Some constructions of quantum MDS codes

Simeon Ball[1] ⬤

Abstract

We construct quantum MDS codes with parameters $[\![q^2 + 1, q^2 + 3 - 2d, d]\!]_q$ for all $d \leq q + 1$, $d \neq q$. These codes are shown to exist by proving that there are classical generalised Reed–Solomon codes which contain their Hermitian dual. These constructions include many constructions which were previously known but in some cases these codes are new. We go on to prove that if $d \geq q + 2$ then there is no generalised Reed–Solomon $[n, n - d + 1, d]_{q^2}$ code which contains its Hermitian dual. We also construct an $[\![18, 0, 10]\!]_5$ quantum MDS code, an $[\![18, 0, 10]\!]_7$ quantum MDS code and a $[\![14, 0, 8]\!]_5$ quantum MDS code, which are the first quantum MDS codes discovered for which $d \geq q + 3$, apart from the $[\![10, 0, 6]\!]_3$ quantum MDS code derived from Glynn's code.

Keywords Quantum error-correction · Quantum MDS codes · Arcs

Mathematics Subject Classification 94B99 · 51E21

1 Introduction

To be able to store information on a quantum system and process that information, it is essential to use a quantum error-correcting code. In this way any small perturbation of the system can be corrected and the information restored. As with classical error-correcting codes, if there is no limit to the size of the alphabet (the local dimension of the quantum particles in the case of a quantum error-correcting code) then we can employ optimal codes which meet the Singleton bound (the quantum Singleton bound for quantum error-correcting codes) which are called maximum distance separable (MDS) codes. Nearly all quantum error-correcting MDS codes known are constructed by means of the more general construction of employing a classical linear code over $\mathbb{F}_{q^2}$ which contains its Hermitian dual. In most cases,

✉ Simeon Ball
   simeon.michael.ball@upc.edu

[1]   Univ. Politecnica De Catalunya, Barcelona, Spain

🌀 Springer

this has been done by proving that there are generalised (possibly truncated) Reed–Solomon codes which contain their Hermitian dual. In this article we prove that if the minimum distance d satisfies $d \leq q + 1$ and $d \neq q$, then there are generalised Reed–Solomon codes of length $q^2 + 1$ which contain their Hermitian dual. This was not previously known when both d and q are even. More surprisingly, we go on to prove that if $d \geq q + 2$ then there are no generalised Reed–Solomon codes of any length which contain their Hermitian dual. However, we do provide some sporadic examples of quantum MDS codes for which $d \geq q + 3$.

2 Linear and quantum error-correcting codes

Let A be a finite set. A *code* C over A of length n is a subset of A^n. The elements of C are called *codewords*. The minimum distance d is the minimum number of coordinates in which two codewords differ. The *Singleton bound* states that

$$|C| \leq |A|^{n-d+1}.$$

A code for which $|C| = |A|^{n-d+1}$ is called a *maximum distance separable* code or simply an MDS code.

Let $\mathbb{F}_q$ denote the finite field with q elements, where q is the power of some prime p. The *weight* of a vector of $\mathbb{F}_q^n$ is the number of non-zero coordinates that it has.

A k-dimensional *linear code* C of length n is a k-dimensional subspace of $\mathbb{F}_q^n$. We will denote such a code with minimum distance d as an $[n, k, d]_q$ code.

Let α be a Hermitian form defined on $\mathbb{F}_{q^2}^n \times \mathbb{F}_{q^2}^n$ by

$$\alpha(u, v) = u_1 v_1^q + \cdots + u_n v_n^q.$$

The Hermitian dual of a linear code C over $\mathbb{F}_{q^2}$ is

$$C^{\perp_h} = \{v \in \mathbb{F}_q^n \mid \alpha(u, v) = 0, \text{ for all } u \in C\}.$$

In this article we will construct linear MDS codes C over $\mathbb{F}_{q^2}$ for which $C^{\perp_h} \leq C$ and from these we will construct previously unknown quantum MDS codes.

The following lemma is from [3, Proposition 2.1].

Lemma 1 *C is a linear $[n, k, n - k + 1]_{q^2}$ MDS code if and only if $C^{\perp_h}$ is a linear $[n, n - k, k + 1]_{q^2}$ MDS code. Moreover, $(C^{\perp_h})^{\perp_h} = C$.*

A quantum code on n subsystems is a K-dimensional subspace of $(\mathbb{C}^q)^{\otimes n}$. A code with minimum distance d is able to detect errors, which act non-trivially on the code space, on up to $d - 1$ of the subsystems and correct errors on up to $\frac{1}{2}(d - 1)$ of the subsystems. If the dimension $K = q^k$ for some k then we say the quantum code is an $[\![n, k, d]\!]_q$ code and if not simply an $((n, K, d))_q$ code.

