Bull. Korean Math. Soc. **56** (2019), No. 3, pp. 609–619
https://doi.org/10.4134/BKMS.b180295
pISSN: 1015-8634 / eISSN: 2234-3016

QUANTUM CODES WITH IMPROVED MINIMUM DISTANCE

Emre Kolotoğlu and Mustafa Sari

Abstract. The methods for constructing quantum codes is not always sufficient by itself. Also, the constructed quantum codes as in the classical coding theory have to enjoy a quality of its parameters that play a very important role in recovering data efficiently. In a very recent study quantum construction and examples of quantum codes over a finite field of order q are presented by La Garcia in [14]. Being inspired by La Garcia's the paper, here we extend the results over a finite field with q^2 elements by studying necessary and sufficient conditions for constructions quantum codes over this field. We determine a criteria for the existence of q^2-cyclotomic cosets containing at least three elements and present a construction method for quantum maximum-distance separable (MDS) codes. Moreover, we derive a way to construct quantum codes and show that this construction method leads to quantum codes with better parameters than the ones in [14].

1. Introduction

Since Shor discovered the first quantum code that encodes one qubit to highly entangled state of nine qubits [20], quantum error correcting codes have been intensively studied by researchers. A q-ary quantum code of length n is a subspace of q^n-dimensional Hilbert space $H = \underbrace{C^q \otimes C^q \otimes \cdots \otimes C^q}_{n\ times}$ where C^q is the q-dimensional complex vector space and the bar $\otimes$ denotes the tensor product. The notation $[\![n,k,d]\!]_q$ denotes a quantum code having the parameters, length n, dimension q^k and minimum distance d, where the parameter d indicates the error detecting and correcting capability, i.e., a quantum code with minimum distance d can detect up to $d-1$ errors and correct up to $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors.

One of the main and most difficult problems in quantum error correction is to construct quantum codes having better parameters, i.e., having large

Received April 2, 2018; Revised July 16, 2018; Accepted September 17, 2018.
2010 *Mathematics Subject Classification.* 81P45, 81P70, 94B05, 94B15.
Key words and phrases. quantum codes, cyclic codes, constacyclic codes, cyclotomic cosets.

minimum distance and large dimension for a fixed length. Nevertheless, there is a restriction on the dimension and the minimum distance for a fixed length.

Proposition 1.1 (Singleton bound for quantum codes, [2,12])**.** *For an* $[\![n,k,d]\!]_q$ *quantum code,* $k \leq n-2d+2$.

An $[\![n,k,d]\!]_q$ quantum code is called maximum-distance separable (MDS) code if its parameters satisfy $k = n-2d+2$. Lately, there have been many studies on the construction of quantum MDS codes [6–11, 14, 17, 19, 22]. On the other hand, the construction of quantum codes that do not have to be MDS and have better parameters than previously constructed ones also have had much attention [4, 5, 15, 16, 18, 21]. These studies motivate us to derive quantum codes with better parameters. Via Hermitian construction, we derive good quantum codes from cyclic codes over F_{q^2} and show that these quantum codes are better than ones derived in [15].

We organize this paper as follows: In Section 2, we give fundamental concepts. In Section 3, by seeking the condition for q^2-cyclotomic cosets to contain m-consecutive terms and using Hermitian construction, we construct a family of quantum MDS codes. In Section 4, we explore a way to construct quantum codes that have better parameters than quantum codes derived in [15]. In Section 5, we compare our results with the parameters in [15]. We conclude the paper in Section 6.

