Designs, Codes and Cryptography (2022) 90:1103–1112
https://doi.org/10.1007/s10623-022-01018-2

On the generalization of the construction of quantum codes from Hermitian self-orthogonal codes

Carlos Galindo[1] · **Fernando Hernando**[1]

Received: 8 March 2021 / Revised: 21 October 2021 / Accepted: 3 February 2022 /
Published online: 21 March 2022

Abstract
Many q-ary stabilizer quantum codes can be constructed from Hermitian self-orthogonal q^2-ary linear codes. This result can be generalized to q^{2m}-ary linear codes, $m > 1$. We give a result for easily obtaining quantum codes from that generalization. As a consequence we provide several new binary stabilizer quantum codes which are records according to Grassl (Bounds on the minimum distance of linear codes, http://www.codetables.de, 2020) and new q-ary ones, with $q \neq 2$, improving others in the literature.

Keywords Stabilizer quantum codes · Hermitian duality · Self-orthogonal codes

Mathematics Subject Classification 81P70 · 94B27

1 Introduction

The importance of quantum information processing is beyond doubt due to its spectacular applications. Nowadays there is some evidence of quantum processors capable of executing certain tasks greatly improving classical processors [2] which increases the interest in tools for the proper functioning of quantum computers such as the quantum error-correcting codes (QECCs). QECCs are mainly designed for protecting quantum information from quantum noise and decoherence. Notice that, despite quantum information cannot be cloned [14, 42], quantum error correction works [38,40]. These facts explain why many researchers are

Communicated by D. Panario.

Partially supported by MCIN/AEI/10.13039/501100011033/FEDER "A way to make Europe", Grants PGC2018-096446-B-C22 and RED2018-102583-T, as well as by Universitat Jaume I, Grant UJI-B2021-02.

✉ Carlos Galindo
galindo@uji.es

Fernando Hernando
carrillf@uji.es

[1] Instituto Universitario de Matemáticas y Aplicaciones de Castellón and Departamento de Matemáticas, Universitat Jaume I, Campus de Riu Sec., 12071 Castelló, Spain

interested in obtaining QECCs with good parameters (which measure the behaviour of the codes) and the literature contains a large quantity of papers devoted to finding QECCs with better parameters than others previously obtained.

QECCs were firstly introduced in the binary case, where one finds the seminal papers on the subject [4,5,7–9,21,24]. Later QECCs were studied for the general q-ary case (see [1,3,6,11,12,16–20,25,27,28,30–32,35,39] among many other articles). The general case is particularly interesting for fault-tolerant computing [10,22,29,33,36,37,41].

Let q be a prime power, a q-ary QECC of length n is a subspace of the Hilbert space $\mathcal{H} = \mathbb{C}^{q^n}$. The most used class of quantum codes are stabilizer quantum codes. They are obtained as the intersection of the eigenspaces, corresponding to the eigenvalue 1, of the elements of some subgroup of the error group generated by a suitable error basis of the Hilbert space $\mathcal{H}$. The parameters of a QECC, length, dimension and minimum distance, are usually denoted by $((n, K, d))_q$, where errors with weight less than d either can be detected or have no effect on C but some error with weight d cannot be detected. We are only interested in q^k-dimensional subspaces of $\mathcal{H}$ and, abusing of notation and when no confusion arises, we say that these QECCs have dimension k; in this case, the parameters are usually written as $[[n, k, d]]_q$.

One of the main advantages of stabilizer codes is that their existence is equivalent to that of self-orthogonal additive codes with respect to a certain trace-symplectic form (see [3] or [28, Theorem 13]). This trace-symplectic form is not very used but the above result allows us to deduce that many stabilizer quantum codes can be derived from self-orthogonal classical codes with respect to the Hermitian or the Euclidean inner product. Usually one finds good q-ary stabilizer codes by considering Hermitian self-orthogonal codes over $\mathbb{F}_{q^2}$. The specific result, Theorem 2.1, shows that an $[[n, n-2k, \geq d^{\perp_h}]]_q$ quantum code can be constructed from a Hermitian self-orthogonal $[n, k]_{q^2}$ linear code C over $\mathbb{F}_{q^2}$, where $d^{\perp_h}$ stands for the minimum distance of the Hermitian dual code $C^{\perp_h}$. This result has been extensively used in many papers to give many good QECCs [27,30,31,43].

