




MDS, Hermitian almost MDS, and Gilbert–Varshamov quantum codes from generalized monomial-Cartesian codes

Beatriz Barbero-Lucas¹ · Fernando Hernando² · Helena Martín-Cruz² · Gary McGuire¹ 

Received: 30 July 2023 / Accepted: 31 January 2024 / Published online: 1 March 2024
© The Author(s) 2024

Abstract

We construct new stabilizer quantum error-correcting codes from generalized monomial-Cartesian codes. Our construction uses an explicitly defined twist vector, and we present formulas for the minimum distance and dimension. Generalized monomial-Cartesian codes arise from polynomials in m variables. When $m = 1$ our codes are MDS, and when $m = 2$ and our lower bound for the minimum distance is 3, the codes are at least Hermitian almost MDS. For an infinite family of parameters, when $m = 2$ we prove that our codes beat the Gilbert–Varshamov bound. We also present many examples of our codes that are better than any known code in the literature.

Keywords error-correction · Hermitian · MDS · Gilbert-Varshamov

1 Introduction

Certain classically intractable problems can become feasible when approached with the computational power of quantum computers. This was demonstrated through Shor’s algorithm, which solves in polynomial time the prime factorization problem and discrete logarithm problem on quantum computers [50]. Due to this fact, researchers and companies are actively engaged in constructing quantum computers with many qubits [10, 15]. Quantum computer implementations have higher error rates than classical computers, making reliability a challenge. However, despite quantum information being unclonable [18, 56], it was shown that quantum error correction techniques can

✉ Gary McGuire
gary.mcguire@ucd.ie

¹ School of Mathematics and Statistics, University College Dublin, Dublin, Ireland

² Instituto Universitario de Matemáticas y Aplicaciones de Castellón and Departamento de Matemáticas, Universitat Jaume I, Campus de Riu Sec, 12071 Castelló, Spain

be used [49, 53]. Over the last twenty-five years, error correction has proved to be one of the main obstacles to scaling up quantum computing and quantum information processing.

There is an extensive study of quantum error-correcting codes, see for example the papers [3, 4, 11, 12, 31, 33, 52] for the binary case and [5, 6, 9, 14, 21, 24, 27, 32, 35, 40, 41, 47, 51] for the general case. Many of the known quantum error-correcting codes are stabilizer codes. Let \mathbb{C} be the complex field, let q be a prime power and let n be a positive integer. A stabilizer code $Q \neq \{0\}$ is the common eigenspace of an abelian subgroup of the error group G_n generated by a nice error basis on the space \mathbb{C}^{q^n} (see [36, 37] for details). The code Q has minimum distance d whenever all errors in G_n with weight less than d can be detected, or have no effect on Q , but some errors of weight d cannot be detected. A code as above has parameters $[[n, k, d]]_q$ when it is a q^k -dimensional subspace of \mathbb{C}^{q^n} and has minimum distance d (see, for instance, [12, 35]). Stabilizer quantum error-correcting codes have been studied by many authors because they can be constructed from classical additive codes in \mathbb{F}_q^{2n} , which are self-orthogonal with respect to a trace symplectic form. In particular, stabilizer codes can be obtained from suitable Hermitian self-orthogonal classical linear codes (see [35] or [5, 9, 12] for details). We will utilize this construction.

Many constructions of classical codes start with a quotient polynomial ring of the form $\mathbb{F}_q[X_1, \dots, X_m]/I$ where I is an ideal. Affine variety codes were introduced by Fitzgerald and Lax in [23], with a general ideal I . Our codes $C_{v,\Delta,Z}$ (defined in the next section) are a type of generalized affine variety code, so we could use this name. However, since the codes we define are generalized monomial-Cartesian codes, introduced in [45], and although the definition is slightly different, we are going to call our codes $C_{v,\Delta,Z}$ *generalized monomial-Cartesian codes*.

Monomial-Cartesian codes (MCCs) are a class of evaluation codes obtained as the image of maps

$$\text{ev}_S: V_\Delta \subset \mathbb{F}_q[X_1, \dots, X_m]/I \longrightarrow \mathbb{F}_q^n, \quad \text{ev}_S(f) = (f(\beta_1), \dots, f(\beta_n)),$$

where m is a positive integer larger than 1, $S = S_1 \times \dots \times S_m = \{\beta_1, \dots, \beta_n\}$ is a Cartesian-product subset of \mathbb{F}_q^m , I is the vanishing ideal at S of $\mathbb{F}_q[X_1, \dots, X_m]$, and V_Δ is an \mathbb{F}_q -linear space generated by classes of monomials. MCCs were introduced in [45] with only algebraic tools, see also [46]. These codes have several different applications in the literature, such as quantum codes, locally recoverable codes (LRCs) with availability, polar codes and (r, δ) -LRCs [13, 26, 45].

Generalized monomial-Cartesian codes arise when changing the evaluation map ev_S to twist each coordinate of $\text{ev}_S(f)$ by nonzero elements of \mathbb{F}_q . In this article, we will use generalized MCCs, where the set S_1 is a certain fixed set, and we will use the same name for this construction, see Definition 2.3. We will use generalized monomial-Cartesian codes to construct Hermitian self-orthogonal classical linear codes and thereby construct stabilizer quantum codes. We present some evidence comparing our codes to codes in [8, 14, 16, 28, 38, 43, 55], which shows that they are very good quantum codes, and sometimes optimal.

Quantum MDS codes are those achieving the quantum singleton bound; there are many papers on this type of codes. (Some recent papers are [7, 19, 42].) The MDS

conjecture limits the length of a q -ary quantum MDS code to be at most $q^2 + 2$ [35]. Thus, another goal is to obtain longer q -ary codes with good parameters. With our construction, we achieve this.

The paper is laid out as follows: After the preliminaries in Sect. 2, we present our construction in Sect. 3. Previous works using a twist vector have proved the existence of a twist vector with the required properties, whereas a feature of our construction is that we define the twist vector explicitly, see (3) in Sect. 3. We present a general construction first (Theorem 3.4) and then a more specific construction that allows us to control the minimum distance (Theorem 3.7). In Sect. 4, we will show that our construction with $m = 1$ gives MDS codes. We also prove that when $m = 2$ and our lower bound for the minimum distance is 3 the codes are at least Hermitian almost MDS. Section 5 contains a proof that for an infinite family of parameters when $m = 2$, our codes beat the Gilbert–Varshamov bound. Finally, in Sect. 6 we present some examples with small parameters that beat the best known codes in the literature.

2 Preliminaries

In this paper, we will assume that q is odd, although in this section the definitions hold for any q . Let us denote by \mathbb{N} the set of positive integers and by \mathbb{N}_0 the set of nonnegative integers. For any two vectors $\mathbf{a} = (a_0, \dots, a_{n-1})$, $\mathbf{b} = (b_0, \dots, b_{n-1}) \in \mathbb{F}_{q^2}^n$, their Hermitian inner product is defined as:

$$\mathbf{a} \cdot_h \mathbf{b} = \sum_{i=0}^{n-1} a_i b_i^q,$$

their Euclidean inner product is defined as:

$$\mathbf{a} \cdot_e \mathbf{b} = \sum_{i=0}^{n-1} a_i b_i,$$

and their $*$ product is defined as:

$$(a_0, \dots, a_{n-1}) * (b_0, \dots, b_{n-1}) = (a_0 \cdot b_0, \dots, a_{n-1} \cdot b_{n-1}).$$

Let the symbol \perp_h (respectively, \perp_e) mean dual with respect to Hermitian (respectively, Euclidean) inner product. For a vector subspace (or code) C of $\mathbb{F}_{q^2}^n$, we let C^{\perp_h} (respectively, C^{\perp_e}) denote the orthogonal vector subspace (the dual code) with respect to the Hermitian (respectively, Euclidean) inner product. We denote by $d(C)$ the minimum distance of C . Let s be a nonnegative integer and $\mathbf{c} = (c_0, \dots, c_{n-1}) \in C$ be a codeword. We denote $\mathbf{c}^s = (c_0^s, \dots, c_{n-1}^s)$ and

$$C^s := \{\mathbf{c}^s \mid \mathbf{c} \in C\} \subseteq \mathbb{F}_{q^2}^n.$$

Let us denote by $w(c)$ the Hamming weight of c . We say that two codes are isometric if there exists a bijective mapping between them that preserves Hamming weights.

Theorem 2.1 ([1, 35]) *Let C be a linear $[n, k, d]$ error-correcting code over the field \mathbb{F}_{q^2} such that $C \subseteq C^{\perp h}$. Then, there exists an $[[n, n - 2k, \geq d^{\perp h}]]_q$ stabilizer quantum code, where $d^{\perp h}$ stands for the minimum distance of $C^{\perp h}$.*

The idea in this paper is to construct codes that satisfy the hypotheses of Theorem 2.1. In order to do so, we fix a finite field \mathbb{F}_{q^2} . Let $\mathbb{F}_{q^2}[X_1, \dots, X_m]$ be the polynomial ring in $m \geq 1$ variables over \mathbb{F}_{q^2} . For each element $e = (e_1, \dots, e_m) \in \mathbb{N}_0^m$, we write X^e for $X_1^{e_1} X_2^{e_2} \dots X_m^{e_m}$. We will refer to e as an exponent and use the lexicographic order in \mathbb{N}_0^m for the exponents. That is, given $e, e' \in \mathbb{N}_0^m$, we say $e < e'$ if and only if $e_1 < e'_1$ or there exists $j \in \{2, \dots, m\}$ such that $e_1 = e'_1, \dots, e_{j-1} = e'_{j-1}$ and $e_j < e'_j$. Any order can be used.

