Quantum Inf Process (2016) 15:2745–2758
DOI 10.1007/s11128-016-1311-2

New q-ary quantum MDS codes with distances bigger than $\frac{q}{2}$

Xianmang He[1] · Liqing Xu[2] · Hao Chen[2]

Received: 19 November 2015 / Accepted: 1 April 2016 / Published online: 18 April 2016

Abstract The construction of quantum MDS codes has been studied by many authors. We refer to the table in page 1482 of (IEEE Trans Inf Theory 61(3):1474–1484, 2015) for known constructions. However, there have been constructed only a few q-ary quantum MDS $[[n, n-2d+2, d]]_q$ codes with minimum distances $d > \frac{q}{2}$ for sparse lengths $n > q+1$. In the case $n = \frac{q^2-1}{m}$ where $m|q+1$ or $m|q-1$ there are complete results. In the case $n = \frac{q^2-1}{m}$ while $m|q^2-1$ is neither a factor of $q-1$ nor $q+1$, no q-ary quantum MDS code with $d > \frac{q}{2}$ has been constructed. In this paper we propose a direct approach to construct Hermitian self-orthogonal codes over $\mathbf{F}_{q^2}$. Then we give some new q-ary quantum codes in this case. Moreover many new q-ary quantum MDS codes with lengths of the form $\frac{w(q^2-1)}{u}$ and minimum distances $d > \frac{q}{2}$ are presented.

Keywords Quantum MDS code · Hermitian self-orthogonal code · Generalized Reed–Solomon code

X. He was supported by NSFC Grant 61202007; L. Xu and H. Chen were supported by NSFC Grants 11371138 and 11531002.

✉ Hao Chen
haochen@hdu.edu.cn

Xianmang He
hexianmang@nbu.edu.cn

Liqing Xu
lqxu@hdu.edu.cn

[1] School of Information Science and Technology, Ningbo University, Ningbo 315211, Zhejiang Province, China

[2] The Department of Mathematics, School of Sciences, Hangzhou Dianzi University, Hangzhou 310018, Zhejiang Province, China

1 Introduction

Quantum error-correcting codes are important for quantum information processing and quantum computation. The construction of quantum error-correcting codes has been an active field of quantum information theory since the publication of [15,19,20]. It is known for any pure quantum $[[n, k, d]]_q$ code the parameters satisfy the quantum singleton bound $k \leq n - 2d + 2$. The q-ary quantum codes reaching this bound are called quantum MDS codes [2,14,15]. Many constructions of q-ary quantum MDS codes have been proposed based on the Hermitian self-orthogonal codes over $\mathbf{F}_{q^2}$.

The Hermitian inner product over $\mathbf{F}_{q^2}^n$ is defined as follows. $< \mathbf{u}, \mathbf{v} >_h = u_1 v_1^q + \cdots + u_n v_n^q$, where $\mathbf{u} = (u_1, \ldots, u_n)$ and $\mathbf{v} = (v_1, \ldots, v_n)$ are vectors in $\mathbf{F}_{q^2}^n$. The following result gives a construction of q-ary quantum MDS codes from Hermitian self-orthogonal MDS codes over $\mathbf{F}_{q^2}$.

Theorem 1.1 ([2]) *If* $\mathbf{C}$ *is a* $[n, k, n-k+1]_{q^2}$ *MDS code over* $\mathbf{F}_{q^2}$ *which is orthogonal under the Hermitian inner product. Then we have a* q*-ary quantum MDS* $[[n, n - 2k, k + 1]]_q$ *code.*

There have been published many papers on the construction of quantum MDS codes [1,2,4–17]. They were constructed from generalized Reed–Solomon codes [8–10], cyclic or constacyclic codes [3,7,11,12]. However, it seems that for many lengths $q + 1 < n < q^2 - 1$ whether there is a q-ary quantum MDS code with length n and minimum distance $d > \frac{q}{2}$ is still an un-solved problem. For only very few sparse lengths such q-ary quantum MDS codes with $d > \frac{q}{2}$ have been constructed [3,7–12,21]. In the case of length $n = \frac{q^2-1}{m}$ where m is an integer satisfying $m|q + 1$ or $m|q - 1$ the following results have been proved ([3,13,21], or see lines 13, 14 and 20 in the table of page 1482 of [3]).

1. For odd prime powers $q = 2^e s + 1$ where s is odd, an odd factor $\lambda|s$ of s and $f \leq e - 1$, a quantum MDS $[[2^f \lambda(q + 1), 2^f \lambda(q + 1) - 2d + 2, d]]_q$ code with minimum distance d for each integer d in the range $2 \leq d \leq \frac{q+1}{2} + 2^f \lambda$ was constructed ([3] Theorem 4.11).
2. In the case $m|q+1$ and m odd there is a q-ary quantum MDS code with length $\frac{q^2-1}{m}$ and minimum distance d for each integer d in the range $2 \leq d \leq \frac{q+1}{2} + \frac{q+1}{2m} - 1$. In the case $m|q + 1$ and m even there is a q-ary quantum MDS code with length $\frac{q^2-1}{m}$ and minimum distance d for each integer d in the range $2 \leq d \leq \frac{q+1}{2} + \frac{q+1}{m} - 1$ (see [3,21]).

However, in the case $n = \frac{q^2-1}{m}$ where $m|q^2 - 1$ is neither a factor of $q - 1$ nor $q + 1$, no q-ary quantum MDS code with length $\frac{q^2-1}{m}$ and minimum distance $d > \frac{q}{2}$ has been constructed. Though in this case each cyclotomic set has only one element, the technique in [3,8,12,13] is not sufficient to get the desirable q-ary quantum MDS codes. In this paper some new q-ary quantum MDS codes in this case with minimum distance $d > \frac{q}{2}$ are constructed. We use a direct approach of constructing Hermitian self-orthogonal MDS codes over $\mathbf{F}_{q^2}$. Many new q-ary quantum MDS codes for the length $n = \frac{w(q^2-1)}{u}$ and $d > \frac{q}{2}$ for some integers w and u are also presented.

We need the following lemmas in this paper.