To be able to describe in more detail the quantum error-correcting codes we shall construct here, we have to discuss the type of errors we wish to correct. Let $\{|x\rangle \mid x \in \mathbb{F}_q\}$ be a basis of $\mathbb{C}^q$. We define the following set of endomorphisms of $\mathbb{C}^q$ called the *generalised Pauli operators*. For each $a, b \in \mathbb{F}_q$, we define $X(a)$ by its action on the basis vectors, $X(a)|x\rangle = |x + a\rangle$, and likewise $Z(b)$ by $Z(b)|x\rangle = e^{2\pi i \text{tr}(bx)/p}|x\rangle$, where tr denotes the usual trace map from $\mathbb{F}_q$ to $\mathbb{F}_p$. The generalised Pauli operators are of the form $X(a)Z(b)$, for some $a, b \in \mathbb{F}_q$. In the error model, the (Pauli) errors on $(\mathbb{C}^q)^{\otimes n}$ are tensor products of generalised Pauli operators. An error has weight t if precisely t of the components in the

tensor product are not the identity operator, whilst the remaining $n-t$ are the identity operator. A quantum error-correcting code of minimum distance d is able to correct all Pauli errors of weight at most $\frac{1}{2}(d-1)$ which act non-trivially on the code subspace. Such quantum error-correcting codes are most commonly constructed by taking the joint eigenspace of eigenvalue 1 of a subgroup of Pauli operators. These codes are called *stabiliser* codes. It turns out that stabiliser codes are equivalent to certain classical codes which are additive over $\mathbb{F}_{q^2}$. One construction of a particular subset of these codes is that employed in Theorem 2. Thus the quantum codes which will construct here are stabiliser codes. We refer to [20] for a more detailed discussion of stabiliser codes.

We rely on the following theorem from [20, Corollary 19].

Theorem 2 *If there is an $[n, n-k, d]_{q^2}$ linear code C such that $C^{\perp_h} \leq C$ then there exists an $[\![n, n-2k, d']\!]_q$ quantum code with $d' \geq d$.*

The quantum Singleton bound states that for an $[\![n, k, d]\!]_q$ quantum code, $k \leq n-2d+2$. A code reaching this bound is called a *quantum MDS code*. The quantum Singleton bound implies that for an $[\![n, n-2k, d']\!]_q$ quantum code, $d' \leq k+1$. Thus, Theorem 2 implies for MDS codes that $d' = d$. Hence, we have the following, see [15, Corollary 3.2].

Theorem 3 *If there is an $[n, n-k, k+1]_{q^2}$ linear MDS code C such that $C^{\perp_h} \leq C$ then there is an $[\![n, n-2k, k+1]\!]_q$ quantum MDS code.*

In the next section we will give a simple construction of a $[q^2+1, k, q^2+2-k]_{q^2}$ MDS codes which is contained in its Hermitian dual, for all $k \leq q$, $k \neq q-1$. This code is a generalised Reed–Solomon code. The Hermitian dual of this code is a $[q^2+1, q^2+1-k, k+1]_{q^2}$ generalised Reed–Solomon code which contains its Hermitian dual. Thus, Theorem 3 implies the existence of $[\![q^2+1, q^2+1-2k, k+1]\!]_q$ quantum MDS codes for all $k \leq q$, $k \neq q-1$.

In Huber and Grassl [13], we find the following bounds on the existence of an $[\![n, k, d]\!]_q$ quantum MDS code for $q=5$. If $n+k=14$ then $4 \leq d \leq 8$. The lower bound comes from a construction of a $[10, 3, 8]_{25}$ linear MDS code which is contained in its Hermitian dual. The upper bound would be attained by a $[14, 7, 8]_{25}$ linear MDS code which is equal to its Hermitian dual. We will construct such a code here. If $n+k=18$ then we have $5 \leq d \leq 10$. The upper bound would be attained if there is a $[18, 9, 10]_{25}$ linear MDS code which is equal to its Hermitian dual. Again, we will construct such a code here.

3 A construction of quantum MDS codes based on generalised Reed–Solomon codes

There are many constructions of quantum MDS codes with $d \leq q+1$, mostly based on cyclic or constacyclic constructions and generalised Reed–Solomon codes. For example those contained in [4–6,10,11,14–18,21,22,26–28,30–33].

Here we give a short proof that for all $k \leq q, k \neq q-1$, there are $[\![q^2+1, q^2+1-2k, k+1]\!]_q$ quantum MDS codes arising from generalised Reed–Solomon codes of length q^2+1. This extends the results of Jin et al [15], who proved the existence for $k \leq \frac{1}{2}q$ and Grassl and Rötteler [10] who proved the existence for $k \leq q$ unless q is even and k is odd. Grassl and Rötteler [10] also prove the existence for $k = q-1$ and $q \in \{8, 16, 32, 64, 128\}$, cases which are not covered by Theorem 4. Note that a similar result to Theorem 4 is claimed in [16, Theorem 4.6] but this relies on the erroneous [16, Corollary 3.2, part (ii)].