Let $\lambda \in \mathbb{N}$ such that $\lambda \mid q - 1$. Let A_1 be the set of roots of the polynomial $X_1^{\lambda(q+1)} - 1$, which lie in \mathbb{F}_{q^2} . We also consider arbitrary subsets $A_j \subseteq \mathbb{F}_{q^2}^*$ for $j = 2, \dots, m$ which have cardinality greater than or equal to 2. Let $a_j := \#A_j$ for $j = 1, \dots, m$, so that $a_1 = \lambda(q + 1)$. Let

$$Z := A_1 \times \dots \times A_m,$$

which has cardinality

$$n := \prod_{j=1}^m a_j.$$

Let

$$Q_j(X_j) = \prod_{\beta \in A_j} (X_j - \beta)$$

be the monic polynomial in one variable whose roots are the elements of A_j , then $\deg(Q_j) = a_j$ for $j = 1, \dots, m$. Let I be the ideal of $\mathbb{F}_{q^2}[X_1, \dots, X_m]$ generated by the polynomials $Q_1(X_1) = X_1^{\lambda(q+1)} - 1$ and $Q_j(X_j)$ for $j = 2, \dots, m$. Let

$$R := \mathbb{F}_{q^2}[X_1, \dots, X_m] / I$$

and let

$$E := \{0, 1, \dots, a_1 - 1\} \times \dots \times \{0, 1, \dots, a_m - 1\}. \tag{1}$$

Given $f \in R$, in this paper f is going to denote both the equivalence class in R and the unique polynomial representing f in $\mathbb{F}_{q^2}[X_1, \dots, X_m]$ with degree in X_j less than a_j , $1 \leq j \leq m$. Thus, one can write any $f \in R$ uniquely as

$$f(X_1, \dots, X_m) = \sum_{(e_1, \dots, e_m) \in E} f_{e_1, \dots, e_m} X_1^{e_1} \dots X_m^{e_m},$$

with $f_{e_1, \dots, e_m} \in \mathbb{F}_{q^2}$. Let us denote $\text{supp}(f) = \{(e_1, \dots, e_m) \in E \mid f_{e_1, \dots, e_m} \neq 0\}$.

Definition 2.2 Let E be as defined earlier in (1). For each nonempty subset $\Delta \subseteq E$, define $V_\Delta := \{f \in R \mid \text{supp}(f) \subseteq \Delta\}$.

Note that V_Δ is the \mathbb{F}_{q^2} -vector space consisting of the \mathbb{F}_{q^2} -span of $\{X^e \mid e \in \Delta\}$.

For any positive integer t , we denote by ζ_t a primitive t -th root of unity. Since A_j has a_j elements, we choose a bijection between A_j and the set $\{0, 1, \dots, a_j - 1\}$, and this is going to give us an ordering of A_j , $j = 2, \dots, m$. Let us represent by $\xi_{(j,s)}$ the elements of each set A_j , where the subindex $s \in \{0, 1, \dots, a_j - 1\}$ is given by the ordering. For $\alpha = (\alpha_1, \dots, \alpha_m) \in E$, we define $P_\alpha \in Z$ by

$$P_\alpha := (\zeta_{\lambda(q+1)}^{\alpha_1}, \xi_{(1,\alpha_2)}, \dots, \xi_{(m,\alpha_m)}),$$

where α_1 indicates the exponent of $\zeta_{\lambda(q+1)}$ and $\alpha_j \in \{0, 1, \dots, a_j - 1\}$ gives the position of the element $\xi_{(j,\alpha_j)} \in A_j$ in the ordering of A_j , $j = 2, \dots, m$. Every element of Z has the form P_α for some $\alpha \in E$. This sets up a bijection between Z and E .

We order the set Z using the (lexicographic) order in \mathbb{N}_0^m restricted to E . That is, given $P_\alpha, P_{\alpha'} \in Z$, then $P_\alpha < P_{\alpha'}$ if and only if $\alpha < \alpha'$. Then, we can rename the points in Z as

$$P_0 := P_{(0, \dots, 0)}, P_1 := P_{(0, \dots, 0, 1)}, \dots, P_{n-1} := P_{(a_1-1, a_2-1, \dots, a_m-1)}.$$

Let $v = (v_0, \dots, v_{n-1}) \in (\mathbb{F}_{q^2}^*)^n$, we will refer to this vector as the *twist vector*. We index the coordinates of v by the elements of E , and we order the coordinates of v in the same way as we ordered the elements of Z . That is,

$$v_0 := v_{(0, \dots, 0)}, v_1 := v_{(0, \dots, 0, 1)}, \dots, v_{n-1} := v_{(a_1-1, a_2-1, \dots, a_m-1)}.$$

The linear evaluation map in Z :

$$\text{ev}_{v,Z} : R \longrightarrow \mathbb{F}_{q^2}^n, \quad \text{ev}_{v,Z}(f) = (v_0 f(P_0), \dots, v_{n-1} f(P_{n-1}))$$

is injective by the definition of R . It provides the following class of evaluation codes.

Definition 2.3 Let V_Δ be as defined in Definition 2.2. The *generalized monomial-Cartesian code (GMCC)* $C_{v,\Delta,Z}$ is the image of V_Δ via the evaluation map $\text{ev}_{v,Z}$, that is,

$$C_{v,\Delta,Z} := \text{ev}_{v,Z}(V_\Delta) = \text{span}\{\text{ev}_{v,Z}(X^e) \mid e \in \Delta\} \subseteq \mathbb{F}_{q^2}^n.$$

Since the order of the set Z will be fixed for the rest of the article, we will use the notation $\text{ev}_v := \text{ev}_{v,Z}$ and $C_{v,\Delta} := C_{v,\Delta,Z}$.

Remark 2.4 Evaluation maps of our codes are defined on subsets of coordinate rings of certain affine varieties, but these codes can also be introduced with algebraic tools. Monomial-Cartesian codes were introduced in [45] using only algebraic tools. When the set $A_1 \subseteq \mathbb{F}_{q^2}$ is arbitrary, GMCCs extend monomial-Cartesian codes. This should be the accurate definition, but for our purposes in this paper we use this particular set A_1 , namely the $\lambda(q + 1)$ -th roots of unity.

Here is a standard fact, that the dual of a GMCC is another GMCC.

Lemma 2.5 *The dual code $(C_{v,\Delta})^{\perp h}$ is a GMCC $C_{w,\Delta}$ for some twist vector w .*

Proof Consider any two codewords $c = (c_0, \dots, c_{n-1}) \in C_{1,\Delta}$ and $b = (b_0, \dots, b_{n-1}) \in (C_{1,\Delta})^{\perp h}$. Then, the following equation holds:

$$c_0 b_0^q + \dots + c_{n-1} b_{n-1}^q = 0. \tag{2}$$

Let $v = (v_0, \dots, v_{n-1})$ be a (fixed) vector in $(\mathbb{F}_{q^2}^*)^n$ and consider $C_{v,\Delta}$. We know that $v * c = (v_0 c_0, \dots, v_{n-1} c_{n-1}) \in C_{v,\Delta}$ whenever $c = (c_0, \dots, c_{n-1}) \in C_{1,\Delta}$, because

$$C_{1,\Delta} \longrightarrow C_{v,\Delta}, \quad c \mapsto v * c$$

is a bijective mapping. We use this presentation of $C_{v,\Delta}$.

We will prove that $(C_{v,\Delta})^{\perp h} = C_{w,\Delta}$ where $w = (w_0, \dots, w_{n-1})$ is defined by $w_i := \frac{1}{v_i^q}$ for all $i = 0, \dots, n - 1$.

First we claim that for any $b \in (C_{1,\Delta})^{\perp h}$ we have that $w * b = (w_0 b_0, \dots, w_{n-1} b_{n-1}) \in (C_{v,\Delta})^{\perp h}$. To see this, choose $v * c \in C_{v,\Delta}$ and note that

$$v_0 c_0 w_0^q b_0^q + \dots + v_{n-1} c_{n-1} w_{n-1}^q b_{n-1}^q = 0$$

using the fact that $w_i^q = 1/v_i^{q^2} = 1/v_i$ for all i , and using (2). This shows that all the vectors $w * b$ are in $(C_{v,\Delta})^{\perp h}$.

Finally note that

$$(C_{1,\Delta})^{\perp h} \longrightarrow (C_{v,\Delta})^{\perp h}, \quad b \mapsto w * b$$

is a bijective mapping, which shows that $(C_{v,\Delta})^{\perp h} = C_{w,\Delta}$. □

The length and the dimension of a GMCC are n and $\#\Delta$, respectively. A bound for the minimum distance is provided in Corollary 2.8.