Lemma 1.1 *If θ is a primitive element of the multiplicative group $\mathbf{F}_{q^2}^*$ and suppose m is a factor of q^2-1, then $\Sigma_{j=1}^{\frac{q^2-1}{m}}\theta^{jtm}=0$ except the case that t is divisible by $\frac{q^2-1}{m}$.*

Proof For any $1 \leq t \leq \frac{q^2-1}{m}-1$, θ^{mt} generates a subgroup G of the group $\mathbf{Z}/(\frac{q^2-1}{m})\mathbf{Z}$ generated by θ^m. The order of the group G is $\frac{\frac{q^2-1}{m}}{gcd(t,\frac{q^2-1}{m})} > 1$. Since $G \neq \{1\}$, for any non-unit element θ^{mt}, $\theta^{mt}G = G$. Thus $\theta^{mt}\Sigma_{j=1}^{\frac{q^2-1}{m}}\theta^{mtj} = \Sigma_{j=1}^{\frac{q^2-1}{m}}\theta^{mtj}$. It is clear $\theta^{mt} \neq 1$ when t is not divisible by $\frac{q^2-1}{m}$. The conclusion follows directly. □

Lemma 1.2 *Suppose $v_1,\ldots,v_n$ are n nonzero elements in the multiplicative group $\mathbf{F}_q^*$. If $\mathbf{g}_l=(g_{1l},\ldots,g_{nl})$ where $l=1,\ldots,k$, are k linear independent rows in $\mathbf{F}_{q^2}^n$ satisfying that $\Sigma_{j=1}^n v_j g_{jl_1} g_{jl_2}^q = 0$ for any two indices l_1 and l_2 in the set $\{1,\ldots,k\}$ (here $l_1 = l_2$ is possible). Then we have a Hermitian self-orthogonal $[n,k]_{q^2}$ code generated by these k rows.*

Proof We can set $v_j = (v_j')^{q+1}$ for $j=1,\ldots,n$. Thus the equivalent code $(v_1',\ldots,v_n')\mathbf{C}$ is a Hermitian self-orthogonal code, where $\mathbf{C}$ is a q^2-ary code generated by these k rows $\mathbf{g}_1,\ldots,\mathbf{g}_k$.

The main idea to construct Hermitian self-orthogonal codes in this paper is as follows. It is well known that from Lemma 1.1 we can prove that the dual of a Reed–Solomon code (evaluation vectors of all polynomials with degrees less than k at a subset $\mathbf{S}$ of $\mathbf{F}_{q^2}$) is another Reed–Solomon code (evaluation vectors of all polynomials with degrees less than $|\mathbf{S}|-k$ at this subset $\mathbf{S}$ of $\mathbf{F}_{q^2}$) (see [18]). Hence we only need to guarantee the condition of Lemma 1.1 is satisfied so that Hermitian self-orthogonal MDS codes can be constructed. There are q-th powers in the Hermitian inner product $\Sigma_{i=1}^n u_i v_i^q$. For the purpose to enlarge dimensions of constructed Hermitian self-orthogonal MDS codes, we need some number theoretical conditions on the lengths to guarantee that the exponential sums in the Hermitian inner products are zero. Then q-ary quantum MDS codes with minimum distances bigger than $\frac{q}{2}$ can be constructed. □

2 New quantum MDS codes I

2.1 Construction 1

Let m be a factor of q^2-1. For any fixed positive integer w we define a length $\frac{q^2-1}{m}$ linear error code over $\mathbf{F}_{q^2}$ as follows.

$$\mathbf{C}_w = \{(\theta^m f(\theta^m), \theta^{2m} f(\theta^{2m}), \ldots, \theta^{jm} f(\theta^{jm}), \ldots,$$
$$\theta^{(\frac{q^2-1}{m}-1)m} f(\theta^{(\frac{q^2}{m}-1)m}), f(1)) : f \in \mathbf{F}_{q^2}[x], \deg(f) \leq w-1\}$$

It is clear that $\mathbf{C}_w$ is a MDS $[\frac{q^2-1}{m}, w, \frac{q^2-1}{m} - w + 1]$ code over $\mathbf{F}_{q^2}$. Actually this code is equivalent to a evaluation code at the elements $\theta^m, \theta^{2m}, \ldots, \theta^{(\frac{q^2-1}{m}-1)m}, 1$. Hence it is equivalent to a Reed–Solomon code.

The Hermitian inner product of any two codewords (corresponding to two polynomials f and g) is $\Sigma_{j=1}^{\frac{q^2-1}{m}} \theta^{jm+jqm} f g^q(\theta^{jm})$. Thus we only need to check

$$\Sigma_{j=1}^{\frac{q^2-1}{m}} \theta^{(q+1)mj} \theta^{jm(t_1+t_2q)} = \Sigma_{j=1}^{\frac{q^2-1}{m}} \theta^{jm(q+1+t_1+t_2q)} = 0,$$

where $0 \leq t_1, t_2 \leq w - 1$.

Theorem 2.1 *If $m = 2k+1$ is an odd positive factor of $q+1$ and $w < \frac{k+1}{2k+1}(q-1)$, then for all non-negative integers t_1 and t_2 satisfying $0 \leq t_1, t_2 \leq w-1$, $q+1+t_1+t_2q$ is not divisible by $\frac{q^2-1}{m}$. Hence the code $\mathbf{C}_w$ is Hermitian self-orthogonal.*

Proof It is clear that if $\Sigma_{j=1}^{\frac{q^2-1}{m}} \theta^{jm(q+1+t_1+t_2q)} = 0$ for all t_1 and t_2 satisfying $0 \leq t_1, t_2 \leq w-1$, the code is Hermitian self-orthogonal. Hence from Lemma 1.1 it is sufficient to prove that if $w < \frac{k+1}{2k+1}(q-1)$, $q+1+t_1+t_2q$, where $t_1 < w, t_2 < w$, is not divisible by $\frac{q^2-1}{m}$. Since $q+1+t_1+t_2q \leq (q+1)(1+w-1) < (k+1)\frac{q^2-1}{m}$, if $q+1+t_1+t_2q$ is divisible by $\frac{q^2-1}{m}$, the quotient $\frac{q+1+t_1+t_2q}{\frac{q^2-1}{m}} \leq k$. On the other hand $\frac{q^2-1}{m} = \frac{q+1}{m}q - \frac{q+1}{m}$. That is, $\frac{q^2-1}{m} \equiv q - \frac{q+1}{m}$ *mod* q because $\frac{q+1}{m}$ is an integer. Therefore, if $q+1+t_1+t_2q$ is divisible by $\frac{q^2-1}{m}$, then residue of $q+1+t_1+t_2q$ module q is in the range $[\frac{k+1}{m}(q+1)-1, q-1]$. It is obvious that the residue of $q+t_2q+1+t_1$ module q is $1+t_1 \leq w < \frac{k+1}{2k+1}(q-1)$. Since $\frac{k+1}{m}(q+1)$ is a positive integer and $\frac{k+1}{m}(q-1) = \frac{k+1}{m}(q+1) - 1 - \frac{1}{m} < \frac{k+1}{m}(q+1)$, the conclusion follows directly. □

Corollary 2.1 *If $m = 2k+1$ is an odd factor of $q+1$, for each positive integer d in the range $2 \leq d \leq \lfloor \frac{k+1}{2k+1}(q-1)+1 \rfloor$, there exists a q-ary quantum MDS code with length $\frac{q^2-1}{m}$ and minimum distance d.*

Suppose q is a prime power and $q+1 = \lambda r$ where r is an odd integer, then for each integer d in the range $2 \leq d \leq \frac{q-1}{2} + \frac{\lambda}{2}$, a length $\lambda(q-1)$ q-ary quantum MDS code with the minimum distance d was constructed in [3,12,13,21]. Its construction was based on constacyclic codes over $\mathbf{F}_{q^2}$. However, this kind of quantum q-ary MDS codes is a direct consequence from the constructed quantum MDS codes in Corollary 2.1.