In the present paper we recall that Theorem 2.1 can be regarded as a special case of a more general result by considering linear codes over certain extensions of $\mathbb{F}_q$. Indeed, Theorem 2.2 states that if C is a linear code over $\mathbb{F}_{q^{2m}}$, $m \geq 1$, with parameters $[n, k]_{q^{2m}}$ which is self-orthogonal with respect to the Hermitian inner product, then there exists an $[[mn, mn - 2mk, \geq d^{\perp_h}]]_q$ stabilizer quantum code. Theorem 2.2 is a straightforward consequence of [28, Lemma 76] which seems to have gone unnoticed by many researchers because, in the literature, we have not found new quantum codes considering $m > 1$.

We expect that many good quantum codes can be established by this result. Our goal is to give some evidence by stating (and proving) Theorem 3.2 which combined with Theorem 2.2 gives rise to a number of stabilizer quantum codes with good parameters. Theorem 3.2 derives from [27] and gives an easy way to find Hermitian self-orthogonal codes. The above mentioned combination produces, in the binary case, new QECCs which are records according to [23]. Here, the word record means we provide codes for entries in [23] whose constructions were missing. There is no collection of tables as [23] for non-binary QECCs but one can find many papers in the literature about them. Most of these papers are devoted to quantum MDS codes which have relatively small length [13,26,43]. Since we are able to construct long QECCs, we use recent articles [12,34,39] for comparison and show that with our method we can improve the parameters of a number of codes therein.

Section 2 of the paper is devoted to recall Theorem 2.2 for obtaining QECCs from linear codes. Theorem 3.2 and parameters (some of them displayed in tables) of new QECCs can be found in Section 3. As mentioned all the provided parameters correspond to QECCs obtained

by applying Theorems 3.2 and 2.2. In the binary case, our results together with propagation rules determine 91 new QECCs which are records according to [23]. We use the rules that state that the existence of an $[[n, k, d]]_q$ stabilizer code $\mathcal{D}$ implies that of an $[[n+1, k, d]]_q$ stabilizer code (lengthening) and, also, when $k > 1$ or $\mathcal{D}$ is pure, that of an $[[n, k-1, \geq d]]_q$ stabilizer code (subcode-construction) [28, Lemmas 69 and 71].

2 A construction of stabilizer quantum codes

Let $q = p^r$, where p is a prime and r a positive integer. Many good q-ary stabilizer quantum codes are obtained from linear codes over the finite field with q^2 elements, $\mathbb{F}_{q^2}$, which are self-orthogonal under the Hermitian inner-product. Recall that given two vectors $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$ and $\boldsymbol{y} = (y_1, y_2, \ldots, y_n)$ in $\mathbb{F}_{q^2}^n$, $n \geq 1$, their *Hermitian inner product* is defined by

$$\boldsymbol{x} \cdot_h \boldsymbol{y} := \sum_{i=1}^{n} x_i y_i^q \in \mathbb{F}_{q^2},$$

and the specific result to construct stabilizer quantum codes is the following (see [28, Corollary 16 and Lemma 18]).

Theorem 2.1 *Let C be an $\mathbb{F}_{q^2}$-linear code of length n and dimension k. Assume that C is Hermitian self-orthogonal, i.e.*

$$C \subseteq C^{\perp_h} := \left\{ \boldsymbol{x} \in \mathbb{F}_{q^2}^n \mid \boldsymbol{x} \cdot_h \boldsymbol{y} = 0 \text{ for all } \boldsymbol{y} \text{ in } C \right\}.$$

Then, there exists a q-ary stabilizer quantum code with parameters $[[n, n-2k, \geq d^{\perp_h}]]_q$, where $d^{\perp_h}$ stands for the minimum distance of the code $C^{\perp_h}$.

Next we recall a generalization of Theorem 2.1 allowing the use of codes over extension fields of $\mathbb{F}_{q^2}$. We will prove that one can obtain long q-ary stabilizer codes with good parameters by considering linear codes over fields $\mathbb{F}_{q^{2m}}$, $m > 0$, which are self-orthogonal with respect to the Hermitian inner product.