Lemma 2.6 *The GMCCs $C_{1,\Delta}$ and $C_{v,\Delta}$ are isometric.*

Proof For any codeword $c = (c_0, \dots, c_{n-1}) \in C_{1,\Delta}$, its twisted analogue codeword $v * c = (v_0 c_0, \dots, v_{n-1} c_{n-1}) \in C_{v,\Delta}$ under the bijective mapping $C_{1,\Delta} \rightarrow C_{v,\Delta}$, $c \mapsto v * c$ has the same Hamming weight, this is because $v_i \neq 0$ for all $i = 1, \dots, n$. □

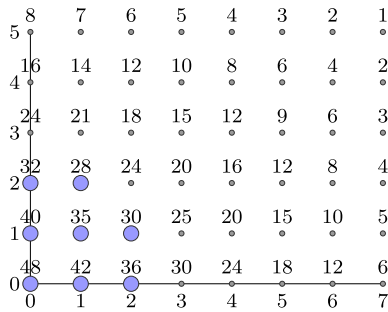


Fig. 1 In the case $m = 2$, we can use a grid to represent the set E so that an exponent $e = (e_1, e_2) \in E$ corresponds to the point with coordinates (e_1, e_2) in the grid and that point is labelled with the integer $D(e)$. Exponents in the set $\Delta \subseteq E$ are coloured in blue. This example shows the grid representation of E , where $a_1 = 8, a_2 = 6$, and $\Delta = (\{0, 1, 2\} \times \{0, 1\}) \cup \{(0, 2), (1, 2)\}$. In this example, the lower bound for the minimum distance of the code $C_{v,\Delta}$ for any $v \in (\mathbb{F}_q^*)^n$ is $d_0(C_{v,\Delta}) = \min\{D(e) \mid e \in \Delta\} = 28$ by Corollary 2.8

Affine variety codes admit a bound on the minimum distance, known as the footprint bound [29]. Monomial-Cartesian codes $C_{1,\Delta}$ in the sense of our Definition 2.3 (the evaluation map is defined over the coordinate ring of some affine variety) are affine variety codes. This fact and Lemma 2.6 prove the next lemma, stating that this bound is also valid for GMCCs. For every exponent $e \in E$, we define

$$D(e) := \prod_{j=1}^m (a_j - e_j).$$

Lemma 2.7 *Let $C_{v,\Delta}$ be a GMCC and let $c = \text{ev}_v(f) \in C_{v,\Delta}$ be a codeword, $f \in R$. Fix a monomial ordering on $(\mathbb{N}_0)^m$ and let X^e be the leading monomial of f . Then, $w(c) \geq D(e)$.*

Corollary 2.8 *Let $C_{v,\Delta}$ be a GMCC and let d be its minimum distance. Define $d_0 = d_0(C_{v,\Delta}) := \min\{D(e) \mid e \in \Delta\}$. Then, $d \geq d_0$.*

Remark 2.9 Affine variety codes were introduced in [23] for any ideal I . A classical result coming from the theory of Gröbner basis [17] implies that $d \geq d_0$, where d stands for the minimum distance of an affine variety code and d_0 is the cited footprint bound [29]. Independently, inspired by the algebraic geometric codes [34] the so-called Feng–Rao bound for the minimum distance of the dual code is derived [20]. It is known that every linear code is an algebraic geometric code. A similar bound (Andersen–Geil) was also given for an algebraic geometric code [2]. It turns out that for monomial-Cartesian codes the footprint bound applied to the dual code and the Feng–Rao bound coincide [25]. Although the footprint bound is more natural for the primal code, and the Feng–Rao bound is more natural for the dual code, we will always refer to them as d_0 .

Lemma 2.10 *Let $C_{v,\Delta}$ be a GMCC. Then, $(C_{v,\Delta})^{\perp h}$ and $(C_{v,\Delta})^{\perp e}$ are isometric.*

Proof It is straightforward because $(C_{v,\Delta})^{\perp h} = ((C_{v,\Delta})^{\perp e})^q$. □

Lemma 2.11 *Let $C_{v,\Delta}$ be a GMCC. Then $(C_{1,\Delta})^{\perp h}$ and $(C_{v,\Delta})^{\perp h}$ are isometric.*

Proof It follows from the fact that the family of GMCCs is closed under duality by Lemma 2.5 and by Lemma 2.6. □

Corollary 2.12 *Let $C_{v,\Delta}$ be a GMCC. Then $d((C_{v,\Delta})^{\perp h}) = d((C_{1,\Delta})^{\perp e})$.*

Proof This is because $(C_{v,\Delta})^{\perp h}$ and $(C_{1,\Delta})^{\perp h}$ are isometric (by Lemma 2.11) and also $(C_{1,\Delta})^{\perp h}$ is isometric to $(C_{1,\Delta})^{\perp e}$ (by Lemma 2.10). □

3 Stabilizer quantum codes from generalized monomial-Cartesian codes

In the present section, we construct stabilizer quantum codes by applying Theorem 2.1 to GMCCs (Definition 2.3) with a specific twist vector. Recall from Sect. 2 that q is an odd prime power, ζ_{q^2-1} denotes a primitive $q^2 - 1$ -th root of unity, $\lambda \in \mathbb{N}$ is such that $\lambda \mid q - 1$, $a_1 = \lambda(q + 1)$, $2 \leq a_j \leq q^2 - 1$ for all $j = 2, \dots, m$, and $n = a_1 a_2 \cdots a_m$. We are going to choose the twist vector defined explicitly as follows:

$$v = \underbrace{(\zeta_{q^2-1}^{\frac{q-1}{2}}, \dots, \zeta_{q^2-1}^{\frac{q-1}{2}})}_{\frac{n}{q+1}}, \underbrace{1, \dots, 1}_{\frac{n}{q+1}}, \underbrace{(\zeta_{q^2-1}^{\frac{q-1}{2}}, \dots, \zeta_{q^2-1}^{\frac{q-1}{2}})}_{\frac{n}{q+1}}, \dots, \underbrace{1, \dots, 1}_{\frac{n}{q+1}} \in (\mathbb{F}_q^*)^n. \tag{3}$$

Because

$$\left(\zeta_{q^2-1}^{\frac{q-1}{2}} \right)^{q+1} = \zeta_{q^2-1}^{\frac{(q+1)(q-1)}{2}} = \zeta_{q^2-1}^{\frac{q^2-1}{2}} = -1$$

it follows that

$$v^{q+1} = \underbrace{(-1, \dots, -1)}_{\frac{n}{q+1}}, \underbrace{1, \dots, 1}_{\frac{n}{q+1}}, \underbrace{-1, \dots, -1}_{\frac{n}{q+1}}, \dots, \underbrace{1, \dots, 1}_{\frac{n}{q+1}}.$$

Observe that there are $q + 1$ blocks of -1 's or 1 's. Recall that the coordinates v_α of v are labelled and ordered in the same way as the points $P_\alpha \in Z$. This twist vector works as follows. For each $\alpha \in E$,

$$v_\alpha^{q+1} = \begin{cases} -1 & \text{if } 0 \leq (\alpha_1 \bmod 2\lambda) \leq \lambda - 1, \\ 1 & \text{if } \lambda \leq (\alpha_1 \bmod 2\lambda) \leq 2\lambda - 1. \end{cases} \tag{4}$$

Notice that v_α only depends on α_1 . The reason why we choose this specific twist vector is going to become clear in Proposition 3.1.

3.1 Self-orthogonality conditions

First we present some conditions for the evaluation vectors of monomials in R to be orthogonal for the Hermitian inner product, when our twist vector is used.

Proposition 3.1 *Keep the same notations as before. Let q be an odd prime power and consider the twist vector \mathbf{v} defined in (3). Let $\mathbf{e} = (e_1, \dots, e_m)$, $\mathbf{e}' = (e'_1, \dots, e'_m) \in E$ be exponents of two monomials $X^{\mathbf{e}}, X^{\mathbf{e}'} \in R$. Then, the evaluation vectors under the map $ev_{\mathbf{v}}$ of these monomials are orthogonal for the Hermitian inner product if one of the following conditions hold:*

- $e_1 \equiv e'_1 \pmod{q + 1}$, or
- $e_1 \not\equiv e'_1 \pmod{\frac{q+1}{2}}$.

Proof In order to compute some conditions under which two evaluations of monomials of the quotient ring R are orthogonal for the Hermitian inner product, we have to see when the following sum vanishes:

$$ev_{\mathbf{v}}(X^{\mathbf{e}}) \cdot_h ev_{\mathbf{v}}(X^{\mathbf{e}'}) = \sum_{\alpha \in E} v_{\alpha}^{q+1} \zeta_{\lambda(q+1)}^{\alpha_1(e_1+qe'_1)} \xi_{(2,\alpha_2)}^{(e_2+qe'_2)} \dots \xi_{(m,\alpha_m)}^{(e_m+qe'_m)}.$$

Since v_{α} only depends on α_1 , we can denote by $v_{\alpha_1} := v_{(\alpha_1, \dots, \alpha_m)} = v_{\alpha}$ and reorder the above sum in the following way:

$$ev_{\mathbf{v}}(X^{\mathbf{e}}) \cdot_h ev_{\mathbf{v}}(X^{\mathbf{e}'}) = \left(\sum_{\alpha_1=0}^{\lambda(q+1)-1} v_{\alpha_1}^{q+1} \zeta_{\lambda(q+1)}^{\alpha_1(e_1+qe'_1)} \right) \left(\sum_{\alpha_2=0}^{a_2-1} \xi_{(2,\alpha_2)}^{(e_2+qe'_2)} \right) \dots \left(\sum_{\alpha_m=0}^{a_m-1} \xi_{(m,\alpha_m)}^{(e_m+qe'_m)} \right).$$