We can extend the construction 1 to $[\frac{q^2-1}{m}+1, w+1, \frac{q^2-1}{m} - w + 1]$ Hermitian self-orthogonal code over $\mathbf{F}_{q^2}$ with the following generator matrix.

Table 1 $[[\frac{q^2+m-1}{m}, \frac{q^2+m-1}{m} - 2d, d+1]]_q$ quantum MDS codes

Quantum MDS code	q, m, d
$[[33, 15, 10]]_{17}$	17, 9, 9
$[[73, 51, 12]]_{19}$	19, 5, 11
$[[57, 27, 16]]_{29}$	29, 15, 15
$[[73, 35, 20]]_{37}$	37, 19, 19
$[[81, 41, 21]]_{41}$	41, 21, 20
$[[169, 125, 23]]_{43}$	43,11, 22
$[[105, 53, 27]]_{53}$	53, 27, 26

$$\begin{pmatrix} \frac{q+1}{m} & 1 & \cdots & 1 & 1 \\ 0 & \theta^{m} & \cdots & \theta^{\left(\frac{q^2-1}{m}-2\right)m} & \theta^{\frac{q^2-1}{m}m} = 1 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \theta^{im} & \cdots & \theta^{\left(\frac{q^2-1}{m}-2\right)im} & 1 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \theta^{wm} & \cdots & \theta^{\left(\frac{q^2-1}{m}-2\right)wm} & 1 \end{pmatrix}$$

Therefore, the following result which can be thought as a generalization of Theorem 4.4 of [11] is proved.

Theorem 2.2 *For each odd number $m = 2k+1$ satisfying $m|q+1$, we have a $[[\frac{q^2+m-1}{m}, \frac{q^2+m-1}{m} - 2d, d+1]]_q$ quantum MDS code for each integer d in the range $2 \le d \le \lfloor \frac{k+1}{2k+1}(q-1)+1 \rfloor$.*

In the case $q+1$ is divisible by 3 we have a length $\frac{q^2-1}{3}+1 = \frac{q^2+2}{3}$ q-ary quantum MDS code with minimum distance d for each integer d in the range $2 \le d \le \frac{2(q+1)}{3}$. This recovers the 2nd conclusion of Theorem 4.4 of [10]. Moreover if $5|q+1$, then we have a length $\frac{q^2-1}{5}+1 = \frac{q^2+4}{5}$ q-ary quantum MDS code with the minimum distance d for each integer d in the range $2 \le d \le \frac{3(q+1)}{5}$. We list some new quantum MDS codes from Theorem 2.2 in Table 1.

2.2 Construction 2

We need the following two lemmas in construction 2. The main idea of the construction 2 is the consideration of the sum of two identities as in Lemma 1.1 with respect to two subsets. Then we have new identities that some exponential sums at a new subset are zero. This leads to some new Hermitian self-orthogonal codes with different lengths.

Lemma 2.1 *Suppose q is an even prime power 2^h. Let $\theta \in \mathbf{F}_{q^2}$ be a primitive element which generate the multiplicative group $\mathbf{F}_{q^2}^*$. If m_1 and m_2 are factors of q^2-1*

satisfying $\gcd(m_1, m_2) = 1$. *We set* $m_3 = \frac{q^2-1}{m_1}$ *and* $m_4 = \frac{q^2-1}{m_2}$. *Let* $\mathbf{M}_1$ *be the set of all indices* j *satisfying* $1 \le j \le m_3 - 1$ *and* j *is not divisible by* m_2, *and* $\mathbf{M}_2$ *be the set of all indices* j *satisfying* $1 \le j \le m_4 - 1$ *and* j *is not divisible by* m_1. *Then* $\Sigma_{j\in\mathbf{M}_1}\theta^{m_1tj} + \Sigma_{j\in\mathbf{M}_2}\theta^{m_2tj} = 0$ *for* $t = 1, \ldots, min\{m_3, m_4\} - 1$.

Proof From Lemma 1.1 and the fact $-1 = 1$ in the finite field $\mathbf{F}_{2^{2h}}$ we get the conclusion. Here we should note that in the two equalities $\Sigma_{j=1}^{m_3}\theta^{m_1tj} = 0$ and $\Sigma_{j=1}^{m_4}\theta^{m_2tj} = 0$. The common part is $\Sigma_{j=1}^{m_5}\theta^{m_1m_2tj}$, where $m_5 = \frac{q^2-1}{m_1m_2}$. □

Here $|\mathbf{M}_1| = m_3 - \frac{q^2-1}{m_1m_2}$ and $|\mathbf{M}_2| = m_4 - \frac{q^2-1}{m_1m_2}$.

Similarly we have the following Lemma 2.2. Suppose q is an even prime power 2^h. Let $\theta \in \mathbf{F}_{q^2}$ be a primitive element which generate the multiplicative group $\mathbf{F}_{q^2}^*$. Consider $m_1, \ldots, m_s$ factors of $q^2 - 1$ satisfying $\gcd(m_{s_1}, m_{s_2}) = 1$ for any $s_1 \neq s_2$. We set $m_1' = \frac{q^2-1}{m_1}, \ldots, m_s' = \frac{q^2-1}{m_s}$. Set $\mathbf{M}_u$ the subgroup of the multiplicative group $\mathbf{F}_{q^2}^*$ generated by θ^{m_u}. Let $\mathbf{M}_{s_1,\ldots,s_l}$ be the intersection of $\mathbf{M}_{s_1}, \ldots, \mathbf{M}_{s_l}$ for distinct indices $s_1, \ldots, s_l$ in the set $\{1, \ldots, s\}$. The set $\mathbf{M}$ is defined as the set of elements in $\mathbf{M}_1 \cup \cdots \cup \mathbf{M}_s$ by deleting these elements in the set $\mathbf{M}_{s_1,\ldots,s_l}$ where l is even. The elements in $\mathbf{M}_{s_1,\ldots,s_{l'}}$ where l' is odd are remained.

Lemma 2.2 $\Sigma_{j\in\mathbf{M}\cap\mathbf{M}_1}\theta^{m_1tj} + \Sigma_{j\in\mathbf{M}_2\cap\mathbf{M}}\theta^{jm_2t} + \cdots + \Sigma_{j\in\mathbf{M}\cap\mathbf{M}_s}\theta^{jm_2t} = 0$ *for* $t = 1, \ldots, min\{m_1', \ldots, m_s'\} - 1$.