Indeed, the hypothesis of [16, Theorem 4.6] includes the case $k = q - 1$ and $q = 4$. The proof involves showing that there is a generalised Reed–Solomon code with parameters $[17, 3, 15]_{16}$ contained in its Hermitian dual. However, a quick computer search reveals that no such code exists. In fact, computer searches reveal that neither the $[18, 3, 16]_{16}$ coming from a regular or a Lunelli-Sce hyperoval of PG(2, 16) (where PG($k - 1, q$) denotes the $(k - 1)$-dimensional projective space over $\mathbb{F}_q$) can be truncated to a $[17, 3, 15]_{16}$ code which is contained in its Hermitian dual. In other words, the puncture code has no codewords of weight 17, or in fact any odd weight. We refer to [10] for more on constructions of quantum MDS codes via the puncture code. The only other complete arc of PG(2, 16) of size at least 13 is the Kestenband arc (from [19]) constructed as the intersection of two Hermitian curves. Again, by employing a computer search, we discover that any $[13, 3, 11]_{16}$ code obtained from this Kestenband arc is not contained in its Hermitian dual. These are the only complete arcs in PG(2, 16) of size at least 13 (see for example [12]), so all linear $[n, 3, n - 2]_{16}$ MDS codes with $n \geq 13$ come from one of these examples. We conclude that there is no way to construct an $[\![n, n - 6, 4]\!]_4$ quantum MDS code, for $n \in \{13, 15, 17\}$, from a linear $[n, 3, n - 2]_{16}$ MDS code contained in its Hermitian dual. To clarify, any such code must be linearly equivalent to (the truncation of) either a Reed–Solomon code, a Kestenband arc or the Lunelli-Sce hyperoval and none of these examples can be truncated to give such a code.

Theorem 4 *For q a prime power, there exists a $[\![q^2 + 1, q^2 + 1 - 2k, k + 1]\!]_q$ quantum MDS code for all $k \leq q$ where $k \neq q - 1$.*

Proof For all $k \leq q$, where $k \neq q - 1$, we will construct a $[q^2 + 1, k, q^2 + 2 - k]_{q^2}$ MDS code D such that $D \leq D^{\perp_h}$. Lemma 1 implies that $C = D^{\perp_h}$ is a $[q^2 + 1, q^2 + 1 - k, k + 1]_{q^2}$ linear MDS code such that $C^{\perp_h} \leq C$. Theorem 3 then implies that there exists a $[\![q^2 + 1, q^2 + 1 - 2k, k + 1]\!]_q$ quantum MDS code.

Denote by $\{a_1, \ldots, a_{q^2}\}$ the elements of $\mathbb{F}_{q^2}$.

Let $h(X)$ be a monic polynomial of $\mathbb{F}_{q^2}[X]$ of degree $q - k$ such that $h(a_j) \neq 0$ for all j. If $k = q$ then we can take $h(X) = 1$. If $k \leq q - 2$ then we can take $h(X)$ to be an irreducible polynomial in $\mathbb{F}_{q^2}[X]$.

Define

$$D = \{(h(a_1)f(a_1), \ldots, h(a_{q^2})f(a_{q^2}), f_{k-1}) \mid f \in \mathbb{F}_{q^2}[X], \ \deg f \leq k - 1\},$$

where f_i denotes the coefficient of X^i in $f(X)$.

Firstly, we prove that D is an MDS code. Observe that D is a $[q^2 + 1, k, d]_{q^2}$ linear code, so we have to prove that $d = q^2 + 2 - k$.

Consider u and v two codewords of D given respectively by polynomials f and g of degree at most $k - 1$.

If $f_{k-1} \neq g_{k-1}$ and u and v agree in the coordinate indexed by a_i then a_i is a zero of $h(X)(f(X) - g(X))$. Since $(f - g)(X)$ has at most $k - 1$ zeros and $h(a_i) \neq 0$, the codewords u and v agree in at most $k - 1$ coordinates.

If $f_{k-1} = g_{k-1}$ then $(f - g)(X)$ has degree at most $k - 2$ and therefore has at most $k - 2$ zeros. Thus, the codewords u and v agree in at most $k - 1$ coordinates.

Hence, the minimum distance of D is at least $q^2 + 1 - (k - 1)$ which attains the Singleton bound.

Let r_m denote the coefficient of X^m in $h(X)^{q+1}$. Then

$$\alpha(u, v) = f_{k-1} g_{k-1}^q + \sum_{t \in \mathbb{F}_{q^2}} h(t)^{q+1} f(t) g(t)^q$$

$$= f_{k-1} g_{k-1}^q + \sum_{t \in \mathbb{F}_{q^2}} \sum_{m=0}^{(q-k)(q+1)} \sum_{i,j=0}^{k-1} f_i g_j^q r_m t^{i+jq+m}$$

$$= f_{k-1} g_{k-1}^q + \sum_{m=0}^{(q-k)(q+1)} \sum_{i,j=0}^{k-1} f_i g_j^q r_m \sum_{t \in \mathbb{F}_{q^2}} t^{i+m+jq}$$

Since $\sum_{t \in \mathbb{F}_{q^2}} t^i = 0$ for all $i = 0, \ldots, q^2 - 2$ and $\sum_{t \in \mathbb{F}_{q^2}} t^{q^2-1} = -1$, we have that $\alpha(u, v) = 0$. Note that $r_{(q-k)(q+1)} = 1$, since h is monic.