We can do that because all the coordinates v_{α} in \mathbf{v} that have the same α_1 have the same value. Now we study when the first factor equals 0, and we will ignore the other factors, since the first one gives enough information for the proof. Consider then

$$\sum_{\alpha_1=0}^{\lambda(q+1)-1} v_{\alpha_1}^{q+1} \zeta_{\lambda(q+1)}^{\alpha_1(e_1+qe'_1)}, \tag{5}$$

which is a sum over $\alpha_1 \in \{0, 1, \dots, \lambda(q + 1) - 1\}$. We write each α_1 in the form $k\lambda + r$ where $0 \leq k \leq q$ and $0 \leq r < \lambda$. Using this to break (5) into λ blocks of size $q + 1$, using the fact that $\zeta_{q+1} := \zeta_{\lambda(q+1)}^{\lambda}$ is a primitive $q + 1$ -th root of unity and using the structure of the twist vector \mathbf{v} , we can write (5) as

$$\sum_{\alpha_1=0}^{\lambda(q+1)-1} v_{\alpha_1}^{q+1} \zeta_{\lambda(q+1)}^{\alpha_1(e_1+qe'_1)} = \sum_{\substack{0 \leq k \leq q \\ 0 \leq r < \lambda}} v_{k\lambda+r}^{q+1} \zeta_{\lambda(q+1)}^{(k\lambda+r)(e_1+qe'_1)}$$

$$\begin{aligned}
 &= \sum_{k=0}^q v_{k\lambda}^{q+1} \zeta_{q+1}^{k(e_1+qe'_1)} \\
 &\quad + \zeta_{\lambda(q+1)}^{e_1+qe'_1} \sum_{k=0}^q v_{k\lambda+1}^{q+1} \zeta_{q+1}^{k(e_1+qe'_1)} \\
 &\quad + \dots + \zeta_{\lambda(q+1)}^{(\lambda-1)(e_1+qe'_1)} \sum_{k=0}^q v_{k\lambda+\lambda-1}^{q+1} \zeta_{q+1}^{k(e_1+qe'_1)} \\
 &= \left(1 + \zeta_{\lambda(q+1)}^{(e_1+qe'_1)} + \dots + \zeta_{\lambda(q+1)}^{(\lambda-1)(e_1+qe'_1)} \right) \\
 &\quad \left(\sum_{k=0}^q v_{k\lambda}^{q+1} \zeta_{q+1}^{k(e_1+qe'_1)} \right).
 \end{aligned}$$

Notice that we can do that because from (4) and the fact that $1 \leq \lambda \leq q - 1$ we have that $v_{k\lambda}^{q+1} = v_{k\lambda+1}^{q+1} = \dots = v_{k\lambda+\lambda-1}^{q+1}$ for all $0 \leq k \leq q$. Now using again (4) and the fact that $\zeta_{\frac{q+1}{2}} := \zeta_{q+1}^2$ is a primitive $\frac{q+1}{2}$ -th root of unity, we rewrite the last sum in the following way:

$$\begin{aligned}
 \sum_{k=0}^q v_{k\lambda}^{q+1} \zeta_{q+1}^{k(e_1+qe'_1)} &= \sum_{k=0}^{\frac{q-1}{2}} v_{2k\lambda}^{q+1} \zeta_{q+1}^{2k(e_1+qe'_1)} + \sum_{k=0}^{\frac{q-1}{2}} v_{2k\lambda+1}^{q+1} \zeta_{q+1}^{(2k+1)(e_1+qe'_1)} \\
 &= \sum_{k=0}^{\frac{q-1}{2}} v_{2k\lambda}^{q+1} \zeta_{q+1}^{2k(e_1+qe'_1)} - \zeta_{q+1}^{e_1+qe'_1} \sum_{k=0}^{\frac{q-1}{2}} v_{2k\lambda}^{q+1} \zeta_{q+1}^{2k(e_1+qe'_1)} \\
 &= \zeta_{q+1}^{e_1+qe'_1} \left(\sum_{k=0}^{\frac{q-1}{2}} \zeta_{\frac{q+1}{2}}^{k(e_1+qe'_1)} \right) - \left(\sum_{k=0}^{\frac{q-1}{2}} \zeta_{\frac{q+1}{2}}^{k(e_1+qe'_1)} \right) \\
 &= (\zeta_{q+1}^{e_1+qe'_1} - 1) \left(\sum_{k=0}^{\frac{q-1}{2}} \zeta_{\frac{q+1}{2}}^{k(e_1+qe'_1)} \right).
 \end{aligned}$$

Thus, we have shown that we can write (5) as

$$\sum_{\alpha_1=0}^{\lambda(q+1)-1} v_{\alpha_1}^{q+1} \zeta_{\lambda(q+1)}^{\alpha_1(e_1+qe'_1)} = P(\zeta_{\lambda(q+1)}^{e_1+qe'_1}) \left(\zeta_{q+1}^{e_1+qe'_1} - 1 \right) \left(\sum_{k=0}^{\frac{q-1}{2}} \zeta_{\frac{q+1}{2}}^{k(e_1+qe'_1)} \right),$$

where $P(x) = 1 + x + x^2 + \dots + x^{\lambda-1}$. The above product equals 0 if and only if one of the following conditions holds:

- $\zeta_{q+1}^{e_1+qe'_1} - 1 = 0 \iff e_1 + qe'_1 \equiv 0 \pmod{q + 1}$. That is, $e_1 \equiv e'_1 \pmod{q + 1}$; or

- $\left(\sum_{k=0}^{\frac{q-1}{2}} \zeta_{\frac{q+1}{2}}^{k(e_1+qe'_1)} \right) = 0 \iff e_1 + qe'_1 \not\equiv 0 \pmod{\frac{q+1}{2}}$. Since $q \equiv -1 \pmod{\frac{q+1}{2}}$, this is equivalent to $e_1 \not\equiv e'_1 \pmod{\frac{q+1}{2}}$; or
- $P\left(\zeta_{\lambda(q+1)}^{(e_1+qe'_1)}\right) = 0$. This is true if and only if $\zeta_{\lambda(q+1)}^{(e_1+qe'_1)}$ is a λ -th root of unity other than 1. That is equivalent to $e_1 + qe'_1 \equiv 0 \pmod{q+1}$ and $e_1 + qe'_1 \not\equiv 0 \pmod{\lambda(q+1)}$, which is a particular case of the first condition.

Therefore, if either of the first two conditions hold, the sum (5) equals 0 and that implies that $ev_v(X^e)$ and $ev_v(X^{e'})$ are orthogonal for the Hermitian inner product. \square

Remark 3.2 Consider the case when the twist vector is $\mathbf{1}$, $\lambda = 1$ and A_j is the set of $q + 1$ -th roots of unity, that is the solutions to $X_j^{q+1} - 1 = 0$, for every $j = 1, \dots, m$. Then for any $\Delta \subseteq E$ the GMCC $C_{\mathbf{1}, \Delta}$ is an Affine Variety Code (AVC) and it is not self-orthogonal (for the Hermitian inner product). This is because when we compute the Hermitian inner product of the evaluations of any monomial $X^e = X^{(e_1, \dots, e_m)}$ with itself, one obtains that

$$\begin{aligned} ev_{\mathbf{1}}(X^e) \cdot_h ev_{\mathbf{1}}(X^e) &= \sum_{\alpha \in E} \zeta_{q+1}^{\alpha_1 e_1(1+q)} \zeta_{q+1}^{\alpha_2 e_2(1+q)} \dots \zeta_{q+1}^{\alpha_m e_m(1+q)} \\ &= \left(\sum_{\alpha_1=0}^q \zeta_{q+1}^{\alpha_1 e_1(1+q)} \right) \left(\sum_{\alpha_2=0}^q \zeta_{q+1}^{\alpha_2 e_2(1+q)} \right) \dots \left(\sum_{\alpha_m=0}^q \zeta_{q+1}^{\alpha_m e_m(1+q)} \right) \end{aligned}$$

and every factor above is

$$\sum_{k=0}^q \zeta_{q+1}^{ke_1(1+q)} = q + 1 \neq 0.$$

Thus, the evaluation of a monomial is not orthogonal to itself, and these codes are not self-orthogonal. However, we are able to provide a twist vector \mathbf{v} (3) to construct a self-orthogonal GMCC $C_{\mathbf{v}, \Delta}$ which is isometric to the non-self-orthogonal AVC $C_{\mathbf{1}, \Delta}$. The problem of not getting evaluations of monomials to be self-orthogonal can happen also with other twist vectors, that is why one has to choose the twist vector carefully.

3.2 Our general construction

Before stating the theorem that is the general construction of this paper, recall the definition of the set E in the previous section. We define a subset in E which will be useful in the following.

Definition 3.3 Let $E_0 := \left\{ e = (e_1, \dots, e_m) \in E \mid 0 \leq e_1 \leq \frac{q-1}{2} \right\} \subseteq E$.

The next theorem shows that the set E_0 introduced in Definition 3.3 is used as a reference to construct Hermitian self-orthogonal GMCCs.

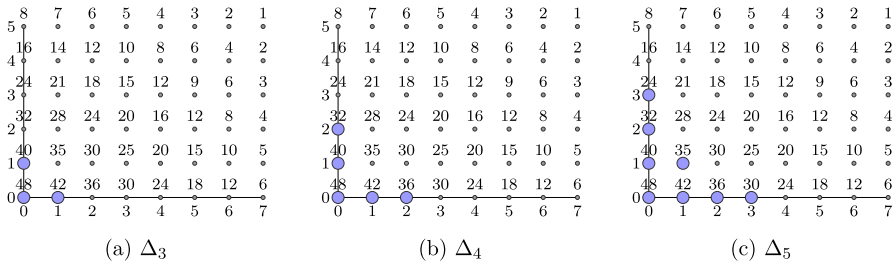


Fig. 2 Sets Δ_3 , Δ_4 and Δ_5 , where $m = 2$, $a_1 = 8$ and $a_2 = 6$. We use the same conventions as in Fig. 1

Theorem 3.4 *Let q be an odd prime power and let $m \geq 1$, $\lambda \mid q - 1$, $a_1 := \lambda(q + 1)$ and $2 \leq a_j \leq q^2 - 1$, $j = 2, \dots, m$ be positive integers. Let $n := a_1 \cdots a_m$. Consider the twist vector \mathbf{v} defined in (3) and the set $E_0 \subseteq E$ introduced in Definition 3.3. Let Δ be a subset of E_0 . Then,*

$$C_{\mathbf{v}, \Delta} \subseteq (C_{\mathbf{v}, \Delta})^{\perp h}.$$

Therefore, there exists a stabilizer quantum code with parameters

$$[[n, n - 2\#\Delta, \geq d]]_q$$

where $d = d((C_{\mathbf{1}, \Delta})^{\perp e})$.