Theorem 2.2 *Let C be an $\mathbb{F}_{q^{2m}}$-linear code of length n and dimension k, $m > 0$. Suppose that $C \subseteq C^{\perp_h}$, where*

$$C^{\perp_h} := \left\{ \boldsymbol{x} \in \left(\mathbb{F}_{q^{2m}}\right)^n \mid \boldsymbol{x} \cdot_h \boldsymbol{y} := \sum_{i=1}^{n} x_i y_i^{q^m} = 0 \text{ for all } \boldsymbol{y} \text{ in } C \right\}.$$

Then, there exists a stabilizer quantum code with parameters

$$\left[\left[mn, mn - 2mk, \geq d_h^{\perp}\right]\right]_q,$$

where $d_h^{\perp}$ is the minimum distance of the code $C^{\perp_h}$.

This result can be deduced from Lemma 76 in [28] (see also [3]) which states that the existence of an $((n, K, d))_{q^m}$ stabilizer code implies that of an $((mn, K, \geq d))_q$ stabilizer code. Then, to deduce Theorem 2.2, it suffices to consider the above code C to obtain an $[[n, n-2k, \geq d^{\perp_h}]]_{q^m}$ stabilizer code by applying Theorem 2.1 and by [28, Lemma 76] there exists a q-ary stabilizer code as in the statement.

Surprisingly we have not found in the literature new quantum codes obtained from Theorem 2.2, $m > 1$. We think that this result goes unnoticed by many researchers. We learned it when a reviewer pointed out to us the existence of [28, Lemma 76] after a first version of this paper where, in a different way, we proved Theorem 2.2 for the particular case where $m = 2^{\ell-1}$, $\ell \geq 1$.

3 Hermitian self-orthogonal codes and examples

We devote this section to show that Theorem 2.2 allows us to obtain stabilizer quantum codes with better parameters than those in the present literature.

3.1 A useful result

Next we state and prove a result derived from [27, Theorem 2.5] which provides suitable linear codes to apply Theorem 2.2. This procedure gives some binary stabilizer quantum codes which are records according to [23] (in the sense explained in the introduction) and also some q-ary stabilizer quantum codes, $q \neq 2$, improving the parameters of codes in the recent literature.

We start by recalling Theorem 2.5 in [27].

Theorem 3.1 *Let e be a prime power and set $Q = e^2$. Consider an integer $2 \leq n \leq Q$ and write $n = n_1 + n_2 + \cdots + n_t$, where $1 \leq t \leq e$ and $2 \leq n_i \leq e$ for all $1 \leq i \leq t$. Then, for any positive integer*

$$1 \leq k \leq \frac{\min\{n_1, n_2, \ldots, n_t\}}{2},$$

there exists an $[n, k]_Q$ linear code $\mathcal{C}$ over the field $\mathbb{F}_Q$ which is Hermitian self-orthogonal. $\mathcal{C}$ is a generalized Reed-Solomon code and, therefore, it is a maximum distance separable (MDS) code and the minimum distance of $\mathcal{C}^{\perp_h}$ is $k + 1$.

Next we state a new result which will be useful.

Theorem 3.2 *Let $e > 2$ be a prime power and set $Q := e^2$. Consider an integer $2 \leq n \leq Q$ and write n as $n = ae + b$, where $0 \leq a < e$ and $0 \leq b < e$, i.e. the e-adic expression of n, and include the case $a = e$ and $b = 0$.*

Define K_n as follows: $K_n := \lfloor e/2 \rfloor$ when $b = 0$. $K_n := \lfloor n/2 \rfloor$ when $a = 0$. $K_n := \lfloor (e-1)/2 \rfloor$ when $a \neq 0$, $b \neq 0$ and $a + b \geq e$. Otherwise,

$$K_n := \left\lfloor \frac{\max\{\lfloor n/(a+1) \rfloor, a + b\}}{2} \right\rfloor.$$

Then, for each $1 \leq k \leq K_n$, there exists an $[n, k]_Q$ linear code $\mathcal{C}$ which is self-orthogonal for the Hermitian inner product. $\mathcal{C}$ is a generalized Reed-Solomon code and therefore the minimum distance of the Hermitian dual code $\mathcal{C}^{\perp_h}$ is $k + 1$.