Thus, $D \leq D^{\perp_h}$, as required. □

The codes constructed in Theorem 4 are examples of generalised Reed–Solomon codes. A generalised Reed–Solomon code over $\mathbb{F}_{q^2}$ is a code

$$D = \{(c_1 f(a_1), \ldots, c_{q^2} f(a_{q^2}), c_{q^2+1} f_{k-1}) \mid f \in \mathbb{F}_{q^2}[X], \ \deg f \leq k - 1\},$$

where $c_1, \ldots, c_{q^2+1}$ are elements of $\mathbb{F}_{q^2}$. In Theorem 4, we proved that there are generalised Reed–Solomon codes over $\mathbb{F}_{q^2}$ which are contained in their Hermitian duals in which $c_i = h(a_i)$ for some polynomial $h(X)$. However, for larger dimensions generalised Reed–Solomon codes are not contained in their Hermitian duals, as we shall now prove.

Theorem 5 *If $k \geq q + 1$ then a k-dimensional generalised Reed–Solomon code over $\mathbb{F}_{q^2}$ is not contained in its Hermitian dual.*

Proof Let $A = \{a_1, \ldots, a_{q^2}\}$ be the set of elements of $\mathbb{F}_{q^2}$, where $a_{q^2} = 0$. Let D be a generalised Reed–Solomon code over $\mathbb{F}_{q^2}$ which is contained in its Hermitian dual.

Since D is a generalised Reed–Solomon code, there are $v_1, \ldots, v_n$, elements of $\mathbb{F}_{q^2}$, such that

$$D = \{(v_1 f(a_1), \ldots, v_{q^2} f(a_{q^2}), c_f) \mid f \in \mathbb{F}_{q^2}[X], \ \deg f \leq k - 1\},$$

where c_f is the coefficient of X^{k-1} of f or possibly zero. We also allow some of the v_i to be zero too, which would be equivalent to taking a shorter length generalised Reed–Solomon code.

Consider u and v two codewords of D given respectively by polynomials f and g of degree at most $k - 1$.

Since D is contained in its Hermitian dual,

$$c_f c_g^q + \sum_{i=1}^{q^2} v_i^{q+1} f(a_i) g(a_i)^q = 0.$$

Let f_i denote the coefficient of X^i in $f(X)$ and g_m denote the coefficient of X^m in $g(X)$. Then the above is

$$c_f c_g^q + \sum_{i=1}^{q^2} \sum_{j=0}^{k-1} \sum_{m=0}^{k-1} v_i^{q+1} f_j g_m^q a_i^{mq+j} = 0.$$

For all $\ell = 1, \ldots, q^2 - 2$, where $\ell = \ell_0 + \ell_1 q$, with $f(X) = X^{\ell_0}$ and $g(X) = X^{\ell_1}$, this implies that

$$\sum_{i=1}^{q^2-1} v_i^{q+1} a_i^\ell = 0.$$

Considering this set of equations in matrix form Au=0, where A $= (b_{\ell i})$ is a $(q^2 - 2) \times (q^2 - 1)$ matrix given by $b_{\ell i} = a_i^\ell$ and where u is the vector of $\mathbb{F}_q^{q^2-1}$ whose i-th coordinate is v_i^{q+1}.

The matrix A contains $(q^2 - 2) \times (q^2 - 2)$ submatrix which is a Vandermonde matrix, so has rank $q^2 - 2$. Therefore, the solution space has dimension one and is spanned by the all-one vector. This implies that $v_i^{q+1} = \lambda^{q+1} \neq 0$ for all $i = 1, \ldots, q^2 - 1$, for some $\lambda \in \mathbb{F}_{q^2}$.

Thus, we have that

$$c_f c_g^q + (v_{q^2}^{q+1} - \lambda^{q+1}) f_0 g_0^q - \lambda^{q+1} \sum_{j,m:q^2-1 | j+mq \neq 0} f_j g_m^q = 0. \tag{1}$$

Since $c_f = f_{k-1}$ or zero, with $f(X) = g(X) = 1$, (1) implies $v_{q^2}^{q+1} = \lambda^{q+1}$. Then, with $f(X) = g(X) = X^{q-1}$, (1) implies $\lambda = 0$, a contradiction. $\qquad \square$

Since the dual of a generalised Reed–Solomon code is a generalised Reed–Solomon code [23, Chapter 10], Theorem 5 tells us that if $k \geq q + 1$ then there are no $[n, n - k, k + 1]_{q^2}$ generalised Reed–Solomon codes which contain their Hermitian dual. Thus, we should look elsewhere if we want to construct quantum MDS codes via Theorem 3, for $d \geq q + 2$. This we will do in the next section.