Proof Since for all $(e_1, \dots, e_m) \in \Delta$ we have $e_1 \leq \frac{q-1}{2}$, the self-orthogonality follows from Proposition 3.1. The existence and parameters of the stabilizer quantum code follow from Theorem 2.1. Notice that $d = d((C_{\mathbf{v}, \Delta})^{\perp h})$, but from Corollary 2.12 we can conclude that $d = d((C_{\mathbf{1}, \Delta})^{\perp e})$. \square

Notice that in the above theorem we do not give an explicit bound for the minimum distance, but it can be computed using Corollary 2.8 in every particular case.

3.3 Our specific construction

Now we are going to provide a strategy [30] to choose a set $\Delta \subseteq E_0$ so that we can control the minimum distance $d((C_{\mathbf{1}, \Delta})^{\perp e})$ and it maximizes the dimension of the resulting stabilizer quantum code. To that purpose, we need the following

Definition 3.5 Let $2 \leq t \leq \frac{q+3}{2}$ be a positive integer. Define

$$\Delta_t := \left\{ \mathbf{e} = (e_1, \dots, e_m) \in E \mid \prod_{j=1}^m (e_j + 1) < t \right\} \subseteq E.$$

Some instances of the above set are represented in Fig. 2.

Lemma 3.6 *Let $\Delta_t \subseteq E$ be the set introduced in Definition 3.5. Then,*

$$d\left((C_{\mathbf{1}, \Delta_t})^{\perp_e}\right) \geq t.$$

Proof Using the notations in [25, Section 3], the authors define a code $C(L_2)$, where

$$L_2 = \{X_1^{i_1} \cdots X_m^{i_m} \in \Delta(s_1, \dots, s_m) \mid D^\perp(X_1^{i_1} \cdots X_m^{i_m}) < \delta^\perp\}.$$

By choosing their (s_1, \dots, s_m) and δ^\perp equal to our (a_1, \dots, a_m) and t , respectively, then we have that

$$L_2 = \{X^e \mid e \in \Delta_t\},$$

so $C(L_2) = C_{\mathbf{1}, \Delta_t}$, see [25, Definition 15]. The statement follows from their equation (8) in Section 3. □

Theorem 3.7 *Let q be an odd prime power and let $m \geq 1$, $\lambda \mid q - 1$, $a_1 := \lambda(q + 1)$ and $2 \leq a_j \leq q^2 - 1$, $j = 2, \dots, m$ be positive integers. Let $n := a_1 \cdots a_m$. Consider the twist vector \mathbf{v} defined in (3), a positive integer*

$$2 \leq t \leq \frac{q + 3}{2}$$

and the set $\Delta_t \subseteq E$ introduced in Definition 3.5. Then, the following inclusion holds

$$C_{\mathbf{v}, \Delta_t} \subseteq (C_{\mathbf{v}, \Delta_t})^{\perp_h}.$$

Therefore, there exists a stabilizer quantum code with parameters

$$[[n, n - 2\#\Delta_t, \geq t]]_q.$$

Proof Let $e \in \Delta_t$. From $\prod_{j=1}^m (e_j + 1) < t$, we have that $e_1 < t - 1$. Since $t \leq \frac{q+3}{2}$, then $e_1 < t - 1 \leq \frac{q+1}{2}$ and therefore $\Delta_t \subseteq E_0$. So, from Theorem 3.4 we have that $C_{\mathbf{v}, \Delta_t} \subseteq (C_{\mathbf{v}, \Delta_t})^{\perp_h}$.

The existence and parameters of the stabilizer quantum code follows from Theorem 2.1. Notice that from Corollary 2.12 and Lemma 3.6, we have $d((C_{\mathbf{v}, \Delta_t})^{\perp_h}) = d((C_{\mathbf{1}, \Delta_t})^{\perp_e}) \geq t$. □

3.4 The dimension

We state a recursive formula for the dimension of the quantum code, which is shown in [30].

Let $a, b \in \mathbb{N}$. Consider the case when $a_j = b$ for all $j = 1, \dots, m$. We define

$$V_b(m, a) := \# \left\{ (l_1, \dots, l_m) \mid l_j \in \mathbb{N}, 1 \leq l_j \leq b, j = 1, \dots, m, \prod_{j=1}^m l_j \leq a \right\}.$$

In [30], they give the following recursive formula:

$$V_b(m, a) = \sum_{s=1}^b V \left(m - 1, \left\lfloor \frac{a}{s} \right\rfloor \right),$$

where $V_b(1, a) = \min\{a, b\}$.

Observe that $\#\Delta_t = V_{\lambda(q+1)}(m, t-1)$, where all of a_1, \dots, a_m are equal to $\lambda(q+1)$. Therefore, we can use the recursive formula described above to compute $\#\Delta_t$, and hence the dimension of the quantum code in Theorem 3.7. For example, when $m = 2$

$$\#\Delta_t = V_{\lambda(q+1)}(2, t-1) = t-1 + \left\lfloor \frac{t-1}{2} \right\rfloor + \left\lfloor \frac{t-1}{3} \right\rfloor + \dots + \left\lfloor \frac{t-1}{t-2} \right\rfloor + \left\lfloor \frac{t-1}{t-1} \right\rfloor, \tag{6}$$

and when $m = 3$

$$\#\Delta_t = V_{\lambda(q+1)}(3, t-1) = \sum_{\alpha=1}^{t-1} \sum_{\beta=1}^{\left\lfloor \frac{t-1}{\alpha} \right\rfloor} \left\lfloor \frac{t-1}{\alpha\beta} \right\rfloor.$$

4 We obtain MDS and Hermitian almost MDS quantum codes

In this section, we prove that we can obtain quantum codes that are close to the singleton bound. Let us recall first the quantum singleton bound.

Lemma 4.1 (Quantum Singleton bound [48]) *If a stabilizer quantum code with parameters $[[n, k, d]]_q$ exists, then $n \geq k + 2d - 2$.*

Codes attaining equality are called quantum MDS codes.

4.1 MDS

Theorem 4.2 *The stabilizer quantum codes obtained from Theorem 3.7 with $m = 1$ are quantum MDS codes.*

Proof For any given bound for the minimum distance $t \in \{2, \dots, \frac{q+3}{2}\}$, we have $\Delta_t = \{0, 1, 2, \dots, t-2\}$. The parameters of the stabilizer quantum code constructed from Theorem 3.7 are:

$$[[n, k, d]]_q = [[\lambda(q+1), \lambda(q+1) - 2(t-1), \geq t]]_q.$$

It is easily verified that the above parameters provide a quantum MDS code, because $k + 2d \geq \lambda(q + 1) - 2(t - 1) + 2t = \lambda(q + 1) + 2 = n + 2$ and the quantum singleton bound gives an equality. \square

Some sample parameters are given in Tables 3, 4, 5, 6, 7. For example, we obtain quantum MDS codes with parameters $[[12, 8, 3]]_5$ in Table 4, $[[8, 4, 3]]_7$ and $[[16, 8, 5]]_7$ in Table 5 and $[[20, 12, 5]]_9$ in Table 6. We do not claim that these examples are new.

The article [54] recently appeared on the arxiv and has a construction of MDS codes with lengths of the form $r(q^2 - 1)/h$ where h is an even divisor of $q - 1$ and $r \leq h/2$ (their Theorems 3, 4 and 5). This article does not provide an explicit twist vector (they prove the existence of it). Our construction has an explicit twist vector and (in the $m = 1$ case) gives codes with the same parameters.

4.2 Hermitian almost MDS

The quantum singleton defect of a parameter set n, k, d is defined to be $n - (k + 2d - 2)$. MDS codes have quantum singleton defect 0, by definition. Codes with quantum Singleton defect 1 are called quantum almost MDS (QAMDS) codes. However, from the statement of Theorem 2.1, one can see that the quantum singleton defect of any code constructed using Theorem 2.1 must be even, and thus, a quantum singleton defect of 1 cannot be achieved. The smallest nonzero singleton defect of a code constructed using Theorem 2.1 is therefore 2. This motivates the following definition.

Definition 4.3 A quantum code constructed from Theorem 2.1 with parameters $[[n, k, d]]_q$ such that $n = k + 2d$ is called a *quantum Hermitian almost MDS (QHAMDS)* code.

In Theorem 4.2, we showed that we can construct quantum MDS codes. Recall that the quantum MDS conjecture [35] states that $n \leq q^2 + 1$ for a quantum MDS code with parameters $[[n, k, d]]_q$ and q odd. Now we are going to show that we can also construct quantum codes with $n > q^2 + 1$ that are at least QHAMDS. That is, they are either QHAMDS or MDS. If the quantum MDS conjecture is true, they cannot be MDS, and therefore they would have the best possible parameters.

Theorem 4.4 *The stabilizer quantum codes obtained from Theorem 3.7 with $m = 2$, $n > q^2 + 1$ and $t = 3$ are at least QHAMDS.*

Proof Let $m = 2$, $t = 3$ and λ and a_2 be as defined in Theorem 3.7 such that $n > q^2 + 1$. We have $\Delta_3 = \{(0, 0), (1, 0), (0, 1)\}$ (see Fig. 2). The parameters of the stabilizer quantum code constructed from Theorem 3.7 are

$$[[n, k, d]]_q = [[\lambda(q + 1)a_2, \lambda(q + 1)a_2 - 6, \geq 3]]_q.$$

It is easily verified that the above parameters provide a code which is at least QHAMDS. This is because $k + 2d \geq \lambda(q + 1)a_2 - 6 + 2 \cdot 3 = \lambda(q + 1)a_2 = n$. \square

Some examples will be given in Tables 3 to 7. In [16], the authors study ternary quantum codes of minimum distance three. In that paper (their Theorem 4.4), quantum codes with parameters $[[n, n - 7, 3]]_3$ are shown for certain lengths n . For those lengths which are a multiple of 4 and less than 64, we can improve the dimension by 1, using the codes in Theorem 4.4. See also Table 3.