2. Preliminaries

An $[n,k,d]_q$ linear code is a k-dimensional subspace of F_q^n, where n is the length, k is the dimension and d is the minimum distance. Let $F_q^\times$ be the multiplicative group of the finite field F_q and $\alpha \in F_q^\times$. A linear code C of length n over F_q is an α-constacyclic code if $(\alpha c_{n-1}, c_0, \ldots, c_{n-2}) \in C$ whenever $(c_0, c_1, \ldots, c_{n-1}) \in C$. In particular, if $\alpha = 1$, then this constacyclic code is called cyclic code. Let $(n,q) = 1$. Since an α-constacyclic code C of length n over F_q can be viewed as an ideal in the quotient ring $\frac{F_q[x]}{\langle x^n - \alpha \rangle}$, $C = \langle g(x) \rangle$ where $g(x) | \, x^n - \alpha$. Let r denote the multiplicative order of α in $F_q^\times$. Since $(n,q) = 1$, there exists an rn^{th} primitive root β of unity in an extension of F_q such that $\beta^n = \alpha$ and all roots of $x^n - \alpha$ over F_q are $\beta, \beta^{1+r}, \ldots, \beta^{1+(n-1)r}$. The q-cyclotomic coset containing i modulo rn is $C_{q,rn}(i) = \left\{ iq^j \bmod rn : j \in N \right\}$ and the defining set of an α-constacyclic code $C = \langle g(x) \rangle$ of length n is $Z = \left\{ i \in \{0, 1, \ldots, n-1\} : g\left(\beta^{1+ri}\right) = 0 \right\}$. Note that the dimension of an α-constacyclic code of length n and defining set Z is $n - |Z|$. The following gives a lower bound for the minimum distance of a constacyclic code.

Theorem 2.1 (BCH bound for constacyclic codes, [3, 13])**.** *Let* $(n,q) = 1$. *Let* β *be an* rn^{th} *primitive root of unity with* $\beta^n = \alpha$ *where* $\alpha \in F_{q^2}^\times$ *and* r *is the multiplicative order of* α *in* $F_{q^2}^\times$. *Then, the minimum distance of an*

α-constacyclic code of length n over F_{q^2} with the defining set including the set $\{1+rj,\, l \le j \le l+d-2\}$ is at least d.

The Euclidean dual $C^{\perp_E}$ of a linear code C is the set

$$C^{\perp_E} = \left\{ y \in F_q^n : \sum_{i=0}^{n-1} x_i y_i = 0,\ \forall x \in C \right\} \tag{1}$$

and the Hermitian dual $C^{\perp_H}$ of a linear code C over F_{q^2} is the set

$$C^{\perp_H} = \left\{ y \in F_{q^2}^n : \sum_{i=0}^{n-1} x_i y_i^q = 0,\ \forall x \in C \right\}. \tag{2}$$

The following is crucial in constructing quantum codes from constacyclic codes.

Lemma 2.2. *Let α be a nonzero element in F_{q^2} whose multiplicative order divides $q+1$. Suppose that C_1 is a cyclic code over F_q with length n and defining set Z_1 and C_2 is an α-constacyclic code over F_{q^2} with length n and defining set Z_2. Let $(n,q)=1$. Then,*

(1) [1] $C_1^{\perp_E} \le C_1 \Leftrightarrow -Z_1 \cap Z_1 = \emptyset$.
(2) [11] $C_2^{\perp_H} \le C_2 \Leftrightarrow -qZ_2 \cap Z_2 = \emptyset$.

We say that C is a dual-containing code if $C^{\perp_E} \le C$ and a Hermitian dual-containing code if $C^{\perp_H} \le C$.

One of the famous quantum code constructions is Calderbank-Shor-Steane (CSS) construction. For a dual-containing linear code, CSS construction turns into:

Theorem 2.3 ([2])**.** *If there exists a dual-containing $[n,k,d]_q$ linear code, then there exists an $[\![n, 2k-n, \ge d]\!]_q$ stabilizer quantum code which is pure to d.*

Called as Hermitian construction, another famous quantum code construction in the literature is as follows:

Theorem 2.4 ([2,12])**.** *If there exists a Hermitian dual-containing $[n,k,d]_{q^2}$ linear code, then there exists an $[\![n, 2k-n, \ge d]\!]_q$ quantum code that is pure to d.*

3. Quantum codes derived from constacyclic codes

In [15], La Guardia gives a condition for the existence of q-cyclotomic cosets containing m-consecutive terms and presents a new method for obtaining some new quantum codes from cyclic codes over F_q by using CSS construction. In [5], Jian Gao *et al.* consider the results derived in [15] for negacyclic codes over F_q and obtain new quantum codes. In this section, we extend this notion to constacyclic codes over F_{q^2}. We give a criteria for a q^2-cyclotomic coset over F_{q^2} to contain m-consecutive terms and by using Hermitian construction we obtain a class of quantum MDS codes from Hermitian-dual containing constacyclic codes whose defining sets are these q^2-cyclotomic cosets. We also tabulate the parameters of some quantum codes that we derive by this way. We note that throughout this section, α is an element of the finite field F_{q^2} with the multiplicative order r.