If q be an even prime power 2^h, $m_1 = 2k_1 + 1 < m_2 = 2k_2 + 1$ are odd factors of $q + 1$ satisfying $\gcd(m_1, m_2) = 1$. Set $m_3 = \frac{q^2-1}{m_1}$, $m_4 = \frac{q^2-1}{m_2}$, $M = m_3 + m_4 - \frac{2(q^2-1)}{m_1m_2}$. We construct a length M linear code $\mathbf{C_M}$ over $\mathbf{F}_{q^2}$ as follows. $\mathbf{C_M} = \{(xf(x))_{x\in\mathbf{M}} : 0 \le \deg(f) \le w - 1\}$, where $w < \frac{k_2+1}{2k_2+1}(q-1)$. This is equivalent to a evaluation code (a Reed–Solomon code) at all elements of the set $\mathbf{M}$. Thus this is a $[M, w, M - w + 1]$ MDS code over $\mathbf{F}_{q^2}$.

We need to check the exponential sum $\Sigma_{j\in\mathbf{M}_1}\theta^{jm_1(q+1+t_1+t_2q)} + \Sigma_{j\in\mathbf{M}_2}\theta^{jm_2(q+1+t_1+t_2q)}$ for the purpose to get the Hermitian self-orthogonal codes.

Theorem 2.3 *Let* m_1, m_2, m_3, m_4, M *and* w *be positive integers as above. If for all non-negative integers* t_1 *and* t_2 *satisfying* $0 \le t_1, t_2 \le w - 1$, $q + 1 + t_1 + t_2q$ *cannot be divisible by* m_3 *and* m_4, *then the code* $\mathbf{C_M}$ *is Hermitian self-orthogonal. When* $w < \frac{k_2+1}{2k_2+1}(q-1)$, *the above condition is satisfied.*

Proof The conclusion follows from the proof of Theorem 2.1 and the fact $w < min\{\frac{k_1+1}{2k_1+1}(q-1), \frac{k_2+1}{2k_2+1}(q-1)\}$. □

Corollary 2.2 *Suppose that* q *is an even prime power* 2^h, $m_1 = 2k_1 + 1$ *and* $m_2 = 2k_2 + 1$ *are odd positive integers satisfying* $\gcd(m_1, m_2) = 1$, $m_1 < m_2$ *and* $m_1|q + 1$, $m_2|q + 1$. *We set* $m_3 = \frac{q^2-1}{m_1}$, $m_4 = \frac{q^2-1}{m_2}$, $M = m_3 + m_4 - \frac{2(q^2-1)}{m_1m_2}$. *For each positive integer* d *in the range* $2 \le d \le \lfloor\frac{k_2+1}{2k_2+1}(q-1) + 1\rfloor$, *there is a length* M q*-ary quantum MDS code with minimum distance* d.

Table 2 $[[(m_1+m_2-2)(2^h-1), (m_1+m_2-2)(2^h-1)-2k, k+1]]_{2^h}$ quantum MDS codes

Quantum MDS code	h, m_1, m_2, k
$[[372, 340, 17]]_{32}$	5, 3,11, 16
$[[1008, 942, 34]]_{64}$	6, 5, 13, 32
$[[5588, 5460, 65]]_{128}$	7, 3, 43, 64
$[n[22484, 21956, 265]]_{512}$	9, 19, 27, 264

Table 3 $[[\frac{q^2-1}{m_1}+\frac{q^2-1}{m_2}-\frac{q^2-1}{m_1m_2}, \frac{q^2-1}{m_1}+\frac{q^2-1}{m_2}-\frac{q^2-1}{m_1m_2}-2k, k+1]]_q$ quantum MDS codes

Quantum MDS code	q, m_1, m_2, k
$[[412, 412-2k, k+1]]_{29}$	29, 3,5, $1 \le k \le 16$
$[[720, 720-2k, k+1]]_{41}$	41, 3, 7, $1 \le k \le 22$
$[[1624, 1624-2k, k+1]]_{59}$	59, 3, 5, $1 \le k \le 34$
$[[2952, 2952-2k, k+1]]_{83}$	83, 3,7, $1 \le k \le 46$

From Lemma 2.2 we can generalize our recent results to the case that $q+1$ has several factors $m_1, \ldots m_s$, where $\gcd(m_{s_1}, m_{s_2}) = 1$ for $s_1 \neq s_2$. Some quantum MDS codes coming from Corollary 2.2 are listed in Table 2.

Actually in the case q is an odd prime power we can use equivalent codes to get new quantum MDS codes as follows. If q is an odd prime power, then 2 is a nonzero element in $\mathbf{F}_q \subset \mathbf{F}_{q^2}$. If $m_1 = 2k_1+1 < m_2 = 2k_2+1$ are two odd factors of $q+1$, then we have the following identity. When t is not divisible by $\frac{q^2-1}{m_1}$ or $\frac{q^2-1}{m_2}$,

$$\Sigma_{j=1}^{\frac{q^2-1}{m_1}} \theta^{m_1 tj} + \Sigma_{j=1}^{\frac{q^2-1}{m_2}} \theta^{m_2 jt} = 0$$

For those indices j's which are in both summands, that is, $j = m_1 m_2 j'$, we have $2\theta^{m_1 m_2 t j'}$ in the above identity. Since $2 = u^{q+1}$ for some $u \in \mathbf{F}_{q^2}$, the equivalent code can be used to get a Hermitian orthogonal code from Lemma 1.2. Hence we have the following result.

Theorem 2.4 *Suppose that q is an odd prime power, $m_1 = 2k_1+1$ and $m_2 = 2k_2+1$ are odd positive integers satisfying* $\gcd(m_1, m_2) = 1$, *$m_1 < m_2$ and $m_1|q+1$, $m_2|q+1$. We set $m_3 = \frac{q^2-1}{m_1}$, $m_4 = \frac{q^2-1}{m_2}$, $M = m_3 + m_4 - \frac{q^2-1}{m_1 m_2}$. For each positive integer d in the range $2 \le d \le \lfloor \frac{k_2+1}{2k_2+1}(q-1)+1 \rfloor$, there is a length M q-ary quantum MDS code with minimum distance d.*

In Table 3 we give some new quantum MDS q-ary codes from Theorem 2.4.

3 New quantum codes II

3.1 Odd q and even $m|q-1$ (Recovery of Theorem 4.11 in [3])

Suppose q is an odd prime power and $q-1 = 2^h a_1 a_2$ where a_1 and a_2 are odd numbers. We assume $m = 2^{h_1} a_1 \ge 6$ is an even factor of $q-1$ where $h_1 \le h$. We first prove the following lemma.