Proof Assume $b = 0$, then the result holds by setting $n_1 = n_2 = \cdots = n_a = e$ and applying Theorem 3.1. When $a = 0$, the same theorem with $n_1 = n$ proves the result.

Suppose $a \neq 0 \neq b$ and $a + b \geq e$. Let us see that there exist non-negative integers i, j such that $i + j = a$ and positive integers $n_1 = \cdots = n_i = e$, $n_{i+1} = \cdots = n_{i+j} = e - 1$

and $n_{a+1} = e - 1$ that are suitable to apply Theorem 3.1, which concludes the result in this case. Indeed,

$$ie + j(e-1) + e - 1 = (i+j)e + e - 1 - j = ae + e - 1 - j = n,$$

for some j because the fact that $a+b \geq e$ proves the existence of such a j with $0 \leq j \leq e-1$.

Finally, assume $a + b < e$. Then, on the one hand, setting $n_1 = n_2 = \cdots = n_a = e - 1$ and $n_{a+1} = a + b$, we find the second bound for k, $\lfloor (a+b)/2 \rfloor$, by Theorem 3.1. With respect to the first one, it is clear that

$$(a+1)\left\lfloor \frac{n}{a+1} \right\rfloor \leq n \leq (a+1)\left(\left\lfloor \frac{n}{a+1} \right\rfloor + 1\right).$$

This implies that a set $\{n_i\}_{i=1}^{a+1}$ as in Theorem 3.1 can be constructed for values n_i which are either $\left\lfloor \frac{n}{a+1} \right\rfloor$ or $\left\lfloor \frac{n}{a+1} \right\rfloor + 1$. This concludes the proof because we can choose the best bound. □

Remark 3.3 Combining Theorems 3.2 and 2.1, one gets quantum MDS (QMDS) codes, that is $[[n, n-2k, k+1]]_e$ quantum codes achieving the quantum Singleton bound.

3.2 Examples

In this subsection we determine the parameters of some (constructible) q-ary stabilizer quantum codes for small prime powers q.

3.2.1 Binary stabilizer quantum codes

We start with binary codes. In this case we give a number of quantum codes which are records according to [23], that is we give codes for entries in [23] whose constructions were missing. We explain in detail how we get our first binary code.

We start with the values $e = 16$ and $Q = 16^2 = 256$. By Theorem 3.2, we can consider the value $n = 63$ because $2 \leq 63 \leq 256$ and $63 = n = 3 \cdot 16 + 15$. Thus $a = 3$ and $b = 15$. Since $a + b \geq 16$, $K_{63} = \lfloor 15/2 \rfloor = 7$. Then, by Theorem 3.2, there exists a suitable linear code $\mathcal{C}$ over $\mathbb{F}_Q$ with length $n = 63$, dimension $k = 6$ and $d(\mathcal{C}^{\perp_h}) = 7$. The code $\mathcal{C}$ gives rise to a $[[63, 51, 7]]_{16}$ QMDS code by Remark 3.3. Now $Q = q^{2m}$ for $q = 2$ and $m = 4$. Applying Theorem 2.2, we get a $[[252, 204, \geq 7]]_2$ quantum code which is a record. If we pick $n = 62$ and $k = 7$, then a new record is obtained: $[[248, 192, \geq 8]]_2$.

With an analogous procedure we obtain new records according to [23]. By using either lengthening or subcode-construction (the two propagation rules described at the end of the introduction) we get more records. All of them are grouped in Table 1, where the parameters obtained without propagation rules are marked with a * and those obtained by lengthening (respectively, subcode-construction) are marked with an L (respectively, S).

3.2.2 Non-binary stabilizer quantum codes

As we did in the binary case, we explain in detail the construction of some families of good 4-ary stabilizer quantum codes. We will only show the parameters of the remaining stabilizer codes which can be obtained in a similar way.