Proposition 3.1. *Let q be a prime power and n be an integer such that $(q,n)=1$. If there exist some integers $1 \leq a_1, a_2, \ldots, a_{m-1} \leq o_{rn}\left(q^2\right)$, $m \geq 3$ such that $n | \gcd\left(\lambda_1, \lambda_2, \ldots, \lambda_{m-2}\right)$, where $\lambda_j = \left(\frac{q^{2a_{j+1}}-1}{r}\right)^{-1} - \left(\frac{q^{2a_1}-1}{r}\right)^{-1} - jr$ for $1 \leq j \leq m-2$, then there exists an α-constacyclic code over F_{q^2} with parameters $[n, n-\delta, d \geq m+1]_{q^2}$, where δ is the size of q^2-cyclotomic coset modulo rn containing m-consecutive terms.*

Proof. Consider the following system of congruences

$$\begin{aligned} kq^{2a_1} &\equiv k+r \bmod rn \\ (k+r)\, q^{2a_2} &\equiv k+2r \bmod rn \\ (k+2r)\, q^{2a_3} &\equiv k+3r \bmod rn \\ &\vdots \\ (k+(m-2)\,r)\, q^{2a_{m-1}} &\equiv k+(m-1)\,r \bmod rn, \end{aligned}$$

where $m \geq 2$. The above system of congruences implies $(k+jr)\left(\frac{q^{2a_{j+1}}-1}{r}\right) \equiv 1 \bmod n$ for all $0 \leq j \leq m-2$ and so we get the following system which is equivalent to above:

$$\begin{aligned} k &\equiv \left(\frac{q^{2a_1}-1}{r}\right)^{-1} \bmod n \\ k &\equiv \left(\frac{q^{2a_2}-1}{r}\right)^{-1} - r \bmod n \\ k &\equiv \left(\frac{q^{2a_3}-1}{r}\right)^{-1} - 2r \bmod n \\ &\vdots \\ k &\equiv \left(\frac{q^{2a_{m-1}}-1}{r}\right)^{-1} - (m-2)\,r \bmod n, \end{aligned}$$

where $\left(\frac{q^{2a_i}-1}{r}\right)^{-1}$ indicates the multiplicative inverse of $\frac{q^{2a_i}-1}{r}$ modulo n. The last system has a solution if and only if

$$\left(\frac{q^{2a_{j+1}}-1}{r}\right)^{-1} - jr \equiv \left(\frac{q^{2a_{i+1}}-1}{r}\right)^{-1} - ir \bmod n \tag{3}$$

for all $i, j = 1, \ldots, m-2$ and

$$\left(\frac{q^{2a_1}-1}{r}\right)^{-1} \equiv \left(\frac{q^{2a_{j+1}}-1}{r}\right)^{-1} - jr \bmod n \tag{4}$$

Table 1. Some parameters of quantum codes obtained by Theorem 3.2

n	r	$a_1, a_2, \ldots, a_{m-1}$	$[\![n, k, d]\!]_q$
17	3	2,7	$[\![17, 1, d \geq 4]\!]_5$
29	6	1,2,8	$[\![29, 1, d \geq 5]\!]_{11}$

for all $j = 1, \ldots, m-2$. This implies that

$$n \quad \text{divides} \quad \left(\frac{q^{2a_{j+1}}-1}{r}\right)^{-1} - \left(\frac{q^{2a_1}-1}{r}\right)^{-1} - jr \tag{5}$$

for each $j = 1, \ldots, m-2$. The last assertion means that $n | \gcd(\lambda_1, \lambda_2, \ldots, \lambda_{m-2})$, where $\lambda_j = \left(\frac{q^{2a_{j+1}}-1}{r}\right)^{-1} - \left(\frac{q^{2a_1}-1}{r}\right)^{-1} - jr$ for every $j = 1, \ldots, m-2$. Take C as an α-constacyclic code over F_{q^2} whose defining set is $C_{q^2,rn}(k)$. From the above construction, $C_{q^2,rn}(k)$ contains m-consecutive integers $k, k+r, \ldots, k+(m-1)r$. Since $|C_{q^2,rn}(k)| = \delta$, and by the BCH bound for constacyclic codes the minimum distance d of C is at least $m+1$, one gets an $[n, n-\delta, d \geq m+1]_{q^2}$ constacyclic code. □