5 When $m = 2$ we can beat Gilbert–Varshamov bound

In this section, we include a proof that an infinite family of codes obtained from our constructions will beat the quantum Gilbert–Varshamov bound when $m = 2$. We remark that the codes with $m > 2$ can also beat the Gilbert–Varshamov bound, some examples when $m = 3$ are presented in Tables 3, 4 and 6.

Let us recall the quantum Gilbert–Varshamov bound whose proof can be found in [22]:

Theorem 5.1 (Quantum Gilbert–Varshamov Bound) *Suppose that $n > k \geq 2, d \geq 2$, and $n \equiv k \pmod 2$. If*

$$\frac{q^{n-k+2} - 1}{q^2 - 1} \geq \sum_{i=1}^{d-1} (q^2 - 1)^{i-1} \binom{n}{i} \tag{7}$$

then there exists a pure stabilizer quantum code with parameters $[[n, k, d]]_q$.

We say that a parameter set n, k, d, q beats the QGV bound if the inequality (7) is not satisfied.

In the $m = 2$ case, we have the following statement, using the codes constructed in this paper. In this statement, we are using the formula (6).

Theorem 5.2 *Given an odd prime power q , and given d in the range $5 \leq d \leq (q+3)/2$, let n be in the interval*

$$\left((d - 1)^{d-1} \frac{q^2}{(q^2 - 1)^{d-1}} q^{2(d-1)(0.7+\ln(d-1))} \right)^{\frac{1}{d-1}} \leq n \leq (q^2 - 1)^2$$

and have the form $\lambda(q + 1)a_2$ where $\lambda \mid (q - 1)$ and $2 \leq a_2 \leq q^2 - 1$. Then, there exists a quantum code with parameters

$$[[n, n - 2 \sum_{j=1}^{d-1} \left\lfloor \frac{d-1}{j} \right\rfloor, \geq d]]_q$$

and this code beats the quantum Gilbert–Varshamov bound.

Proof. We use the codes whose existence is proved in Theorem 3.7 in the case $m = 2$. The upper bounds $d \leq (q + 3)/2$ and $n \leq (q^2 - 1)^2$ follow from the construction in Theorem 3.7.

Let

$$A = \sum_{i=1}^{d-1} (q^2 - 1)^{i-1} \binom{n}{i}$$

and let

$$D = \frac{q^{n-k+2} - 1}{q^2 - 1}$$

where $k = n - 2 \sum_{j=1}^{d-1} \lfloor \frac{d-1}{j} \rfloor$ (this dimension formula comes from (6) which uses our construction with $m = 2$). We wish to prove that $A > D$ under the stated hypotheses. To prove this, we are going to let

$$B = \frac{1}{(d-1)^{d-1}} n^{d-1} (q^2 - 1)^{d-2}$$

and let

$$C = \left(\frac{q^2}{q^2 - 1} \right) q^{2(d-1)(0.7+\ln(d-1))}$$

and we will prove three things: that $A > B$, that $B \geq C$, and that $C > D$. This will complete the proof that $A > D$.

To show that $A > B$, we will use the estimate for binomial coefficients $\binom{n}{k} > \left(\frac{n}{k}\right)^k$. Then

$$\begin{aligned} A &= \sum_{i=1}^{d-1} (q^2 - 1)^{i-1} \binom{n}{i} > \binom{n}{d-1} (q^2 - 1)^{d-2} \\ &> \left(\frac{n}{d-1}\right)^{d-1} (q^2 - 1)^{d-2} \\ &= \frac{1}{(d-1)^{d-1}} n^{d-1} (q^2 - 1)^{d-2} = B. \end{aligned}$$

To prove that $B \geq C$, rearranging the hypothesis

$$\left((d-1)^{d-1} \frac{q^2}{(q^2 - 1)^{d-1}} q^{2(d-1)(0.7+\ln(d-1))} \right)^{\frac{1}{d-1}} \leq n$$

yields precisely that $B \geq C$.

Table 1 Some instances of the range of lengths of codes (from Theorem 5.2 only) that beat the quantum Gilbert–Varshamov bound

d	$\frac{q}{7}$	9	11	13	17
5	742-2304	1438-6400	2450-14400	3818-28224	7800-82944
6	$d > \frac{q+3}{2}$	3848-6400	7022-14400	11600-28224	26006-82944
7	$d > \frac{q+3}{2}$	$d > \frac{q+3}{2}$	None	None	72590-82944

To prove that $C > D$, we will use the fact that if $r \geq 4$ then $H_r < 0.7 + \ln r$ where H_r is the r -th harmonic number defined by $H_r = \sum_{j=1}^r \frac{1}{j}$. Then,

$$\begin{aligned} \sum_{j=1}^{d-1} \left\lfloor \frac{d-1}{j} \right\rfloor &< \sum_{j=1}^{d-1} \frac{d-1}{j} \\ &= (d-1)H_{d-1} \\ &< (d-1)(0.7 + \ln(d-1)) \quad \text{since } d-1 \geq 4. \end{aligned}$$

It follows that

$$\begin{aligned} D &= \frac{q^{n-k+2} - 1}{q^2 - 1} \\ &< \frac{q^{n-k+2}}{q^2 - 1} \\ &= \left(\frac{q^2}{q^2 - 1} \right) q^{n-k} \\ &= \left(\frac{q^2}{q^2 - 1} \right) q^{2 \sum_{j=1}^{d-1} \left\lfloor \frac{d-1}{j} \right\rfloor} \\ &< \left(\frac{q^2}{q^2 - 1} \right) q^{2(d-1)(0.7 + \ln(d-1))} = C. \quad \square \end{aligned}$$

In this theorem, we assumed that $d \geq 5$ because of the constant 0.7, which is a choice. The cases $d = 3$ and $d = 4$ can be proved separately. They could be included in the proof above but the constant 0.7 would have to be larger. Similarly, we could have stated the theorem for $d \geq 6$ and the constant would be smaller, it would be 0.68. Then, the $d = 5$ case would need to be handled separately. As d gets larger, the constant gets smaller and approaches the Euler–Mascheroni constant.

We show Table 1 where for each q between 7 and 17 and $d = 5, 6, 7$ we give the range of values of n for which the quantum Gilbert–Varshamov bound is beaten, as given by Theorem 5.2.

A separate special analysis for each d , or using better estimates in the proof, or using a computer, will give a better range of values for n than the statement of Theorem 5.2.

For example, when $q = 7$ and $d = 5$, computer calculations show that the Gilbert–Varshamov bound is beaten by our codes as soon as $n > 295$, whereas the proof of Theorem 5.2 gives $n \geq 742$. As another example, when $q = 11$ and $d = 7$, the range of values of n as given by the statement of Theorem 5.2 is empty (in the table we wrote ‘none’). However, there are in fact values of n that beat the Gilbert–Varshamov bound. We state one example $[[7200, 7172, 7]]_{11}$ in Table 7.

We also remark that Theorem 5.2 is for $m = 2$. A similar result will hold for $m > 2$.

5.1 $d = 3$

In the previous theorem, we assumed that $d \geq 5$ to obtain a slightly stronger statement. We will treat the case that $d = 3$ (and $m = 2$) separately, and we will complete the analysis in detail now. We omit the $d = 4$ case, which is similar.

Suppose $d = 3$. By the formula (6) we have that Δ_3 has 3 elements, see also Fig. 2. The two sides of the Gilbert–Varshamov bound become

$$\frac{q^{n-k+2} - 1}{q^2 - 1} = \frac{q^8 - 1}{q^2 - 1} = q^6 + q^4 + q^2 + 1$$

and

$$\sum_{i=1}^{d-1} (q^2 - 1)^{i-1} \binom{n}{i} = n + \binom{n}{2} (q^2 - 1).$$

To beat the G–V bound, we obtain a condition which is a quadratic polynomial in n , namely we require that

$$n + \binom{n}{2} (q^2 - 1) - (q^6 + q^4 + q^2 + 1) > 0.$$

Solving the quadratic yields that the G–V bound is beaten when

$$n > \frac{q^2 - 3 + \sqrt{8q^8 + q^4 - 6q^2 + 1}}{2(q^2 - 1)}.$$

For $m = 2$ the largest possible n is $(q - 1)(q + 1)(q^2 - 1)$. Therefore, for each valid n which is a multiple of $q + 1$ between $\frac{q^2 - 3 + \sqrt{8q^8 + q^4 - 6q^2 + 1}}{2(q^2 - 1)}$ and $(q^2 - 1)^2$ we obtain a code of that length that beats the G–V bound.

We show Table 2 where for each q and $d = 3$ we state the range of values of n for which Gilbert–Varshamov bound is beaten.

In the $d = 4$ case (details omitted), the polynomial in n would be cubic instead of quadratic.