Table 4 $[[(m_1+m_2-1)(2m_1m_2+2), (m_1+m_2-1)(2m_1m_2+2)-2d+2, d]]_q$ quantum MDS codes

Quantum MDS code	q, m_1, m_2, d
$[[224, 224-2d+2, d]]_{29}$	$31, 3, 5, 2 \le d \le 17$
$[[396, 396-2d+2, d]]_{41}$	$43, 3, 7, 2 \le d \le 25$
$[[884, 884-2d+2, d]]_{67}$	$67, 3, 11, 2 \le d \le 37$
$[[792, 792-2d+2, d]]_{71}$	$71, 5, 7, 2 \le d \le 41$
$[[1196, 1196-2d+2, d]]_{91}$	$91, 5, 9, 2 \le d \le 51$

Lemma 3.1 *When* $0 \le t_1, t_2 \le \frac{q+1}{2} + 2^{h-h_1}a_2 - 2$, *the following equality holds:*

$$\Sigma_{j=1}^{\frac{q^2-1}{m}} \theta^{jm(t_1+t_2q+\frac{q+1}{2})} = 0$$

Proof From the condition $m \ge 6$, $t_1 + t_2q + \frac{q+1}{2} < q^2 - 1$. Thus if $(t_1 + \frac{q+1}{2}) + t_2q$ is divisible by $\frac{q^2-1}{m}$, the quotient $u < m$. In the case $t_1 + \frac{q+1}{2} \le q - 1$ we have $u\frac{q^2-1}{m} = t_2q + t_1 + \frac{q+1}{2}$. The quotient is t_2 and the remainder is $t_1 + \frac{q+1}{2}$. The quotient and the remainder have to be the same since $u(\frac{q-1}{m})$ is an integer.

Since $t_1 + \frac{q+1}{2} = t_2$ is divisible by $\frac{q-1}{m}$, $t_1 + 1 + \frac{q-1}{2}$ is divisible by $\frac{q-1}{m} = 2^{h-h_1}a_2$. From $t_1 \ge 0$ we have $t_1 + 1 \ge 1$, and $t_1 \ge 2^{h-h_1}a_2 - 1$. On the other hand $t_2 = t_1 + \frac{q+1}{2}$, $t_2 \ge \frac{q+1}{2} + 2^{h-h_1}a_2 - 1$. This is a contradiction. Thus $t_1 + t_2q + \frac{q^2-1}{2^{h-h_1+1}m}$ is not divisible by $\frac{q^2-1}{m}$.

In the case $t_1 + \frac{q+1}{2} \ge q$ we have $u\frac{q^2-1}{m} = (t_2+1)q + (t_1 - \frac{q-1}{2})$. The quotient is $t_2 + 1$ and the remainder is $t_1 - \frac{q-1}{2}$. These two numbers have to be the same since $u < m$. Thus $t_2 + 1 = t_1 - \frac{q-1}{2}$ is divisible by $\frac{q-1}{m} = 2^{h-h_1}a_2$. From $t_2 + 1 \ge 1$, we have $t_2 \ge 2^{h-h_1}a_2 - 1$. Thus $t_1 \ge t_2 + 1 + \frac{q-1}{2} \ge \frac{q+1}{2} + 2^{h-h_1}a_2 - 1$. This is a contradiction.

The code is the set $\{(f(\theta^{ml}), f(\theta^{2ml}), \ldots, f(\theta^{jml}), \ldots, f(\theta^{\frac{q^2-1}{m}ml}) : \deg(f) < k\}$. In Lemma 1.2 we can set $v'_j = \theta^{j\frac{m(q+1)}{2}} \in \mathbf{F}_q^*$. $\mathbf{g}_l = (\theta^{ml}, \theta^{2ml}, \ldots, \theta^{jml}, \ldots, \theta^{\frac{q^2-1}{m}ml})$, where $0 \le l \le k-1$. Thus a $[\frac{q^2-1}{m}, k]_{q^2}$ Hermitian self-orthogonal MDS code can be constructed from Lemmas 1.2 and 3.1, where k is in the range $1 \le k \le \frac{q+1}{2} + 2^{h-h_1}a_2 - 1$. From Theorem 1.1 we have a length $\frac{q^2-1}{m}$ quantum MDS q-ary code with the minimum distance $d = k+1$ in the range $2 \le d \le \frac{q+1}{2} + 2^{h-h_1}a_2$. □

Theorem 3.1 *If* $q = 2^h a_1 a_2 + 1$ *is an odd prime power where* a_1 *and* a_2 *are odd numbers and* $m = 2^{h_1}a_1 \ge 6$ *is an even factor of* $q-1$ *where* $h_1 \le h$, *then for each integer* d *in the range* $2 \le d \le \frac{q+1}{2} + 2^{h-h_1}a_2$, *we have a* q*-ary quantum MDS code with length* $\frac{q^2-1}{m}$ *and minimum distance* d.

This recovers Theorem 4.11 in [3].

3.2 Length $\frac{w(q^2-1)}{u}$ quantum q-ary MDS codes

The main idea of the construction in this subsection is similar to the Sect. 2.2. We add some identities in Lemma 3.1 to get some new identities that some exponential sums are zero. Thus we can construct some new Hermitian self-orthogonal codes.

Suppose $m_1 = 2^{h_1}a_1 \geq 6$ and $m_2 = 2^{h_2}b_1 \geq 6$ are two even factors of $q-1 = 2^h a_1 a_2 = 2^h b_1 b_2$ where a_1, a_2, b_1, b_2 are odd numbers. Then we have two identities from Lemma 3.1. The addition of these two identities gives another identity. For those indices j which are divisible by both m_1 and m_2, we have to use the element $\theta^{j\frac{m_1(q+1)}{2}} + \theta^{j\frac{m_2(q+1)}{2}} \in \mathbf{F}_q$. It is obvious that this is a nonzero element in $\mathbf{F}_q^*$ when $lcm(m_1, m_2) = q-1$ (here lcm is the least common multiple). Set $\mathbf{M}_1$ the set of indices $m_1 \cdot \{1, \ldots, \frac{q^2-1}{m_1}\}$ and $\mathbf{M}_2 = m_2 \cdot \{1, \ldots, \frac{q^2-1}{m_2}\}$, $\mathbf{M} = \mathbf{M}_1 \cup \mathbf{M}_2$. Here $|\mathbf{M}| = |\mathbf{M}_1| + |\mathbf{M}_2| - \frac{q-1}{lcm(m_1,m_2)}(q+1) = \frac{q^2-1}{m_1} + \frac{q^2-1}{m_2} - (q+1)$ when $lcm(m_1, m_2) = q-1$. The code is the set $\{(f(x))_{x\in\mathbf{M}} : 0 \leq \deg(f) \leq k-1\}$, where $1 \leq k \leq \frac{q-1}{2} + \min\{2^{h-h_1}a_2, 2^{h-h_2}b_2\}$.