4 Linear codes of rate one half

Let M be a $k \times k$ matrix with entries from $\mathbb{F}_q$ and let I_k denote the $k \times k$ identity matrix. For some non-zero $\lambda \in \mathbb{F}_q$, let

$$G = (\lambda I_k \mid M).$$

The subspace spanned by the rows of G is a k-dimensional linear code C of length $2k$ over $\mathbb{F}_q$. In the following theorems we will determine the minimum distance of C depending on certain hypotheses regarding M.

Theorem 6 *If every* $j \times (k - d + 1 + j)$ *sub-matrix of* M *for* $j = 1, \ldots, d - 1$ *has rank* j *then* C *is a* $[2k, k, \geq d]$ *code.*

Proof If C does not have minimum distance at least d then there are two distinct codewords u and v which differ in at most $d - 1$ coordinates. Therefore, $u - v = (a_1, \ldots a_k)G$ has at least $2k - d + 1$ zeros.

Let S be the set of of columns of G viewed as points of PG$(k-1, q)$, the $(k-1)$-dimensional projective space over $\mathbb{F}_q$. Since $(a_1, \ldots, a_k)G$ has at least $2k - d + 1$ zeros, there is a subset S' of S of $2k - d + 1$ points which are incident with the hyperplane $a_1 X_1 + \cdots + a_k X_k = 0$.

For any subset T of S, let G(T) denote the submatrix of G restricted to the columns of T. Observe that the rank of the matrix G(S') is at most $k - 1$.

Suppose that i of the points of S' are in the canonical basis and let S'' be a subset of S' consisting of the $2k - d + 1 - i$ points not in the canonical basis. Since $2k - d + 1 - i \leq k$,

we have $i \geq k - d + 1$. Since $G(S')$ has rank at most $k - 1$, the matrix $G(S'')$ contains a sub-matrix of M which is a $(k - i) \times (2k - d + 1 - i)$ sub-matrix of rank at most $k - i - 1$. The hypothesis then implies $k - i \geq d$ which implies $i \leq k - d$, a contradiction.   □

Theorem 7 *Suppose that* M *is a non-singular* $k \times k$ *matrix. If every* $j \times (k - d + 1 + j)$ *sub-matrix of* M *and* M^{-1} *has rank* j *for all* $j = 1, \ldots, \lfloor \frac{1}{2}(d - 1) \rfloor$ *then* C *is a* $[2k, k, \geq d]$ *code.*

Proof In the proof of Theorem 6, we can assume that $i \geq k - \lfloor \frac{1}{2}(d - 1) \rfloor$ by multiplying the matrix G by M^{-1}. Multiplying by M^{-1} constitutes a change of basis but does not affect the geometry of the point set S and in particular its intersection with hyperplanes. The hypothesis now implies $k - i > \lfloor \frac{1}{2}(d - 1) \rfloor$, a contradiction.   □

Let σ be an automorphism of $\mathbb{F}_q$. For a matrix $A = (a_{ij})$, we define $A^\sigma = (a_{ij}^\sigma)$ and $A^t = (a_{ji})$

Theorem 8 *Suppose that* M *is a non-singular* $k \times k$ *matrix and that* $(M^\sigma)^t = -\lambda^{\sigma+1} M^{-1}$ *for some automorphism* σ *of* $\mathbb{F}_q$ *and for some non-zero* $\lambda \in \mathbb{F}_q$. *If every* $j \times (k - d + 1 + j)$ *sub-matrix of* M *and every* $(k - d + 1 + j) \times j$ *sub-matrix of* M *has rank* j *for all* $j = 1, \ldots, \lfloor \frac{1}{2}(d - 1) \rfloor$ *then* C *is a* $[2k, k, \geq d]$ *code such that* $C \leq C^{\perp_\sigma}$, *where* $\perp_\sigma$ *is defined with respect to the sesqui-linear form*

$$\beta(u, v) = u_1 v_1^\sigma + \cdots + u_{2k} v_{2k}^\sigma.$$

Proof Observe that for a sub-matrix B of A there is a corresponding submatrix B' of A^σ (taking the same restriction to rows and columns) and that the rank of B' is equal to the rank of B. That C is a linear code of minimum distance d now follows from Theorem 7.

Suppose that $M^{-1} = (b_{ij})$.

If u is the i-th row of G and v is the j-th row of G, $i \neq j$, then

$$\beta(u, v) = \sum_{m=1}^{k} a_{im} a_{jm}^\sigma = -\lambda^\sigma \lambda \sum_{m=1}^{k} a_{im} b_{mj} = 0.$$

Meanwhile,

$$\beta(u, u) = \lambda^\sigma \lambda + \sum_{m=1}^{k} a_{im} a_{im}^\sigma = \lambda^\sigma \lambda - \lambda^\sigma \lambda \sum_{m=1}^{k} a_{im} b_{mi} = 0.$$

Thus, $C \leq C^{\perp_\sigma}$.   □

We are now in a position to prove the main theorem of this section. Observe that we now replace q by q^2 and the automorphism σ will be $x \mapsto x^q$.