Theorem 3.2. *Suppose that all the hypotheses of Proposition 3.1 hold. Let $C_{q^2,rn}(k)$ be a q^2-cyclotomic coset containing m-consecutive terms. If*

$$-qC_{q^2,rn}(k) \neq C_{q^2,rn}(k),$$

then there exists a quantum code with parameters $[\![n, n-2\delta, d \geq m+1]\!]$, where $\delta = |C_{q^2,n}(k)|$.

Proof. Let C be an α-constacyclic code of length n over F_{q^2} having the defining set $C_{q^2,rn}(k)$. It follows from $-qC_{q^2,rn}(k) \neq C_{q^2,rn}(k)$ and Lemma 2.2 that $C^{\perp_h} \leq C$. Therefore, by Hermitian construction, one gets a quantum code with desired parameters. □

Now, we present some parameters that are tabulated in Table 1 to illustrate Theorem 3.2. The integers $a_1, a_2, \ldots, a_{m-1}$ appeared in Table 1 are ones satisfying the condition given in Proposition 3.1.

Proposition 3.3. *Let $k \geq 1$ be an integer. Then,*

(1) $\left(2^k+1, 2^{2k}+1\right) = 1$.
(2) $\left(2^k-1, 2^{2k}+1\right) = 1$.

Proof. (1) Since $\left(2^k+1\right)\left(2^{2k}-2^{2k-1}-2^{k-1}+1\right) = 1+\left(2^k-2^{k-1}\right)\left(2^{2k}+1\right)$, we get $\left(2^k+1\right)\left(2^{2k}-2^{2k-1}-2^{k-1}+1\right) \equiv 1 \bmod \left(2^{2k}+1\right)$. This implies that $\left(2^k+1, 2^{2k}+1\right) = 1$.

(2) Since $\left(2^k-1\right)\left(2^k-1\right)2^{k-1} = 1+\left(2^{k-1}-1\right)\left(2^{2k}+1\right)$, it follows that $\left(2^k-1\right)\left(2^k-1\right)2^{k-1} \equiv 1 \bmod \left(2^{2k}+1\right)$. This means $\left(2^k-1, 2^{2k}+1\right) = 1$. □

Lemma 3.4. *Let $q = 2^k$, $k \geq 1$ and $r = q+1$. Suppose that $n = \frac{q^2+1}{\lambda} \geq 5$.*

(1) *For each $0 \leq j \leq q-1$, $C_{q^2,rn}(1+rj) = \{1+rj, 1+r(q-1-j)\}$.*

(2) $-qC_{q^2,rn}\left(1+\frac{(q+1)q}{2}\right) \neq C_{q^2,rn}\left(1+\frac{(q+1)q}{2}\right)$.

Proof. (1) It follows from $q^2 r \equiv -r \bmod rn$ that

$$q^2(1+rj) \equiv 1+r(q-1-j) \bmod rn.$$

Since $o_{rn}(q^2) = 2$, for each $0 \leq j \leq q-1$, we get

$$C_{q^2,rn}(1+rj) = \{1+rj, 1+r(q-1-j)\}.$$

(2) Suppose that $-qC_{q^2,rn}\left(1+\frac{(q+1)q}{2}\right) = C_{q^2,rn}\left(1+\frac{(q+1)q}{2}\right)$. Then, we have two cases: $-q\left(1+\frac{(q+1)q}{2}\right) \equiv 1+\frac{(q+1)q}{2} \bmod rn$ or $-q\left(1+\frac{(q+1)q}{2}\right) \equiv 1+\frac{(q+1)(q-2)}{2} \bmod rn$.

Case 1: Assume that $-q\left(1+\frac{(q+1)q}{2}\right) \equiv 1+\frac{(q+1)q}{2} \bmod rn$. This implies that $1+\frac{(q+1)q}{2} \equiv 0 \bmod n$. Since $(2,n)=1$, we get $q^2+q+2 \equiv 0 \bmod n$ and so $q+1 \equiv 0 \bmod n$. The last assertion is a contradiction because $(q+1,n)=1$ by Proposition 3.3(1).