Set $e = 16$, $Q = 16^2 = 256$ and, applying Theorem 3.2, pick $n = 76$, which accomplishes $2 \leq 76 \leq 256$. Now $n = 76 = 4 \cdot 16 + 12$, then under the notation of that theorem $a = 4$

Table 1 Binary stabilizer quantum records

n	k	$\geq d$	n	k	$\geq d$	n	k	$\geq d$	n	k	$\geq d$
252*	204	7	252*	196	8	248*	200	7	248*	192	8
244*	196	7	244*	188	8	240*	192	7	240*	184	8
252^S	203	7	252^S	195	8	251^L	200	7	251^S	199	7
251^S	198	7	251^L	192	8	251^S	191	8	251^S	190	8
250^L	200	7	250^S	199	7	250^S	198	7	250^S	197	7
250^L	196	7	250^L	192	8	250^S	191	8	250^S	190	8
249^L	200	7	249^S	199	7	249^S	198	7	249^S	197	7
249^S	196	7	249^S	195	7	249^L	192	8	249^S	191	8
249^S	190	8	249^S	189	8	248^S	199	7	248^S	198	7
248^S	197	7	248^S	196	7	248^S	195	7	248^S	194	7
248^S	191	8	248^S	190	8	248^S	189	8	248^S	188	8
247^L	196	7	247^S	195	7	247^S	194	7	247^S	193	7
247^L	188	8	247^S	187	8	246^L	196	7	246^S	195	7
246^S	194	7	246^S	193	7	246^S	192	7	246^L	188	8
246^S	187	8	246^S	186	8	245^L	196	7	245^S	195	7
245^S	194	7	245^S	193	7	245^S	192	7	245^S	191	7
245^L	188	8	245^S	187	8	245^S	186	8	245^S	185	8
244^S	195	7	244^S	194	7	244^S	193	7	244^S	192	7
244^S	191	7	244^S	187	8	244^S	186	8	244^S	185	8
244^S	184	8	243^L	192	7	243^S	191	7	243^L	184	8
243^S	183	8	242^L	192	7	242^S	191	7	242^L	184	8
242^S	183	8	241^L	192	7	241^S	191	7	241^L	184	8
241^S	183	8	240^S	191	7	240^S	183	8	–	–	–

Table 2 4-ary stabilizer quantum codes

n	k	$\geq d$	n	k	$\geq d$
152	148	2	152	144	3
152	140	4	152	136	5
152	132	6	152	128	7
152	124	8	–	–	–

and $b = 12$. Since $a + b \geq 16$, $K_{76} = 7$, and there exists a linear code over $\mathbb{F}_Q$ which is self-orthogonal for the Hermitian inner product, where $Q = q^{2m}$ for $q = 4$ and $m = 2$. Applying Theorem 2.2, we find the 4-ary stabilizer quantum codes shown in Table 2. The $[[152, 148, \geq 2]]_4$ quantum code in Table 2 has worse parameters than the QMDS code with parameters $[[152, 150, 2]]_4$ that is known to exist.

By lengthening some codes in Table 2, we obtain quantum codes with parameters

$$[[153, 140, \geq 4]]_4, [[153, 136, \geq 5]]_4, [[153, 132, \geq 6]]_4 \text{ and } [[153, 128, \geq 7]]_4$$

improving some codes in (and adding a new one to) [39, Table 3].

Table 3 5-ary stabilizer quantum codes

n	k	$\geq d$	n	k	$\geq d$
468	452	5	468	448	6
468	444	7	468	440	8
468	436	9	468	432	10
468	428	11	468	424	12

Looking for more 4-ary stabilizer codes, set $q = 4$ and $m = 3$. Write $Q = q^{2m}$ and $e = q^m = 64$. Pick $n = 255$ which gives $a = 3$ and $b = 63$ with the notation of Theorem 3.2. Then $K_{255} = 31$ and applying Theorems 3.2 and 2.2 one gets a family of stabilizer codes with parameters

$$\{[[765, 765 - 6j, \geq 1 + j]]_4\}_{18 \leq j \leq 31}.$$

These codes have better parameters than some codes given in [39, Table 2] whose minimum distance d satisfies $19 \leq d \leq 32$. For instance we give codes with parameters $[[765, 657, \geq 19]]_4$, $[[765, 651, \geq 20]]_4$ and $[[765, 645, \geq 21]]_4$ while the parameters of the corresponding codes in [39] are $[[765, 643, \geq 19]]_4$, $[[765, 639, \geq 20]]_4$ and $[[765, 631, \geq 21]]_4$.