Theorem 9 *If there is a* $k \times k$ *non-singular matrix* M *with entries from* $\mathbb{F}_{q^2}$ *for which* $(M^\sigma)^t = -\lambda^{q+1} M^{-1}$ *for some non-zero* $\lambda \in \mathbb{F}_{q^2}$, *where* $\sigma(x) = x^q$, *and every* $j \times j$ *sub-matrix of* M *is non-singular for all* $j = 1, \ldots, \lfloor \frac{1}{2} k \rfloor$ *then there is a* $[\![2k - r, r, k + 1 - r]\!]_q$ *quantum MDS code, for all* $r = 0, \ldots, k - 1$.

Proof By Theorem 8, $C \leq C^{\perp_h}$ and C is a $[2k, k, k+1]_{q^2}$ linear MDS code. Since dim $C = $ dim $C^{\perp_h}$, we have that $C = C^{\perp_h}$, so Theorem 3 implies there exists a $[\![2k, 0, k+1]\!]_q$ quantum MDS code.

Rains [24] showed that if there is a pure $[[n, k, d]]_q$ quantum code with $n, d \geq 2$ then there exists a pure $[[n-1, k+1, d-1]]_q$ quantum code. Later, Rains [25] proved that a quantum MDS code must be pure, so there exists a $[[2k-r, r, k+1-r]]_q$ quantum MDS codes, if the hypothesis on M is satisfied, for all $r = 0, \ldots, k-1$. □

5 Circulant matrices

A circulant matrix M is a matrix whose $(i+1)$-st row is a cyclic shift of the first row i places to the right with wrap around. In other words,

$$M = \begin{pmatrix} x_1 & x_2 & \ldots & x_{k-1} & x_k \\ x_k & x_1 & \ldots & x_{k-2} & x_{k-1} \\ . & . & \ddots & . & . \\ . & . & . & \ddots & . \\ x_2 & x_3 & \ldots & x_k & x_1 \end{pmatrix}$$

for some $x = (x_1, \ldots, x_k)$.

A linear code of rate one half which is the row span over $\mathbb{F}_q$ of a matrix

$$G = (\lambda I_k \mid M).$$

for some non-zero $\lambda \in \mathbb{F}_q$, is called a *doubly circulant code*. Such codes have been well studied, see for example [2,29].

Theorem 10 *Let M be a $k \times k$ non-singular circulant matrix with entries from $\mathbb{F}_{q^2}$ whose first row is $x = (x_1, \ldots, x_k)$. Then $(M^\sigma)^t = -\lambda^{q+1} M^{-1}$ for some non-zero $\lambda \in \mathbb{F}_{q^2}$, where $\sigma(x) = x^q$ if and only if $H_m(x) = 0$ for all $m = 1, \ldots, \lfloor \frac{1}{2}k \rfloor$, where*

$$H_m(x) = \sum_{i=1}^{k} x_i x_{i+m}^q$$

and the indices are read modulo k.

Proof If $M = (a_{ij})$ then $a_{ij} = x_{j-i+1}$, since M is circulant whose first row is $x = (x_1, \ldots, x_k)$.

The scalar product of the i-th row of M with the r-th column of $(M^\sigma)^t$ is

$$\sum_{j=1}^{k} a_{ij} a_{rj}^q = \sum_{j=1}^{k} x_{j-i+1} x_{j-r+1}^q = \sum_{j=1}^{k} x_j x_{j+i-r}^q = H_{i-r}(x).$$

Observe that $H_0(x) \in \mathbb{F}_q$, so there is a $\lambda \in \mathbb{F}_{q^2}$ such that $\lambda^{q+1} = H_0(x)$. Moreover, since M is non-singular, $\lambda \neq 0$.

$$H_m(x)^q = \sum_{i=1}^{k} x_i^q x_{i+m} = \sum_{i=1}^{k} x_{i-m}^q x_i = H_{-m},$$

so it suffices that $H_m(x) = 0$ for $m = 1, \ldots, \lfloor \frac{1}{2}k \rfloor$. □

Corollary 11 *Let* M *be a* $k \times k$ *non-singular circulant matrix with entries from* $\mathbb{F}_{q^2}$ *whose first row is* $x = (x_1, \ldots, x_k)$. *If, for all* $m = 1, \ldots, \lfloor \frac{1}{2}k \rfloor$, *all* $m \times m$ *submatrices of* M *are non-singular,*

$$H_m(x) = \sum_{i=1}^{k} x_i x_{i+m}^q = 0$$

and

$$\sum_{i=1}^{k} x_i^{q+1} \neq 0$$

then there exists a $[\![2k - r, r, k + 1 - r]\!]_q$ *quantum MDS code, for all* $r = 0, \ldots, k - 1$.

Proof This follows from Theorem 9 and Theorem 10. □

6 Computational results

Recall that we are interested in constructing $[\![2k, 0, k + 1]\!]_q$ quantum MDS codes with $k \geq q + 1$. This then implies there are $[\![2k - r, r, k + 1 - r]\!]_q$ quantum MDS codes for all $r = 0, \ldots, k - 1$.