Table 2 Some instances of the range of lengths of codes from Theorem 3.7 with $d = 3$ that beat the quantum Gilbert–Varshamov bound

q	3	5	7	9	11
Range of lengths	15-64	38-576	72-2304	117-6400	174-14400

Table 3 A $q = 3$ sample of codes

m	a_1	a_2	a_3	Quantum code	Beats QGV	Comment
1	4			$[[4, 0, 3]]_3$	No	MDS
1	8			$[[8, 4, 3]]_3$	Yes	MDS
2	4	5		$[[20, 14, 3]]_3$	Yes	QHAMDS
2	4	6		$[[24, 18, 3]]_3$	Yes	QHAMDS
2	4	7		$[[28, 22, 3]]_3$	Yes	QHAMDS
2	4	8		$[[32, 26, 3]]_3$	Yes	QHAMDS, equals $[[32, 26, 3]]_3$ in [16]
2	8	5		$[[40, 34, 3]]_3$	Yes	QHAMDS, beats $[[40, 33, 3]]_3$ in [16]
2	8	6		$[[48, 42, 3]]_3$	Yes	QHAMDS, equals $[[48, 42, 3]]_3$ in [16]
2	8	7		$[[56, 50, 3]]_3$	Yes	QHAMDS, beats $[[56, 49, 3]]_3$ in [16]
2	8	8		$[[64, 58, 3]]_3$	Yes	QHAMDS, beats $[[64, 57, 3]]_3$ in [16]
3	8	3	3	$[[72, 64, 3]]_3$	Yes	Beats $[[72, 62, 3]]_3$ in [39]
3	4	8	4	$[[128, 120, 3]]_3$	Yes	Length not obtained with $m = 1, 2$

Table 4 A $q = 5$ sample of codes

m	a_1	a_2	a_3	Quantum Code	Beats QGV	Comment
1	6			$[[6, 2, 3]]_5$	No	MDS
1	12			$[[12, 8, 3]]_5$	Yes	MDS
1	12			$[[12, 6, 4]]_5$	Yes	MDS
2	6	5		$[[30, 24, 3]]_5$	No	QHAMDS, beats $[[33, 13, 3]]_5$ in [8]
2	6	6		$[[36, 30, 3]]_5$	No	QHAMDS
2	6	6		$[[36, 26, 4]]_5$	No	Length not obtained with $m = 1$
2	6	7		$[[42, 36, 3]]_5$	Yes	QHAMDS
2	6	13		$[[78, 72, 3]]_5$	Yes	QHAMDS, beats $[[80, 68, 3]]_5$ in [8]
2	6	13		$[[78, 68, 4]]_5$	Yes	Beats $[[78, 60, 4]]_5$ in [43]
2	6	16		$[[96, 86, 4]]_5$	Yes	Same as in [43]
2	6	19		$[[114, 104, 4]]_5$	Yes	Length not obtained with $m = 1$
2	6	22		$[[132, 122, 4]]_5$	Yes	Beats $[[132, 118, 4]]_5$ in [55]
2	12	24		$[[288, 282, 3]]_5$	Yes	QHAMDS
2	12	24		$[[288, 278, 4]]_5$	Yes	Beats $[[288, 275, 4]]_5$ in [28]
3	24	13	2	$[[624, 612, 4]]_5$	Yes	Same as in [28]
3	24	24	2	$[[1152, 1144, 3]]_5$	Yes	Length not obtained with $m = 1, 2$

Table 5 A $q = 7$ sample of codes

m	a_1	a_2	a_3	Quantum Code	Beats QGV	Comment
1	8			$[[8, 4, 3]]_7$	No	MDS
1	16			$[[16, 12, 3]]_7$	Yes	MDS
1	16			$[[16, 10, 4]]_7$	Yes	MDS
1	16			$[[16, 8, 5]]_7$	Yes	MDS
1	24			$[[24, 20, 3]]_7$	Yes	MDS, same as [54]
1	48			$[[48, 44, 3]]_7$	Yes	MDS
2	8	7		$[[56, 50, 3]]_7$	No	QHAMDS
2	8	8		$[[64, 58, 3]]_7$	No	QHAMDS, beats $[[65, 53, 3]]_7$ in [38]
2	8	8		$[[64, 54, 4]]_7$	No	Length not obtained with $m = 1$
2	8	8		$[[64, 48, 5]]_7$	No	Beats $[[65, 41, 5]]_7$ in [38]
2	8	9		$[[72, 66, 3]]_7$	Yes	QHAMDS, beats $[[75, 63, 3]]_7$ in [43]
2	8	9		$[[72, 56, 5]]_7$	No	Beats $[[75, 51, 5]]_7$ in [43]
2	8	15		$[[120, 114, 3]]_7$	Yes	QHAMDS, beats $[[126, 114, 3]]_7$ in [8]
2	8	21		$[[168, 162, 3]]_7$	Yes	QHAMDS, beats $[[168, 158, 3]]_7$ in [8]
2	8	21		$[[168, 158, 4]]_7$	Yes	Beats $[[168, 152, 4]]_7$ in [8]
2	8	25		$[[200, 190, 4]]_7$	Yes	Same as in [43]
2	8	48		$[[384, 378, 3]]_7$	Yes	QHAMDS, same as in [14]
2	8	48		$[[384, 374, 4]]_7$	Yes	Same as in [14]
2	8	48		$[[384, 368, 5]]_7$	Yes	Same as in [14]
2	16	27		$[[432, 422, 4]]_7$	Yes	Beats $[[432, 419, 4]]_7$ in [28]
3	16	48	2	$[[768, 760, 3]]_7$	Yes	Length not obtained with $m = 1, 2$

Table 6 A $q = 9$ sample of codes

m	a_1	a_2	a_3	Quantum Code	Beats QGV	Comment
1	10			$[[10, 6, 3]]_9$	No	MDS
1	20			$[[20, 16, 3]]_9$	Yes	MDS
1	20			$[[20, 14, 4]]_9$	Yes	MDS
1	20			$[[20, 12, 5]]_9$	Yes	MDS
1	40			$[[40, 36, 3]]_9$	Yes	MDS
2	10	10		$[[100, 80, 6]]_9$	Yes	Length not obtained with $m = 1$
2	10	24		$[[240, 230, 4]]_9$	Yes	Beats $[[246, 228, 4]]_9$ in [43]
2	10	55		$[[550, 534, 5]]_9$	Yes	Length not obtained with $m = 1$
3	80	80	2	$[[12800, 12792, 3]]_9$	Yes	Length not obtained with $m = 1, 2$

Table 7 A $q = 11$ sample of codes

m	a_1	a_2	a_3	Quantum Code	Beats QGV	Comment
1	12			$[[12, 8, 3]]_{11}$	No	MDS
1	12			$[[12, 6, 4]]_{11}$	Yes	MDS
1	12			$[[12, 4, 5]]_{11}$	Yes	MDS
1	60			$[[60, 56, 3]]_{11}$	Yes	MDS
1	60			$[[60, 54, 4]]_{11}$	Yes	MDS
1	60			$[[60, 52, 5]]_{11}$	Yes	MDS
2	12	15		$[[180, 174, 3]]_{11}$	Yes	QHAMDS, beats $[[183, 171, 3]]_{11}$ in [43]
2	12	15		$[[180, 164, 5]]_{11}$	No	Beats $[[183, 159, 5]]_{11}$ in [43]
2	60	120		$[[7200, 7172, 7]]_{11}$	Yes	Length not obtained with $m = 1$

6 Examples

Tables 3, 4, 5, 6, 7 show some samples of small values of the parameters of the quantum codes constructed with Theorem 3.7. For their minimum distance, we give the lower bound t provided by Theorem 3.7. We remind the reader of our notation: q is an odd prime power, a_1 can be any $\lambda(q + 1)$ where λ is a divisor of $q - 1$, and a_2 and a_3 can take any value between 2 and $q^2 - 1$.

Note that for codes $[[n, k, d]]_q = [[n, k, \geq t]]_q$ constructed from Theorem 3.7 we must have $t \leq \frac{q+3}{2} = 3$ when $q = 3$, and $t \leq \frac{q+3}{2} = 4$ when $q = 5$.

Recall also codes with $n + 2 = k + 2d$ are called MDS codes and codes with $n = k + 2d$ are called QHAMDS codes. We also say in the sixth column if that code beats the quantum Gilbert–Varshamov bound in the sense explained before Theorem 5.2.

In order to compare different quantum codes one may use the *length extension*, *subcode* and *smaller distance* propagation rules, as stated in [44] for example. We therefore say that a quantum $[[n, k, d]]_q$ code beats a quantum $[[n', k', d']]_q$ code if at least one of the following holds:

- $n < n'$ and $k = k'$ and $d = d'$ (*length extension*)
- $n = n'$ and $k > k'$ and $d = d'$ (*subcode*)
- $n = n'$ and $k = k'$ and $d > d'$. (*smaller distance*)

In other words, decreasing n , or increasing k , or increasing d , while keeping other parameters fixed, results in a better code. This is well known, see [44] for example, where the authors say that “...all other parameters being equal, we record the smallest n , the largest k , the largest d ,...”.

In the tables below we give some examples of codes that result from our construction, and compare them to the best known codes in the literature. In some cases, we improve on the best known.

It is possible to have more than one improvement. For example, a $[[78, 72, 3]]_5$ code beats a $[[80, 68, 3]]_5$ code in two ways, because it has a smaller n and also has a larger k .

Finally, the article [54] recently appeared on the arxiv and has a construction of MDS codes with lengths of the form $r(q^2 - 1)/h$ where h is an even divisor of $q - 1$ and $r \leq h/2$ (their Theorems 3, 4 and 5). Some of the MDS codes appearing in our tables may also be obtained with their construction.

Acknowledgements This publication has emanated from research conducted with the financial support of Science Foundation Ireland under Grant number 18/CRT/6049. For the purpose of Open Access, the author has applied a CC BY public copyright licence to any Author Accepted Manuscript version arising from this submission.

The second and third authors have been partially supported by MCIN/AEI/10.13039/501100011033 and by the “European Union NextGenerationEU/PRTR”, grants TED2021-130358B-I00 and PID2022-138906NB-C22, as well as by Universitat Jaume I, grants UJI-B2021-02, GACUJIMB/2023/03 and PREDOC/2020/39. The third author would also like to acknowledge the funding received from the UCD School of Mathematics and Statistics.

Funding Open Access funding provided by the IReL Consortium

Data Availability Data sharing is not applicable to this article as no datasets were generated or analysed during the current study.

