$.

n + k	upper	lower		
4	$[\![4,0,3]\!]_4$	$[\![4,0,3]\!]_4$	$*$	Hermitean
6	$[\![6,0,4]\!]_4$	$[\![6,0,4]\!]_4$	$*$	Rains [17]
8	$[\![8,0,5]\!]_4$	$[\![6,2,3]\!]_4$		single-error
10	$[\![10,0,6]\!]_4$	$[\![10,0,6]\!]_4$	$*$	Gulliver et al. [71]
12	$[\![10,2,5]\!]_4$	$[\![9,3,4]\!]_4$		Grassl/Rötteler [30]
14	$[\![14,0,8]\!]_4$	$[\![10,4,4]\!]_4$		shortening $[\![18,12,4]\!]_4$
16	$[\![13,3,6]\!]_4$	$[\![11,5,4]\!]_4$		Grassl/Rötteler [30]
18	$[\![18,0,10]\!]_4$	$[\![12,6,4]\!]_4$		shortening $[\![18,12,4]\!]_4$
20	$[\![16,4,7]\!]_4$	$[\![12,8,3]\!]_4$		single-error
22	$[\![22,0,12]\!]_4$	$[\![14,8,4]\!]_4$		shortening $[\![18,12,4]\!]_4$
24	$[\![19,5,8]\!]_4$	$[\![14,10,3]\!]_4$		single-error
26	$[\![23,3,11]\!]_4$	$[\![17,9,5]\!]_4$		Grassl/Rötteler I
28	$[\![22,6,9]\!]_4$	$[\![16,12,3]\!]_4$		single-error
30	$[\![26,4,12]\!]_4$	$[\![18,12,4]\!]_4$		Grassl/Rötteler II

Table 3: Upper and lower bounds for the highest distance in QMDS families of local dimension $D = 4$.

n + k	upper	lower		
4	$[\![4,0,3]\!]_5$	$[\![4,0,3]\!]_5$	$*$	Hermitean
6	$[\![6,0,4]\!]_5$	$[\![6,0,4]\!]_5$	$*$	Rains [17]
8	$[\![8,0,5]\!]_5$	$[\![8,0,5]\!]_5$	$*$	Kim/Lee [72]
10	$[\![10,0,6]\!]_5$	$[\![10,0,6]\!]_5$	$*$	Kim/Lee [72]
12	$[\![12,0,7]\!]_5$	$[\![10,2,5]\!]_5$		shortening $[\![26,18,5]\!]_5$
14	$[\![14,0,8]\!]_5$	$[\![14,0,8]\!]_5$	$*$	Ball [69]
16	$[\![16,0,9]\!]_5$	$[\![12,4,5]\!]_5$		shortening $[\![26,18,5]\!]_5$
18	$[\![18,0,10]\!]_5$	$[\![18,0,10]\!]_5$	$*$	Ball [69]
20	$[\![20,0,11]\!]_5$	$[\![14,6,5]\!]_5$		shortening $[\![26,18,5]\!]_5$
22	$[\![22,0,12]\!]_5$	$[\![15,7,5]\!]_5$		shortening $[\![26,18,5]\!]_5$
24	$[\![24,0,13]\!]_5$	$[\![16,8,5]\!]_5$		shortening $[\![26,18,5]\!]_5$
26	$[\![26,0,14]\!]_5$	$[\![17,9,5]\!]_5$		shortening $[\![26,18,5]\!]_5$
28	$[\![26,2,13]\!]_5$	$[\![18,10,5]\!]_5$		shortening $[\![26,18,5]\!]_5$
30	$[\![30,0,16]\!]_5$	$[\![19,11,5]\!]_5$		shortening $[\![26,18,5]\!]_5$
32	$[\![30,2,15]\!]_5$	$[\![20,12,5]\!]_5$		shortening $[\![26,18,5]\!]_5$
34	$[\![34,0,18]\!]_5$	$[\![21,13,5]\!]_5$		shortening $[\![26,18,5]\!]_5$
36	$[\![34,2,17]\!]_5$	$[\![22,14,5]\!]_5$		shortening $[\![26,18,5]\!]_5$
38	$[\![38,0,20]\!]_5$	$[\![23,15,5]\!]_5$		shortening $[\![26,18,5]\!]_5$
40	$[\![37,3,18]\!]_5$	$[\![24,16,5]\!]_5$		shortening $[\![26,18,5]\!]_5$
42	$[\![42,0,22]\!]_5$	$[\![26,16,6]\!]_5$		Grassl/Rötteler I
44	$[\![41,3,20]\!]_5$	$[\![26,18,5]\!]_5$		Grassl/Rötteler I
46	$[\![46,0,24]\!]_5$	$[\![26,20,4]\!]_5$		Grassl/Rötteler I
48	$[\![45,3,22]\!]_5$	$[\![26,22,3]\!]_5$		single-error