$\underline{k = 5 \, (q \leq 4)}.$

A $[\![10, 0, 6]\!]_q$ code exists for both $q = 3$ and $q = 4$, since in both cases there are $[10, 5, 6]_q$ codes which are equal to their Hermitian dual. These examples are due to Glynn [7] for $q = 3$ and Grassl and Gulliver [9] for $q = 4$.

For $q = 3$, Corollary 11 applies if $x = (\epsilon^2, \epsilon^3, \epsilon^3, \epsilon^2, 1)$, where $\epsilon^2 = \epsilon + 1$.

For $q = 4$, Corollary 11 applies if $x = (\epsilon^2, \epsilon^{12}, \epsilon^{12}, \epsilon^2, 1)$, where $\epsilon^4 = \epsilon + 1$.

$\underline{k = 6 \, (q \leq 5)}.$

An exhaustive search reveals that there are no circulant matrices M for which the hypothesis of Corollary 11 is satisfied for $q = 4$ or $q = 5$.

There are examples for $q = 7$, for example $x = (\epsilon^{21}, \epsilon^{44}, \epsilon^8, \epsilon^9, \epsilon^{12}, 1)$, where $\epsilon^2 = \epsilon + 4$, which are perhaps interesting in that they are not obtained by truncating a generalised Reed–Solomon code. This can be checked by calculating the dimension of the subspace of quadrics which are zero on the columns of G. The dimension of the subspace of quadrics which are zero on the columns of a generator matrix of a generalised Reed–Solomon code is $\binom{k-1}{2}$, see Glynn [8, Theorem 3.3]. If the k-dimensional MDS code has length at least $2k + 1$ then the converse of this statement is also true, see [1, Theorem 6]. In all the examples in which M satisfies the hypothesis of Corollary 11, the dimension is 9. The existence of a $[\![12, 0, 7]\!]_7$ quantum MDS code was already known, see [10].

$\underline{k = 7 \, (q \leq 5)}.$

An exhaustive search reveals that there are no matrices M for which the hypothesis of Corollary 11 is satisfied for $q = 4$.

For $q = 5$, Corollary 11 applies if $x = (\epsilon^{10}, \epsilon^{10}, 1, \epsilon^6, \epsilon^3, \epsilon^6, 1)$, where $\epsilon^2 = \epsilon + 3$.

Thus, there is a $[\![14, 0, 8]\!]_5$ quantum MDS code. This was not previously known.

There are examples for $q = 7$, for example $x = (\epsilon^4, \epsilon^{40}, \epsilon^{45}, 1, 1, \epsilon^{45}, \epsilon^{40})$, where $\epsilon^2 = \epsilon + 4$. Again, as in the case $k = 6$, these are perhaps interesting because they cannot be obtained from truncating a generalised Reed–Solomon code. The existence of a $[\![14, 0, 8]\!]_7$ quantum MDS code was already known, see [10].

$k = 8 \ (q \leq 7)$.

An exhaustive search was too large to perform and no examples were found under the assumption $x_7 = x_6$.

An exhaustive search was too large to perform for $k \geq 9$. However, under the assumption $x_j = x_{k+2-j}$ further exhaustive searches were executed. This is a natural assumption to make since it is equivalent to assuming $H_m = H_{-m}$. In other words, we assume that H_m is a Hermitian surface, for all m. This is equivalent to assuming that M is symmetric.

Observe that under the assumption that M is symmetric we are obliged to restrict our attention to k odd, since $M = (a_{ij})$ contains a submatrix

$$\begin{pmatrix} a_{1r} & a_{1,k+2-r} \\ a_{\frac{1}{2}k+1,r} & a_{\frac{1}{2}k+1,k+2-r} \end{pmatrix} = \begin{pmatrix} x_r & x_r \\ x_{r+\frac{1}{2}k} & x_{r+\frac{1}{2}k} \end{pmatrix},$$

which has zero determinant.

$k = 9 \ (q \leq 8)$.

An exhaustive search for symmetric matrices satisfying the hypothesis of Corollary 11 reveals that there are examples for $q = 5$ and $q = 7$ and none for $q = 8$.

For $q = 5$, we have $x = (1, \epsilon^{14}, \epsilon^{21}, \epsilon^{16}, \epsilon^{17}, \epsilon^{17}, \epsilon^{16}, \epsilon^{21}, \epsilon^{14})$, where $\epsilon^2 = \epsilon + 3$.

For $q = 7$, we have $x = (1, \epsilon^{12}, \epsilon^2, \epsilon^{17}, \epsilon^{13}, \epsilon^{13}, \epsilon^{17}, \epsilon^2, \epsilon^{12})$, where $\epsilon^2 = \epsilon + 4$.

Thus, there is an $[\![18, 0, 10]\!]_5$ and an $[\![18, 0, 10]\!]_7$ quantum MDS code. These were not previously known.