We conclude this section by giving some more families of stabilizer quantum codes obtained with our procedure.

We start with a 3-ary stablizer quantum code with parameters $[[110, 98, \geq 4]]_3$ which improves the quantum code with parameters $[[110, 96, \geq 4]]_3$ given in [34]. Our code is obtained by setting, with the previous notation, $n = 55$, $q = 3$ and $m = 2$.

Similarly, considering $n = 234$, we get 5-ary stabilizer quantum codes with parameters as in Table 3.

Notice that we significantly improve the parameters of some codes given in [39, Table 4].

Now we provide the parameters of a family of 7-ary QECCs. Consider $Q = 2401 = 7^4$ and $n = 196$, again by Theorems 3.2 and 2.2 we get a family of stabilizer quantum codes with parameters

$$\left\{[[392, 388 - 4j, \geq 2 + j]]_7\right\}_{j=3}^{23}.$$

Comparing with [12, Table 3], we obtain many more 7-ary quantum codes of length 392. For $j = 3, 4$ our parameters coincide with those in [12] and we get a $[[392, 368, \geq 7]]_7$ code which improves the $[[392, 364, \geq 7]]_7$ code in [12].

Our next family corresponds to $q = 8$. Theorems 3.2 and 2.2 for $Q = 8^4 = 4096$ and $n = 283$ give rise to a new family of QECCs with parameters

$$\left\{[[566, 562 - 4j, \geq 2 + j]]_8\right\}_{j=5}^{27}.$$

After lengthening, one gets a set of QECCs with parameters

$$\left\{[[567, 562 - 4j, \geq 2 + j]]_8\right\}_{j=5}^{27}.$$

As before, we add many new codes to those 8-ary ones in [12, Table 1] of length 567 and obtain a code with parameters $[[567, 542, \geq 7]]_8$ improving the $[[567, 539, \geq 7]]_8$ code in [12].

To end, set $Q = 6561 = 9^4$. As above

- Picking $n = 200$, we get a family of 9-ary stabilizer quantum with parameters:

$$\left\{[[400, 396 - 4j, \geq 2 + j]]_9\right\}_{j=3}^{32}.$$

- Setting $n = 400$, we obtain:

$$\left\{[[800, 796 - 4j, \geq 2 + j]]_9\right\}_{j=3}^{39}.$$

- With $n = 405$, we obtain:

$$\left\{[[810, 806 - 4j, \geq 2 + j]]_9\right\}_{j=3}^{39}.$$

- Finally, with $n = 162$, we get:

$$\left\{[[324, 320 - 4j, \geq 2 + j]]_9\right\}_{10\neq j=7}^{39}.$$

With respect to Tables 1, 3, 5 and 8 in [12] we add quite a few new codes. In addition we obtain several codes with better parameters than those given in [12]: $[[400, 376, \geq 7]]_9$, $[[800, 776, \geq 7]]_9$, $[[800, 772, \geq 8]]_9$, $[[810, 786, \geq 7]]_9$, $[[810, 782, \geq 8]]_9$, $[[810, 778, \geq 9]]_9$, $[[324, 276, \geq 13]]_9$ and $[[324, 260, \geq 17]]_9$.

Notice that, when providing our families of q-ary codes, $q = 4, 7, 8, 9$, we have considered different values for the indices j in order to get parameters which are either new or better than or equal to those in [12,39]. Finally it is worth pointing out that, when comparison is possible, the parameters of our codes are much better than those in [15].