Case 2: Assume that $-q\left(1+\frac{(q+1)q}{2}\right) \equiv 1+\frac{(q+1)(q-2)}{2} \bmod rn$. Then, we get $\frac{(q+1)q}{2} \equiv 0 \bmod n$. Since $(2,n)=1$, $q^2+q \equiv 0 \bmod n$. This is a contradiction because $(q-1,n)=1$ by Proposition 3.3(2). □

As a corollary of Theorem 3.2 and Lemma 3.4, we give a class of quantum MDS codes which was also derived by Lingfei Jin *et al.* in [8].

Theorem 3.5. *Let $q = 2^k$, $k \geq 1$. Then, for each positive integer λ dividing q^2+1 such that $\frac{q^2+1}{\lambda} \geq 5$, there exists a quantum MDS code with parameters $\left[\!\left[\frac{q^2+1}{\lambda}, \frac{q^2+1}{\lambda}-4, 3\right]\!\right]_q$.*

Proof. Let $n = \frac{q^2+1}{\lambda} \geq 5$ and $r = q+1$. Let C be an α-constacyclic code of length n over F_{q^2} having the defining set $C_{q^2,rn}\left(1+r\frac{q}{2}\right)$. By Lemma 3.4(2), $-qC_{q^2,rn}\left(1+r\frac{q}{2}\right) \neq C_{q^2,rn}\left(1+r\frac{q}{2}\right)$ and by Lemma 2.2(2), $C_2^{\perp_H} \leq C_2$. By Lemma 3.4(1), $C_{q^2,rn}\left(1+r\frac{q}{2}\right)$ has exactly two elements which are consecutive. Therefore, by Theorem 3.2, we get an $[\![n, n-4, d \geq 3]\!]_q$ quantum code. By Proposition 1.1, this quantum code is an MDS code of the parameters $[\![n, n-4, 3]\!]_q$. □

4. Construction of good quantum codes

In [15], La Guardia derived some new quantum codes from dual-containing cyclic codes over F_q by using CSS construction. In this section, by considering cyclic codes over higher alphabet F_{q^2} and using Hermitian construction, we construct some quantum codes whose parameters are better than ones in [15].

When compared to quantum codes obtained from dual-containing cyclic codes over F_q with CSS construction, we deduce that quantum codes obtained from cyclic codes over F_{q^2} with Hermitian construction are of better parameters.

Let $(n,q)=1$ and $o_n(q)=2m$, $m\geq 1$. Then, clearly $o_n\left(q^2\right)=m$. This means that $\left|C_{q^2,n}(i)\right|=t$ if $|C_{q,n}(i)|=2t$, where $t|\,m$. Suppose that $C_{q,n}(i)$ is a q-cyclotomic coset that contains d consecutive terms and provides $-C_{q,n}(i)\neq C_{q,n}(i)$. Take C as a cyclic code of length n over F_q with defining set $C_{q,n}(i)$. In this case, since $C^{\perp_E}\leq C$ and $d(C)\geq d+1$, by CSS construction one gets an $[\![n,n-4t,\geq d+1]\!]_q$ quantum code. Since $C_{q^2,n}(i)=\left\{i,iq^2,\ldots,iq^{2t-2}\right\}$ and $C_{q^2,n}(iq)=\left\{iq,iq^3,\ldots,iq^{2t-1}\right\}$, we get $C_{q,n}(i)=C_{q^2,n}(i)\cup C_{q^2,n}(iq)$. Hence, it is enough to prove that $-qC_{q,n}(i)\cap C_{q,n}(k)=\emptyset$ whenever $-C_{q,n}(i)\cap C_{q,n}(k)=\emptyset$ to construct a quantum code with the same parameters from Hermitian dual-containing cyclic code over F_{q^2} having defining set $C_{q^2,n}(i)\cup C_{q^2,n}(iq)$ via Hermitian construction.