References

1. Ball S., Pepe V.: On varieties defined by large sets of quadrics and their application to error-correcting codes. Discret. Math. **343**, 112007 (2020).
2. Beenker G.J.M.: On double circulant codes. EUT report. WSK, Dept. of Mathematics and Computing Science; Vol. 80-WSK-04. Eindhoven University of Technology, Eindhoven (1980).
3. Carlet C., Mesnager S., Tang C., Qi Y.: Euclidean and Hermitian LCD MDS codes. Des. Codes Cryptogr. **86**, 2605–2618 (2018).
4. Chen B., Ling S., Zhang G.: Application of constacyclic codes to quantum MDS codes. IEEE Trans. Inf. Theory **61**, 1474–1484 (2015).
5. Fang W., Fu F.: Some new constructions of quantum MDS codes. (2018). arXiv:1804.08213vl.
6. Fang W., Fu F.: Two new classes of quantum MDS codes. Finite Fields Appl. **53**, 85–98 (2018).
7. Glynn D.G.: The non-classical 10-arc of $PG(4, 9)$. Discret. Math. **59**, 43–51 (1986).
8. Glynn D.G.: On the construction of arcs using quadrics. Aust. J. Comb. **9**, 3–19 (1994).
9. Grassl M., Gulliver T.A.: On self-dual MDS codes. In: Proc. Int. Symp. Inf. Theory (ISIT), pp. 1954–1957 (2008).
10. Grassl M., Rötteler M.: Quantum MDS codes over small fields. In: Proc. Int. Symp. Inf. Theory (ISIT), pp. 1104–1108 (2015).
11. He X., Xu L., Chen H.: New q-ary quantum MDS codes with distances bigger than $q/2$. Quantum Inf. Process. **15**, 2745–2758 (2016).
12. Hirschfeld J.W.P., Storme L.: The packing problem in statistics, coding theory and finite projective spaces. J. Stat. l Plan. **72**, 355–380 (1998).
13. Huber F., Grassl M.: Quantum codes of maximal distance and highly entangled subspaces. Quantum **4**, 284 (2020).
14. Jin L., Kan H., Wen J.: Quantum MDS codes with relatively large minimum distance from Hermitian self-orthogonal codes. Des. Codes Cryptogr. **84**, 463–471 (2017).
15. 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).

16. Jin L., Xing C.: A construction of new quantum MDS codes. IEEE Trans. Inf. Theory **60**, 2921–2925 (2014).
17. Kai X., Zhu S.: New quantum MDS codes from negacyclic codes. IEEE Trans. Inf. Theory **59**, 1193–1197 (2012).
18. Kai X., Zhu S., Li P.: Constacyclic codes and some new quantum MDS codes. IEEE Trans. Inf. Theory **60**, 2080–2086 (2014).
19. Kestenband B.C.: Unital intersections in finite projective planes. Geom. Dedicata **11**, 107–117 (1981).
20. Ketkar A., Klappenecker A., Kumar S., Sarvepalli P.K.: Nonbinary stabilizer codes over finite fields. IEEE Trans. Inf. Theory **52**, 4892–4914 (2006).
21. Li R., Xu Z.: Construction of $[[n, n − 4, 3]]_q$ quantum MDS codes for odd prime power q. Phys. Rev. A **82**, 052316-1–052316-4 (2010).
22. Li Z., Xing L., Wang X.: Quantum generalized Reed–Solomon codes: unified framework for quantum MDS codes. Phys. Rev. A **77**, 012308-1–012308-4 (2008).
23. MacWilliams F.J., Sloane N.J.A.: The Theory of Error-Correcting Codes. North-Holland, Amsterdam (1977).
24. Rains E.M.: Quantum weight enumerators. IEEE Trans. Inform. Theory **44**, 1388–1394 (1998).
25. Rains E.M.: Nonbinary quantum codes. IEEE Trans. Inform. Theory **45**, 1827–1832 (1999).
26. Shi X., Yue Q., Chang Y.: Some quantum MDS codes with large minimum distance from generalized Reed–Solomon codes. Cryptogr. Commun. **10**, 1165–1182 (2018).
27. Shi X., Yue Q., Wu Y.: New quantum MDS codes with large minimum distance and short length from generalized Reed–Solomon codes. Discret. Math. **342**, 1989–2001 (2019).
28. Shi X., Yue Q., Zhu X.: Construction of some new quantum MDS codes. Finite Fields Appl. **46**, 347–362 (2017).
29. Ventou M., Rigoni C.: Self-dual doubly circulant codes. Discret. Math. **56**, 291–298 (1985).
30. Wang L., Zhu S.: New quantum MDS codes derived from constacyclic codes. Quantum Inf. Process. **14**, 881–889 (2015).
31. Yan H.: A note on the construction of MDS self-dual codes. Cryptogr. Commun. **11**, 259–268 (2019).
32. Zhang G., Chen B.: New quantum MDS codes. Int. J. Quantum Inf. **12**, 1450019-1–1450019-10 (2014).
33. Zhang T., Ge G.: Quantum MDS codes with large minimum distance. Des. Codes Cryptogr. **83**, 503–517 (2017).