Table 4: Upper and lower bounds for the highest distance in QMDS families of local dimension $D = 5$.

References

[1] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," Phys. Rev. A **52**, 2493(R) (1995).

[2] A. M. Steane, "Error Correcting Codes in Quantum Theory," Phys. Rev. Lett. **77**, 793–797 (1996).

[3] E. Knill and R. Laflamme, "Theory of quantum error-correcting codes," Phys. Rev. A **55**, 900–911 (1997).

[4] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed-state entanglement and quantum error correction," Phys. Rev. A **54**, 3824 (1996).

[5] B. Schumacher and M. A. Nielsen, "Quantum data processing and error correction," Phys. Rev. A **54**, 2629–2635 (1996).

[6] A. R. Calderbank, E. M. Rains, P. M. Shor, and N. J. A. Sloane, "Quantum error correction via codes over GF(4)," IEEE Trans. Inf. Theory **44**, 1369 (1998).

[7] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill, "Topological quantum memory," J. Math. Phys. **43**, 4452–4505 (2002).

[8] H. Bombin and M. A. Martin-Delgado, "Topological Quantum Distillation," Phys. Rev. Lett. **97**, 180501 (2006).

[9] J. Tillich and G. Zémor, "Quantum LDPC Codes With Positive Rate and Minimum Distance Proportional to the Square Root of the Blocklength," IEEE Trans. Inf. Theory **60**, 1193–1202 (2014).

[10] M. B. Hastings and S. Bravyi, "Homological Product Codes," in *Proc. of the 46th ACM Symposium on Theory of Computing* (2014) pp. 273–282.

[11] B. M. Terhal, "Quantum error correction for quantum memories," Rev. Mod. Phys. **87**, 307–346 (2015).

[12] E. T. Campbell, B. M. Terhal, and V. Christophe, "Roads towards fault-tolerant

universal quantum computation," Nature **549**, 172 (2017).

[13] A. Ashikhmin and S. Litsyu, "Upper bounds on the size of quantum codes," IEEE Trans. Inf. Theory **45**, 1206–1215 (1999).

[14] D. Chandra, Z. Babar, H. V. Nguyen, D. Alanis, P. Botsinis, S. X. Ng, and L. Hanzo, "Quantum Coding Bounds and a Closed-Form Approximation of the Minimum Distance Versus Quantum Coding Rate," IEEE Access **5**, 11557–11581 (2017).

[15] N. J. Cerf and R. Cleve, "Information-theoretic interpretation of quantum error-correcting codes," Phys. Rev. A **56**, 1721–1732 (1997).

[16] D. Gottesman, "Lecture Notes CO639," available online at `www.perimeterinstitute.ca/personal/dgottesman/CO639-2004/` (2004).

[17] E. M. Rains, "Nonbinary quantum codes," IEEE Trans. Inf. Theory **45**, 1827 (1999).

[18] W. Dür, G. Vidal, and J. I. Cirac, "Three qubits can be entangled in two inequivalent ways," Phys. Rev. A **62**, 062314 (2000).

[19] M. Walter, D. Gross, and J. Eisert, "Multi-partite entanglement," (2017), arXiv:1612.02437.

[20] I. Bengtsson and K. Życzkowski, *Geometry of Quantum States: An Introduction to Quantum Entanglement*, 2nd ed. (Cambridge University Press, 2017).

[21] T. Cubitt, A. Montanaro, and A. Winter, "On the dimension of subspaces with bounded Schmidt rank," J. Math. Phys. **49**, 022107 (2008).