Theorem 3.2 *Assuming that $q = 2^{h_1}a_1a_2 + 1 = 2^{h_2}b_1b_2 + 1$ is an odd prime power as above and a_1, a_2, b_1, b_2 are odd numbers. Suppose also that $m_1 = 2^{h_1}a_1$ and $m_2 = 2^{h_2}b_1$ are two even factors of $q-1$ satisfying $lcm(m_1, m_2) = q-1$ as above. Then for each integer d in the range $2 \leq d \leq \frac{q+1}{2} + min\{2^{h-h_1}a_2, 2^{h-h_2}b_2\}$ we have a q-ary quantum MDS code with length $|\mathbf{M}| = \frac{q^2-1}{m_1} + \frac{q^2-1}{m_2} - (q+1)$ and minimum distance d.*

Corollary 3.1 *If $2m_1m_2 + 1$ is a prime power where $m_1 < m_2$ are two co-prime odd numbers, then for each integer d in the range $2 \leq d \leq m_1m_2 + m_1 + 1$ we have a length $\frac{(m_1+m_2-1)(q^2-1)}{2m_1m_2} = (m_1 + m_2 - 1)(2m_1m_2 + 2)$ q-ary quantum MDS code and the minimum distance d.*

We list some new quantum MDS codes from Corollary 3.1 in Table 4.

4 New quantum codes III

Just as in Sect. 2.2 the idea of the construction in this section is that the addition of two identities in Lemmas 1.1 and 3.1 gives us some new identities showing that some exponential sums are zero. This leads to some new Hermitian self-orthogonal codes with different lengths.

Let q be an odd prime power and $m_1 = 2k_1 + 1$ is an odd factor of $q+1$. From Theorem 2.1 we have that the following identity holds when $0 \leq t_1, t_2 \leq \frac{q-1}{2} + \frac{q+1}{2m_1} - 2$.

$$\Sigma_{j=1}^{\frac{q^2-1}{m_1}} \theta^{jm_1(t_1+t_2q)} \cdot \theta^{jm_1(q+1)} = 0$$

From Lemma 3.1 if $m_2|q-1$ is an even factor of $q-1$ we have the following identity when $0 \le t_1, t_2 \le \frac{q-1}{2} + \frac{q-1}{m_2} - 1$.

$$\Sigma_{j=1}^{\frac{q^2-1}{m_2}} \theta^{jm_2(t_1+t_2q)} \cdot \theta^{j\frac{m_2(q+1)}{2}} = 0$$

We can get the following identity by adding these two identities.

$$\Sigma_{j=1}^{\frac{q^2-1}{m_1}} \theta^{jm_1(t_1+t_2q)} \cdot \theta^{jm_1(q+1)} + H(\Sigma_{j=1}^{\frac{q^2-1}{m_2}} \theta^{jm_2(t_1+t_2q)} \cdot \theta^{j\frac{m_2(q+1)}{2}}) = 0$$

Here H can be any nonzero $H \in \mathbf{F}_q^*$ and the common t_1 and t_2 are in the range $0 \le t_1, t_2 \le \frac{q-1}{2} + min\{\frac{q+1}{2m_1} - 2, \frac{q-1}{m_2} - 1\}$. At the position $\theta^{m_1m_2t}$ it is clear that $\theta^{m_1^2m_2t(q+1)} + H\theta^{\frac{m_1m_2^2t(q+1)}{2}}$ is an element in $\mathbf{F}_q$. Since $\theta^{(m_1-\frac{m_2}{2})m_1m_2t(q+1)}$ can only be the $\frac{q-1}{m_2}$ nonzero elements in the subgroup of $\mathbf{F}_q^*$ generated by $\theta^{m_2(q+1)}$, there exists a $H \in \mathbf{F}_q^*$ such that $\theta^{m_1^2m_2t(q+1)} + H\theta^{\frac{m_1m_2^2t(q+1)}{2}}$ is a nonzero element in $\mathbf{F}_q^*$ for any possible t.

Let $\mathbf{M}$ be the set $\{\theta^{jm_1} : j = 1, \dots, \frac{q^2-1}{m_1}\} \cup \{\theta^{jm_2} : j = 1, \dots, \frac{q^2-1}{m_2}\}$. The code is the set $\{(f(x))_{x\in\mathbf{M}} : 0 \le \deg(f) \le \frac{q-1}{2} + \min\{\frac{q+1}{2m_1} - 2, \frac{q-1}{m_2} - 1\}\}$. This is equivalent to a Reed–Solomon code.

Theorem 4.1 *If q is an odd prime power, m_1 is an odd factor of $q+1$ and m_2 an even factor of $q-1$, then for each integer d in the range $2 \le d \le \frac{q-1}{2} + \min\{\frac{q+1}{2m_1}, \frac{q-1}{m_2} + 1\}$, we have a q-ary quantum MDS code with length $\frac{q^2-1}{m_1} + \frac{q^2-1}{m_2} - \frac{q^2-1}{m_1m_2}$ and minimum distance d.*

Actually Theorem 4.1 is quite general as illustrated in the following results.

Corollary 4.1 *Let q be an odd prime power. If there exists an odd integer $m|q+1$ such that $m-1$ is an even factor of $q-1$. Then for each integer d in the range $2 \le d \le \frac{q-1}{2} + \frac{q+1}{2m}$ we have a length $\frac{2(q^2-1)}{m}$ q-ary quantum MDS code with minimum distance d.*

There are many such odd prime powers q as illustrated in Table 5.

The lengths of some quantum MDS q-ary codes in Table 5 have the form $4(q-1)$ where q is an odd prime power such that $(q+1)$ is not divisible by 4. This case is not covered in the previous results (see the table in page 1482 of [3]).

Corollary 4.2 *If q is an odd prime power of the form $q \equiv 1 \mod 4$, then for each integer d in the range $2 \le d \le \frac{q+1}{2}$ we have a length $4(q-1)$ q-ary quantum MDS code with minimum distance d.*

From the main result in [9] (or see 3 in the table in page 1482 of [3]), only the range $3 \le d \le \frac{q-1}{2}$ is allowed. Our result gives a quantum q-ary MDS $[[4(q-1), 3q-3, \frac{q+1}{2}]]_q$ code when $q = 4k+1$ is an odd prime power.