Remark 3.4 We have explained how to get q-ary stabilizer codes with length nm by considering a class of Hermitian self-orthogonal codes of length n over the field $\mathbb{F}_{q^{2m}}$, where $2 \leq n \leq q^{2m}$. Dimensions and minimum distances of the stabilizer codes depend on the q^m-adic expression of n. In certain cases, one gets better quantum codes taking Hermitian self-orthogonal codes over fields $\mathbb{F}_{q^{2m'}}$ with $m' < m$. Indeed, when the length of the quantum codes we are looking for is less than or equal to $m'q^{2m'}$ and if there exists $n' \leq q^{2m'}$ such that $nm = n'm'$, then, for distances $d \leq \min\{K_n + 1, K_{n'} + 1\}$ (K_n and $K_{n'}$ defined as in Theorem 3.2 for suitable values $e = q^m$ and $e' = q^{m'}$), we obtain stabilizer codes with parameters $[[nm, nm - 2m(d - 1), \geq d]]_q$ if we use the extension field $\mathbb{F}_{q^{2m}}$ and better stabilizer codes with parameters $[[n'm' = nm, nm - 2m'(d - 1), \geq d]]_q$ when using the extension field $\mathbb{F}_{q^{2m'}}$.

Acknowledgements We thank the anonymous reviewers for their careful reading of our manuscript. We especially thank one of the reviewers for pointing out to us the existence of [28, Lemma 76].

Funding Open Access funding provided thanks to the CRUE-CSIC agreement with Springer Nature.

References

1. Aly S.A., Klappenecker S., Sarvepalli P.K.: On quantum and classical BCH codes. IEEE Trans. Inf. Theory **53**, 1183–1188 (2007).
2. Arute A.F., Babbush K.R., et al.: Quantum supremacy using a programmable superconducting processor. Nature **574**(219), 505–510 (2019).
3. Ashikhmin A., Knill E.: Non-binary quantum stabilizer codes. IEEE Trans. Inf. Theory **47**, 3065–3072 (2001).
4. Ashikhmin A., Barg A., Knill E., Litsyn S.: Quantum error-detection I: statement of the problem. IEEE Trans. Inf. Theory **46**, 778–788 (2000).
5. Ashikhmin A., Barg A., Knill E., Litsyn S.: Quantum error-detection II: bounds. IEEE Trans. Inf. Theory **46**, 789–800 (2000).
6. Bierbrauer J., Edel Y.: Quantum twisted codes. J. Comb. Des. **8**, 174–188 (2000).
7. Calderbank A.R., Shor P.: Good quantum error-correcting codes exist. Phys. Rev. A **54**, 1098–1105 (1996).
8. Calderbank A.R., Rains E.M., Shor P.W., Sloane N.J.A.: Quantum error correction and orthogonal geometry. Phys. Rev. Lett. **76**, 405–409 (1997).
9. Calderbank A.R., Rains E.M., Shor P.W., Sloane N.J.A.: Quantum error correction via codes over GF(4). IEEE Trans. Inf. Theory **44**, 1369–1387 (1998).
10. Campbell E.T., Terhal B.M., Vuillot C.: Roads towards fault-tolerant universal quantum computation. Nature **549**, 172–179 (2017).
11. Cao M., Cui J.: New stabilizer codes from the construction of dual-containing matrix-product codes. Finite Fields Appl. **63**, 101643 (2020).
12. Cao M., Cui J.: Construction of new quantum codes via Hermitian dual-containing matrix-product codes. Quant. Inf. Process. **19**, 427 (2020).
13. Chen B., Ling S., Zhang G.: Application of constancyclic codes to quantum MDS codes. IEEE Trans. Inf. Theory **61**, 1474–1484 (2015).
14. Dieks D.: Communication by EPR devices. Phys. Rev. A **92**, 271 (1982).
15. Edel Y.: Some good quantum twisted codes. http://www.mathi.uni-heidelberg.de/yves/Matritzen/QTBCH/QTBCHIndex.html.
16. Feng K.: Quantum Error Correcting Codes, pp. 91–142. In Coding Theory and Cryptology. Word Scientific, Singapore (2002).
17. Galindo C., Hernando F.: Quantum codes from affine variety codes and their subfield subcodes. Des. Codes Crytogr. **76**, 89–100 (2015).
18. Galindo C., Hernando F., Ruano D.: New quantum codes from evaluation and matrix-product codes. Finite Fields Appl. **36**, 98–120 (2015).
19. Galindo C., Geil O., Hernando F., Ruano D.: On the distance of stabilizer quantum codes from J-affine variety codes and a new Steane-like enlargement. Quant. Inf. Process. **14**, 3211–3231 (2015).
20. Galindo C., Hernando F., Ruano D.: Classical and quantum evaluation codes at the trace roots. IEEE Trans. Inf. Theory **65**, 2593–2602 (2019).
21. Gottesman D.: A class of quantum error-correcting codes saturating the quantum Hamming bound. Phys. Rev. A **54**, 1862–1868 (1996).
22. Gottesman D.: Fault-tolerant computation with higher-dimensional systems. Chaos Solitons Fractals **10**, 1749–1758 (1999).
23. Grassl M.: Bounds on the minimum distance of linear codes. http://www.codetables.de. Accessed 15 Nov (2020).
24. Grassl M., Rötteler M.: Quantum BCH codes. Proc. X Int. Symp. Theor. Elec. Eng. **1**, 207–212 (1999).
25. Grassl M., Beth T., Rötteler M.: On optimal quantum codes. Int. J. Quant. Inf. **2**, 757–775 (2004).
26. He X., Xu L., Chen H.: New q-ary quantum MDS codes with distances bigger than $q/2$. Quant. Inf. Process. **15**, 2745–2758 (2016).
27. Jin L., Ling S., Luo J., Xing C.: Application of classical Hermitian self-orthogonal MDS codes to quantum MDS codes. IEEE Trans. Inf. Theory **56**, 4735–4740 (2010).
28. Ketkar A., Klappenecker A., Kumar S., Sarvepalli P.K.: Nonbinary stabilizer codes over finite fields. IEEE Trans. Inf. Theory **52**, 4892–4914 (2006).
29. Knill E., Laflamme R., Zurek W.H.: Resilient quantum computation: error models and thresholds. Proc. R. Soc. Lond. A **454**, 365–384 (1998).
30. La Guardia G.G.: Construction of new families of nonbinary quantum BCH codes. Phys. Rev. A **80**, 042331 (2009).
31. La Guardia G.G.: On the construction of nonbinary quantum BCH codes. IEEE Trans. Inf. Theory **60**, 1528–1535 (2014).