[22] N. Johnston, "Non-positive-partial-transpose subspaces can be as large as any entangled subspace," Phys. Rev. A **87**, 064302 (2013).

[23] J. Walgate and A. J. Scott, "Generic local distinguishability and completely entangled subspaces," J. Phys. A: Math. Theor. **41**, 375305 (2008).

[24] R. Sengupta, Arvind, and A. I. Singh, "Entanglement properties of positive operators with ranges in completely entangled subspaces," Phys. Rev. A **90**, 062323 (2014).

[25] M. Demianowicz and R. Augusiak, "From unextendible product bases to genuinely entangled subspaces," Phys. Rev. A **98**, 012313 (2018).

[26] M. Demianowicz and R. Augusiak, "Entanglement of genuinely entangled subspaces and states: Exact, approximate, and numerical results," Phys. Rev. A **100**, 062318 (2019).

[27] M. Demianowicz and R. Augusiak, "An approach to constructing genuinely entangled subspaces of maximal dimension," Quantum Inf. Process. **19**, 199 (2020).

[28] G. Gour and N. R. Wallach, "Entanglement of subspaces and error-correcting codes," Phys. Rev. A **76**, 042309 (2007).

[29] M. Grassl, T. Beth, and M. Rötteler, "On optimal quantum codes," Int. J. Quant. Inf. **2**, 55 (2004).

[30] M. Grassl and M. Rötteler, "Quantum MDS codes over small fields," in *IEEE Int. Symp. Inf. Theory (ISIT 2015)* (2015) pp. 1104–1108.

[31] G. G. L. Guardia, "New Quantum MDS Codes," IEEE Trans. Inf. Theory **57**, 5551–5554 (2011).

[32] W. Helwig, *Multipartite Entanglement: Transformations, Quantum Secret Sharing, Quantum Error Correction*, Ph.D. thesis, University of Toronto (2014).

[33] D. Joyner and J.-L. Kim, *Selected Unsolved Problems in Coding Theory (Applied and Numerical Harmonic Analysis)*, 1st ed. (Birkhäuser Basel, 2011).

[34] S. Ball, "On sets of vectors of a finite vector space in which every subset of basis size is a basis," J. Eur. Math. Soc. **14**, 733–748 (2012).

[35] C. Eltschka, F. Huber, O. Gühne, and J. Siewert, "Exponentially many entanglement and correlation constraints for multipartite quantum states," Phys. Rev. A **98**, 052317 (2018).

[36] E. Knill, R. Laflamme, and L. Viola, "Theory of Quantum Error Correction for General Noise," Phys. Rev. Lett. **84**, 2525–2528 (2000).

[37] D. Gottesman, "An Introduction to Quantum Error Correction," in *Quantum computation: A grand mathematical challenge for the twenty-first century and the millennium,* ed. S. J. Lomonaco, Jr., pp. 221–235, (American Mathematical Society, 2002) arXiv:quant-ph/0004072.

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

[39] P. Shor and R. Laflamme, "Quantum Analog of the MacWilliams Identities for Classical Coding Theory," Phys. Rev. Lett. **78**, 1600–1602 (1997).

[40] E. M. Rains, "Quantum weight enumerators," IEEE Trans. Inf. Theory **44**, 1388–1394 (1998).

[41] F. Huber, C. Eltschka, J. Siewert, and O. Gühne, "Bounds on absolutely maximally entangled states from shadow inequalities, and the quantum MacWilliams identity," J. Phys. A: Math. Theor. **51**, 175301 (2018).

[42] A. Ashikhmin and A. Barg, "Binomial moments of the distance distribution: bounds and applications," IEEE Transactions on Information Theory **45**, 438–452 (1999).

[43] D. Gottesman, *Stabilizer Codes and Quantum Error Correction*, Ph.D. thesis, Caltech (1997), arXiv:quant-ph/9705052.

[44] D. Alsina and M. Razavi, "Absolutely maximally entangled states, quantum maximum distance separable codes, and quantum repeaters," (2019), arXiv:1907.11253.

[45] T. A. Brun and D. E. Lidar, *Quantum Error Correction* (Cambridge University Press, 2013).