Table 5 Quantum MDS codes with lengths $\frac{2(q^2-1)}{m}$

Quantum MDS code	q, m, d
$[[48, 48-2d+2, d]]_{13}$	$13, 7, 2 \leq d \leq 7$
$[[48, 48-2d+2, d]]_{25}$	$17, 9, 2 \leq d \leq 9$
$[[56, 56-2d+2, d]]_{29}$	$29, 15, 2 \leq d \leq 15$
$[[144, 144-2d+2, d]]_{41}$	$37, 19, 2 \leq d \leq 19$
$[[192, 192-2d+2, d]]_{49}$	$49, 25, 2 \leq d \leq 25$
$[[960, 960-2d+2, d]]_{49}$	$49, 5, 2 \leq d \leq 29$
$[[288, 288-2d+2, d]]_{73}$	$73, 37, 2 \leq d \leq 37$
$[[1760, 1760-2d+2, d]]_{89}$	$89, 9, 2 \leq d \leq 49$

Table 6 Quantum MDS codes with lengths $\frac{(q-1)}{2k+1} \cdot (q+1)$

Quantum MDS code	q, k, d
$[[56 \cdot 170, 9520-2d+2, d]]_{169}$	$169, 1, 2 \leq d \leq 101$
$[[96 \cdot 290, 27840-2d+2, d]]_{289}$	$289, 1, 2 \leq d \leq 173$
$[[456 \cdot 1370, 624720-2d+2, d]]_{1369}$	$1369, 1, 2 \leq d \leq 821$
$[[616 \cdot 1850, 1139600-2d+2, d]]_{1849}$	$1849, 1, 2 \leq d \leq 1109$
$[[984 \cdot 6870, 6760080-2d+2, d]]_{6889}$	$6889, 3, 2 \leq d \leq 3709$
$[[672 \cdot 57122, 38385984-2d+2, d]]_{57121}$	$57121, 42, 2 \leq d \leq 28729$
$[[1896 \cdot 24650, 46736400-2d+2, d]]_{24649}$	$24649, 6, 2 \leq d \leq 12817$

Corollary 4.3 *Let q be an odd prime power. If there exists an even factor $2(2k+1)$ of $q-1$ such that $4k+1$ is a odd factor of $q+1$, then for each integer d in the range $2 \leq d \leq \frac{q-1}{2} + \frac{q+1}{2(4k+1)}$ we have a length $\frac{q-1}{2k+1} \cdot (q+1)$ q-ary quantum MDS code with minimum distance d.*

In Theorem 4.11 of [3] and Theorem 3.1 here m cannot be an odd factor. This Corollary 4.3 partially solves this case under an assumption on q. However, there are a lot of such odd prime powers q and odd factors $(2k+1)|q-1$ as illustrated in Table 6.

5 New quantum codes IV

In this section we treat the case that q is an odd prime power and $n = \frac{q^2-1}{m}$, where $m|q^2-1$, and m is neither a factor of $q-1$ nor $q+1$.

We need the following two lemmas.

Lemma 5.1 *If m_1 is an even integer and m_2 is an odd integer satisfying $\gcd(m_1, m_2) = 1$, there are infinitely many primes q satisfying $m_1|q-1$ and $m_2|q+1$.*

Proof Since $gcd(m_1, m_2) = 1$ we have two integers l_0 and k_0 satisfying $l_0 m_1 + 2 = k_0 m_2$. Thus $l = l_0 + m_2 t$ and $k = k_0 + m_1 t$ also satisfy $l m_1 + 2 = k m_2$ for all integers

Table 7 Quantum MDS codes from Theorem 5.1

Quantum MDS code	q, m_1, m_2, d
$[[1088 \cdot 1995, 2170560 - 2d + 2, d]]_{11969}$	$11969, 176, 105, 2 \leq d \leq 6041$
$[[2768 \cdot 5075, 14047600 - 2d + 2, d]]_{30449}$	$30449, 176, 105, 2 \leq d \leq 15369$
$[[7758 \cdot 9310, 72226980 - 2d + 2, d]]_{46549}$	$46549, 36, 175, 2 \leq d \leq 23407$
$[[9858 \cdot 11830, 116620140 - 2d + 2, d]]_{59149}$	$59149, 36, 175, 2 \leq d \leq 29743$

$t = 0 \pm 1, \pm 2, \ldots$. It is clear $\gcd(l_0 m_1 + 1, m_1) = 1$. We have $l_0 m_1 + 1 + 1 = k_0 m_2$, then $\gcd(l_0 m_1 + 1, m_2) = 1$.

From Dirichlet Theorem there are infinitely many primes in the arithmetic sequence $m_2 m_1 t + l_0 m_1 + 1$ because of $\gcd(l_0 m_1 + 1, m_1 m_2) = 1$. It is direct to verify $m_1 | q - 1$ and $m_2 | q + 1$. $\square$

Lemma 5.2 *There are infinitely many pairs of positive integers (m_1, m_2) satisfying the following conditions.*

1) *m_1 is even, m_2 is odd and* $\gcd(m_1, m_2) = 1$*;*
2) $\frac{m_1 + m_2 - 1}{m_1 m_2} = \frac{1}{m}$ *where m is a positive integer satisfying $gcd(m_1, m) > 1$ and $gcd(m_2, m) > 1$.*

Proof We consider $m_2 = k_1 k_2$ where k_1 and k_2 are odd numbers. Set k_3 and k_4 two un-determined positive integers satisfying $k_1 k_2 - 1 + 2k_3 k_4 = k_1 k_3$. Then $k_1 k_2 - 1 = k_3(k_1 - 2k_4)$. From the factorization of $k_1 k_2 - 1$ we get suitable k_3 and k_4. Hence $m_1 = k_1 k_2$ and $m_2 = 2k_3 k_4$ are the integers satisfying the conditions.

For example when $k_1 = 35$ and $k_2 = 3$, $105 - 1 = 8 \cdot 13 = k_3(35 - 2k_4)$, we can set $k_3 = 8$ and $k_4 = 11$. Then $m_1 = 176$ and $m_2 = 105$. $\frac{105 + 176 - 1}{176 \cdot 105} = \frac{1}{66}$. When $k_1 = 35$ and $k_2 = 5$. $174 = 6 \cdot 29 = k_3(35 - 2k_4)$, we can set $k_3 = 6$ and $k_4 = 3$. Then $m_1 = 36$ and $m_2 = 175$. $\frac{175 + 36 - 1}{36 \cdot 175} = \frac{1}{30}$. $\square$

Theorem 5.1 *There are infinitely many pairs of integers (m_1, m_2) as in Lemma 5.2 and infinitely many primes q as in Lemma 5.1 for each such pair (m_1, m_2). For each such pair (m_1, m_2) and the infinitely many primes q as in Lemma 5.1, we have a q-ary quantum MDS code with length $n = \frac{q^2 - 1}{m}$ and minimum distance d for each integer d in the range $2 \leq d \leq \frac{q-1}{2} + \min\{\frac{q+1}{2m_2}, \frac{q-1}{m_1} + 1\}$.*

Proof The conclusion follows from Lemmas 5.1 and 5.2 and Theorem 4.1 directly.

We list some new q-ary quantum MDS codes from Theorem 5.1 in Table 7.

$\square$

Corollary 5.1 *Let k be any positive integer satisfying $k \equiv 5 \bmod 9$. If $q = 16k^2 - 12k + 1$ is an odd prime power, then we have a q-ary quantum MDS code with length $\frac{q^2 - 1}{3k}$ and minimum distance d for each integer d in the range $2 \leq d \leq \frac{q+1}{2} + \frac{2k-1}{3}$.*

Proof Set $m_1 = 4k$ and $m_2 = 3(4k - 1)$ in Theorem 5.1 we get the conclusion.