32. La Guardia G.G., Palazzo R.: Constructions of new families of nonbinary CSS codes. Discret. Math. **310**, 2935–2945 (2010).
33. Luo L., Ma Z.: Fault-tolerant quantum computation with non-binary systems. Quant. Inf. Process. **18**, 188 (2019).
34. Lv J., Li R., Wang J.: Quantum codes derived from one-generator quasi-cyclic codes with Hermitean inner product. Int. J. Theor. Phys. **59**, 300–312 (2020).
35. Matsumoto R., Uyematsu T.: Constructing quantum error correcting codes for p^m state systems from classical error correcting codes. IEICE Trans. Fund. **E83**, 1878–1883 (2000).
36. Preskill J.: Reliable quantum computers. Proc. R. Soc. Lond. A **454**, 385–410 (1998).
37. Shor P.W.: Fault-tolerant quantum computation. In Proc. 37th Ann. Symp. Found. Comp. Sci., IEEE Comp. Soc. Press, pp. 56–65 (1996).
38. Shor P.W.: Scheme for reducing decoherence in quantum computer memory. Phys. Rev. A **52**, 2493–2496 (1995).
39. Song H., Li R., Liu Y., Guo G.: New quantum codes from matrix product codes over small fields. Quant. Inf. Process. **19**, 226 (2020).
40. Steane A.M.: Simple quantum error correcting codes. Phys. Rev. Lett. **77**, 793–797 (1996).
41. Steane A.M., Ibinson B.: Fault-tolerant logical gate networks for Calderbank-Shor-Steane codes. Phys. Rev. A **72**, 052335 (2005).
42. Wootters W.K., Zurek W.H.: A single quantum cannot be cloned. Nature **299**, 802–803 (1982).
43. Zhang T., Ge G.: Quantum MDS codes with large minimum distance. Des. Codes Cryptogr. **83**, 503–517 (2017).