[46] A. Winter, private communication (2019).

[47] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes* (Cambridge University Press, 2003).

[48] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes* (North Holland, 1981).

[49] R. P. Stanley, *Enumerative Combinatorics: Volume 1*, 2nd ed. (Cambridge University Press, 2011).

[50] A. J. Scott, "Multipartite entanglement, quantum-error-correcting codes, and entangling power of quantum evolutions," Phys. Rev. A **69**, 052330 (2004).

[51] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, "Nonbinary Stabilizer Codes Over Finite Fields," IEEE Trans. Inf. Theory **52**, 4892–4914 (2006).

[52] W. Helwig, W. Cui, J. I. Latorre, A. Riera, and H.-K. Lo, "Absolute maximal entanglement and quantum secret sharing," Phys. Rev. A **86**, 052335 (2012).

[53] F. Huber, O. Gühne, and J. Siewert, "Absolutely Maximally Entangled States of Seven Qubits Do Not Exist," Phys. Rev. Lett. **118**, 200502 (2017).

[54] F. Huber and N. Wyderka, "Table of AME states," available online at `http://www.tp.nt.uni-siegen.de/+fhuber/ame.html` (2020).

[55] E. M. Rains, "Polynomial invariants of quantum codes," IEEE Trans. Inf. Theory **46**, 54–59 (2000).

[56] E. M. Rains, "Quantum shadow enumerators," IEEE Trans. Inf. Theory **45**, 2361–2366 (1999).

[57] G. Nebe, E. M. Rains, and N. J. A. Sloane, *Self-Dual Codes and Invariant Theory* (Springer Berlin-Heidelberg, 2006).

[58] E. M. Rains, "Quantum codes of minimum distance two," IEEE Trans. Inf. Theory **45**, 266–271 (1999).

[59] P. Horodecki, L. Rudnicki, and K. Życzkowski, "Five open problems in quantum information," (2020), arXiv:2002.03233.

[60] A. Ashikhmin, "Remarks on Bounds for Quantum Codes," (1997), arXiv:quant-ph/9705037.

[61] A. Ashikhmin and S. Litsyu, "Upper bounds on the size of quantum codes," IEEE Transactions on Information Theory **45**, 1206–1215 (1999).

[62] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, 2011).

[63] A. Müller-Hermes, D. Stilck França, and M. M. Wolf, "Relative entropy convergence for depolarizing channels," J. Math. Phys. **57**, 022202 (2016).

[64] A. Klappenecker and M. Rötteler, "Beyond stabilizer codes. I. Nice error bases," IEEE Trans. Inf. Theory **48**, 2392–2395 (2002).

[65] M. Rötteler, M. Grassl, and T. Beth, "On quantum MDS codes," in *Proceedings, Int. Symp. Inf. Theory (ISIT 2004)* (2004) p. 356.

[66] P. K. Sarvepalli and A. Klappenecker, "Nonbinary quantum Reed-Muller codes," in *Proceedings. Int. Symp. Inf. Theory, (ISIT 2005)* (2005) pp. 1023–1027.

[67] L. Jin, S. Ling, J. Luo, and C. Xing, "Application of classical Hermitian self-orthogonal MDS codes to quantum MDS codes," IEEE Trans. Inf. Theory **56**, 4735–4740 (2010).

[68] R. Li and Z. Xu, "Construction of $[\![n, n-4, 3]\!]_q$ quantum codes for odd prime power q," Phys. Rev. A **82**, 052316 (2010).

[69] S. Ball, "Some constructions of quantum MDS codes," (2019), arXiv:1907.04391.

[70] D. G. Glynn, "The non-classical 10-arc of $PG(4, 9)$," Discrete Math. **59**, 43–51 (1986).

[71] T. A. Gulliver, J. Kim, and Y. Lee, "New MDS or near-MDS self-dual codes," IEEE Trans. Inf. Theory **54**, 4354–4360 (2008).

[72] J.-L. Kim and Y. Lee, "Euclidean and Hermitian self-dual MDS codes over large finite fields," J. Comb. Theory A **105**, 79–95 (2004).

Accepted in ⟨ ⟩uantum 2020-06-09, click title to verify. Published under CC-BY 4.0.

15