For example when $k = 14$ and $q = 2969$ is a prime we have a 2969-ary quantum MDS $[[209880, 209880 - 2d + 2, d]]_{2969}$ code for each integer d in the range $2 \leq$

Table 8 Quantum MDS codes

Length	Distance	Reference
$\frac{q^2-1}{m}$, $m\|q+1$, m odd	$2 \leq d \leq \frac{q-1}{2} + \frac{q-1}{2m}$	[3,21] [22]
$\frac{q^2-1}{m}$, $m\|q+1$, m even	$2 \leq d \leq \frac{q-1}{2} + \frac{q-1}{m}$	[21]
$\frac{q^2-1}{m}$, $m\|q-1$, m even	$2 \leq d \leq \frac{q+1}{2} + \frac{q-1}{m}$	[3], Theorem 2.1
$\frac{q^2+m-1}{m}$, $m\|q+1$, m odd	$2 \leq d \leq \frac{q+1}{2} + \frac{q-1}{2m}$	Theorem 2.2
$4(q-1)$, $q \equiv 1$ mod 4	$d = \frac{q+1}{2}$	Corollary 4.2
$\frac{2(q^2-1)}{m}$, odd q, odd $m\|q+1$ $s.t.m-1\|q-1$	$2 \leq d \leq \frac{q-1}{2} + \frac{q+1}{2m}$	Corollary 4.1
$\frac{q-1}{2k+1} \cdot (q+1)$, $2k+1\|q-1$ $s.t.4k+1\|q+1$	$2 \leq d \leq \frac{q-1}{2} + \frac{q+1}{2(4k+1)}$	Corollary 4.3
$\frac{(m_1+m_2-1)(q^2-1)}{2m_1m_2}$, odd $m_1 < m_2$, $gcd(m_1, m_2) = 1, q = 2m_1m_2 + 1$	$2 \leq d \leq \frac{q+1}{2} + m_1$	Corollary 3.1
$\frac{(m_1+m_2-1)(q^2-1)}{2m_1m_2}$, odd $m_1 = 2k_1+1 < m_2 = 2k_2+1$, $gcd(m_1, m_2) = 1$	$2 \leq d \leq \frac{q+1}{2} + \frac{q-1}{2(2k_2+1)}$	Corollary 2.2
$\frac{q^2-1}{m}$, suitable q and m not dividing $q-1$ or$q+1$, $A \geq 1$as in Theorem 3.1	$2 \leq d \leq \frac{q-1}{2} + A$	Theorem 3.2
$\frac{q^2-1}{3k}$, $k \equiv 5 mod 9$, for odd prime power $q = 16k^2 - 12k + 1$	$2 \leq d \leq \frac{q+1}{2} + \frac{2k-1}{3}$	Corollary 5.1

$d \leq 1494$. In the above Corollary 5.1 we should note that $3k$ is not a factor of $q-1$ or $q+1$. This case has not been treated in the previous works [3,8–13]. □

6 Summary

In this paper we give a direct method constructing q^2-ary Hermitian self-orthogonal MDS codes with dimensions $k > \frac{q}{2}$. This leads to many new q-ary quantum MDS codes with minimum distances $d > \frac{q}{2}$. Some new q-ary quantum MDS codes with $q > \frac{q}{2}$ constructed in this paper are listed in Table 8.

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. Ashikhmin, A., Knill, E.: Nonbinary quantum stabilizer codes. IEEE Trans. Inf. Theory **47**(7), 3065–3072 (2001)
3. Chen, B., Ling, S., Zhang, G.: Application of constacyclic codes to quantum MDS codes. IEEE Trans. Inf. Theory **61**(3), 1474–1484 (2015)

4. Feng, K.: Quantum code $[[6, 2, 3]]_p$ and $[[7, 3, 3]]_p$ ($p \geq 3$) exists. IEEE Trans. Inf. Theory **48**(8), 2384–2391 (2002)
5. Grassl, M., Beth, T., Roetteler, M.: On optimal quantum codes. Int. J. Quantum Inf. **2**(1), 757–766 (2004)
6. Grassl, M., Roetteler, M., Beth, T.: On quantum MDS codes. In: Proceedings of the International Symposium on Information Theory. Chicago, p. 356, (2004)
7. Grassl, M., Roetteler, M.: Quantum MDS codes over small fields. arXiv:1502.05267
8. La Guardia, G.G.: New quantum MDS codes. IEEE Trans. Inf. Theory **57**(8), 5551–5554 (2011)
9. 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**(9), 4735–4740 (2010)
10. Jin, L., Xing, C.: Euclidean and Hermitian self-orthogonal algebraic geometry codes and their application to quantum codes. IEEE Trans. Inf. Theory **58**, 5484–5489 (2012)
11. Jin, L., Xing, C.: A construction of new quantum MDS codes. IEEE Trans. Inf. Theory **60**(5), 2921–2925 (2014)
12. Kai, X., Zhu, S.: New quantum MDS codes from negacyclic codes. IEEE Trans. Inf. Theory **59**(2), 1193–1197 (2013)
13. Kai, X., Zhu, S., Li, P.: Constacyclic codes and some new quantum MDS codes. IEEE Trans. Inf. Theory **60**(4), 2080–2086 (2014)
14. Knill, E., Laflamme, R.: Theory of quantum error-correcting codes. Phys. Rev. A **55**(2), 900–911 (1997)
15. Laflamme, R., Miquel, C., Paz, J.P., Zurek, W.H.: Perfect quantum error correcting code. Phys. Rev. Lett. **77**(1), 198–201 (1996)
16. Li, Z., Xing, L.J., Wang, X.M.: Quantum generalized Reed–Solomon codes: unified framework for quantum MDS codes. Phys. Rev. A **77**(1), 012308-1–12308-4 (2008)
17. Li, R., Xu, Z.: Construction of $[[n, n-4, 3]]q$ quantum MDS codes for odd prime power q. Phys. Rev. A **82**(5), 052316-1–052316-4 (2010)
18. MacWilliams, F.J., Sloane, N.J.A.: Theory of Error-Correcting Codes, 2nd edn. North Holland, Amsterdam (1978)
19. Shor, P.W.: Scheme for reducing decoherence in quantum computer memory. Phys. Rev. A **52**(4), R2493–R2496 (1995)
20. Steane, A.M.: Enlargement of Calderbank–Shor–Steane quantum codes. IEEE Trans. Inf. Theory **45**(7), 2492–2495 (1999)
21. Wang, L., Zhu, S.: New quantum MDS codes derived from constacyclic codes. Quantum Inf. Process. **14**(3), 881–889 (2015). arXiv:1405.5421v1