Declarations

Conflict of interest We declare no conflicts of interest.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article’s Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article’s Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

1. Aly, S.A., Klappenecker, A., Sarvepalli, P.K.: On quantum and classical BCH codes. *IEEE Trans. Inf. Theory* **53**(3), 1183–1188 (2007)
2. Andersen, H.E., Geil, O.: Evaluation codes from order domain theory. *Finite Fields their Appl.* **14**(1), 92–123 (2008)
3. Ashikhmin, A., Barg, A., Knill, E., Litsyn, S.: Quantum error-detection I: Statement of the problem. *IEEE Trans. Inf. Theory* **46**, 778–788 (2000)
4. Ashikhmin, A., Barg, A., Knill, E., Litsyn, S.: Quantum error-detection II: bounds. *IEEE Trans. Inf. Theory* **46**, 789–800 (2000)
5. Ashikhmin, A., Knill, E.: Non-binary quantum stabilizer codes. *IEEE Trans. Inf. Theory* **47**, 3065–3072 (2001)
6. Ashikhmin, A., Litsyn, S., Tsfasman, M.A.: Asymptotically good quantum codes. *Phys. Rev. A* **63**(3), 032311 (2001)
7. Ball, S.: Some constructions of quantum MDS codes. *Des. Codes Cryptogr.* **89**, 811–821 (2021)
8. Bhardwaj, S., Goyal, M., Raka, M.: New quantum codes from constacyclic codes over a general non-chain ring. arXiv preprint [arXiv:2212.02821](https://arxiv.org/abs/2212.02821), (2022)
9. Bierbrauer, J., Edel, Y.: Quantum twisted codes. *J. Comb. Designs* **8**, 174–188 (2000)
10. Brooks, M.: Quantum computers: what are they good for? *Nature* **617**, S1–S3 (2023)

11. 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)
12. 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**(4), 1369–1387 (1998)
13. Camps, E., López, H.H., Matthews, G.L., Sarmiento, E.: Polar decreasing monomial-Cartesian codes. *IEEE Trans. Inf. Theory* **67**(6), 3664–3674 (2021)
14. Cao, M., Cui, J.: Construction of new quantum codes via Hermitian dual-containing matrix-product codes. *Quantum Inf. Process.* **19**, 427 (2020)
15. Castelvecchi, D.: Quantum computers ready to leap out of the lab in 2017. *Nature* **541**(7635), 9–10 (2017)
16. Chen, G., Li, R.: Ternary self-orthogonal codes of dual distance three and ternary quantum codes of distance three. *Des. Codes Cryptogr.* **69**, 53–63 (2013)
17. Cox, D., Little, J., O’Shea, D.: An Introduction to Computational Algebraic Geometry and Commutative Algebra. In: Axler, S., Ribet, K. (eds.) *Ideals, Varieties, and Algorithms*, Undergraduate Texts in Mathematics. Springer, New York (2007)
18. Dieks, D.: Communication by EPR devices. *Phys. Rev. A* **92**, 271 (1982)
19. Fang, W., Fu, F.W.: Some new constructions of quantum MDS codes. *IEEE Trans. Inf. Theory* **65**, 7840–7847 (2019)
20. Feng, G.-L., Rao, T.R.N.: Decoding algebraic-geometric codes up to the designed minimum distance. *IEEE Trans. Inf. Theory* **39**(1), 37–45 (1993)
21. Feng, K.: Quantum error correcting codes. In: Niederreiter, H. (ed.) *Coding Theory and Cryptology*. Lecture Notes Series, vol. 1, pp. 91–142. National University of Singapore, Institute for Mathematical Sciences (2002)
22. Feng, K., Ma, Z.: A finite Gilbert-Varshamov bound for pure stabilizer quantum codes. *IEEE Trans. Inf. Theory* **50**(12), 3323–3325 (2004)
23. Fitzgerald, J., Lax, R.F.: Decoding Affine Variety Codes Using Gröbner Basis. *Des. Codes Cryptogr.* **13**, 147–158 (1998)
24. Galindo, C., Geil, O., Hernando, F., Ruano, D.: On the distance of stabilizer quantum codes from J -affine variety codes. *Quantum Inf Process.* **164**, 111 (2017)
25. Galindo, C., Geil, O., Hernando, F., Ruano, D.: Improved constructions of nested code pairs. *IEEE Trans. Inf. Theory* **64**(4), 2444–2459 (2018)
26. Galindo, C., Hernando, F., Martín-Cruz, H.: Optimal (r, δ) -LRCs from monomial-Cartesian codes and their subfield-subcodes. *arXiv preprint arXiv:2205.01485*, (2023)
27. Galindo, C., Hernando, F., Martín-Cruz, H., Ruano, D.: Stabilizer quantum codes defined by trace-dependent polynomials. *Finite Fields their Appl.* **87**, 102138 (2023)
28. Galindo, C., Hernando, F., Ruano, D.: New quantum codes from evaluation and matrix-product codes. *Finite Fields their Appl.* **36**, 98–120 (2015)
29. Geil, O., Høholdt, T.: Footprints or generalized Bezout’s theorem. *IEEE Trans. Inf. Theory* **46**(2), 635–641 (2000)
30. Geil, O., Høholdt, T.: On hyperbolic codes. In: Boztas, S., Shparlinski, I.E. (eds.) *Applied Algebra. Algebraic Algorithms and Error-Correcting Codes*, volume 2227 of *Lecture Notes in Computer Science*, pp. 159–171. Springer, Berlin, Germany (2001)
31. Gottesman, D.: Class of quantum error-correcting codes saturating the quantum Hamming bound. *Phys. Rev. A* **54**(3), 1862–1868 (1996)
32. Grassl, M., Beth, T., Rötteler, M.: On optimal quantum codes. *Int. J. Quantum Inf.* **2**(1), 55–64 (2004)
33. Grassl, M., Rötteler, M.: Quantum BCH codes. In *Proc. X Int. Symp. Theor. Elec. Eng.*, pages 207–212, (1999)
34. Høholdt, T., van Lint, J.H., Pellikaan, G.R.: Algebraic geometry codes. In: Pless, V.S., Huffman, W.C. (eds.) *Handbook of Coding Theory*, pp. 871–961. Elsevier, Netherlands (1998)
35. Ketkar, A., Klappenecker, A., Kumar, S., Sarvepalli, P.K.: Nonbinary stabilizer codes over finite fields. *IEEE Trans. Inf. Theory* **52**(11), 4892–4914 (2006)
36. Klappenecker, A., Rötteler, M.: Beyond stabilizer codes I: nice error bases. *IEEE Trans. Inf. Theory* **48**(8), 2392–2395 (2002)
37. Knill, E.: Non-Binary Unitary Error Bases and Quantum Codes. Technical report, Los Alamos National Laboratory, LAUR-96-2717, (1996)
38. Kolotoğlu, E., Sari, M.: Quantum codes with improved minimum distance. *Bull. Korean Math. Soc.* **56**(3), 609–619 (2019)

39. Kong, B., Zheng, X.: Quantum codes from constacyclic codes over S_k . *EPJ Quantum Technol.*, **10**(3), (2023)
40. La Guardia, G.G.: Construction of new families of nonbinary quantum codes. *Phys. Rev. A* **80**, 042331 (2009)
41. La Guardia, G.G.: On the construction of nonbinary quantum BCH codes. *IEEE Trans. Inf. Theory* **60**(3), 1528–1535 (2014)
42. Liu, H., Liu, X.: Constructions of quantum MDS codes. *Quantum Inf. Process.* **20**(14), 1–3 (2021)
43. Liu, X., Dinh, H.Q., Liu, H., Yu, L.: On new quantum codes from matrix product codes. *Cryptogr. Commun.* **10**, 579–589 (2018)
44. Luo, G., Ezerman, M.F., Grassl, M., Ling, S.: Constructing quantum error-correcting codes that require a variable amount of entanglement. *Quantum Inf. Process.* **23**, 4 (2024)
45. López, H.H., Matthews, G.L., Soprunov, I.: Monomial-Cartesian codes and their duals, with applications to LCD codes, quantum codes, and locally recoverable codes. *Des. Codes Cryptogr.* **88**, 1673–1685 (2020)
46. López, H.H., Soprunov, I., Villarreal, R.H.: The dual of an evaluation code. *Des. Codes Cryptogr.* **89**, 1367–1403 (2021)
47. Matsumoto, R., Uyematsu, T.: Constructing quantum error-correcting codes for p^m -state systems from classical error-correcting codes. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **83**(10), 1878–1883 (2000)
48. Rains, E.M.: Quantum weight enumerators. *IEEE Trans. Inf. Theory* **44**(4), 1388–1394 (1998)
49. Shor, P.W.: Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A* **52**(4), 2493–2496 (1995)
50. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.* **26**(5), 1484–1509 (1997)
51. Song, H., Li, R., Liu, Y., Guo, G.: New quantum codes from matrix-product codes over small fields. *Quantum Inf. Process.* **19**(226), 1–22 (2020)
52. Steane, A.: Multiple-particle interference and quantum error correction. *Proc. R. Soc. Lond. A* **452**, 2551–2577 (1996)
53. Steane, A.M.: Simple quantum error-correcting codes. *Phys. Rev. A* **54**(6), 4741–4751 (1996)
54. Wan, R., Zhu, S.: New Quantum MDS codes from Hermitian self-orthogonal generalized Reed-Solomon codes. *arXiv preprint arXiv:2302.06169*, (2023)
55. Wang, Y., Kai, X., Sun, Z., Zhu, S.: Quantum codes from Hermitian dual-containing constacyclic codes over $\mathbb{F}_{q^2} + v\mathbb{F}_{q^2}$. *Quantum Inf. Process.* **20**(122), 1–17 (2021)
56. Wootters, W.K., Zurek, W.H.: A single quantum cannot be cloned. *Nature* **299**, 802–803 (1982)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.