Proposition 4.1. *$-qC_{q,n}(i)\cap C_{q,n}(k)=\emptyset$ if and only if $-C_{q,n}(i)\cap C_{q,n}(k)=\emptyset$.*

Proof. Since $(n,q)=1$ and two cyclotomic cosets are the same or distinct, we get $-i\equiv kq^j\,(\mathrm{mod}n)\;\Leftrightarrow\;-qi\equiv kq^{j+1}\,(\mathrm{mod}n)$ for some j, which completes the proof. □

Proposition 4.1 guarantees that all parameters obtained in [15] can be also derived from cyclic codes over F_{q^2} with Hermitian construction. Let us give an example to illustrate this. We use the notation $C_{q,n}(i,k)$ instead of $C_{q,n}(i)\cup C_{q,n}(k)$.

Example 1. Let C be a cyclic code over F_{13} of length 35 with the defining set $C_{13,35}(3)=\{3,4,17,11\}$. See that $-C_{13,35}(3)\cap C_{13,35}(3)=\emptyset$. By CSS construction, one gets a quantum code with the parameters $[\![35,27,\geq 3]\!]_{13}$ from the cyclic code C, which was constructed in [15]. See that $C_{13^2,35}(3)=\{3,17\}$ and $C_{13^2,35}(4)=\{4,11\}$. Take C' as a cyclic code over F_{13^2} of length 35 with the defining set $Z=C_{13^2,35}(3,4)$. Proposition 4.1 ensures that $Z\cap -13Z=\emptyset$ and by Lemma 2.2, $C'^{\perp_H}\leq C'$. By Hermitian construction, we get a quantum code with same parameters $[\![35,27,\geq 3]\!]_{13}$.

We show that Hermitian dual-containing cyclic codes over F_{q^2} are more fertile than dual-containing cyclic codes over F_q to construct quantum codes.

Proposition 4.2. *Suppose that $n|\,q^{2m}+1$ for some $m\geq 1$. Then, $-C_{q,n}(i)=C_{q,n}(i)$. Moreover, $-qC_{q^2,n}(i)=C_{q^2,n}(iq)$.*

Proof. Since $q^{2m}\equiv -1\,(\mathrm{mod}n)$, $-1\in C_{q,n}(1)$ and $-C_{q,n}(1)=C_{q,n}(1)$. So, $-C_{q,n}(i)=C_{q,n}(i)$ for any $0\leq i\leq n-1$ and by Proposition 4.1, we get $-qC_{q,n}(i)=C_{q,n}(i)$. It follows from $q^{2m}\equiv -1\,(\mathrm{mod}n)$ that $-qi\equiv q^{2m+1}i\,(\mathrm{mod}n)$. This implies that $-qi\in C_{q^2,n}(iq)$ and so $-qC_{q^2,n}(i)=C_{q^2,n}(iq)$. □

Proposition 4.2 says that for length n dividing $q^{2m}+1$, one can not construct a quantum code from dual-containing cyclic codes of length n over F_q using CSS construction since there doesn't exist a dual-containing cyclic code of length n over F_q as a result of $-C_{q,n}(i) = C_{q,n}(i)$ for all $0 \leq i \leq n-1$.

Example 2. Let $q = 7$ and $n = 65$. Then, $65|\, 7^6 + 1$ and by Proposition 4.2, $-C_{7,65}(i) = C_{7,65}(i)$ for all i. Hence, it is impossible to find a non-trivial cyclic code over F_7 of length 65 containing its Euclidean dual and so to construct quantum codes from these cyclic codes via CSS construction. However, consider cyclic codes over F_{7^2} and 7^2-cyclotomic cosets modulo 65. Note that $-7C_{7^2,65}(2) = C_{7^2,65}(9)$ and $C_{7^2,65}(2) = \{2, 8, 32, 33, 57, 63\}$. If C_1 is a cyclic code with defining set $Z_1 = C_{7^2,65}(2)$, then $C_1^{\perp_H} \leq C_1$ and via Hermitian construction we get $[\![65, 53, d \geq 3]\!]_7$ quantum code. See that $-7C_{7^2,65}(6) = C_{7^2,65}(22)$ and $C_{7^2,65}(6) = \{6, 24, 31, 34, 41, 59\}$. If C_2 is a cyclic code with defining set $Z_2 = C_{7^2,65}(2, 6)$, then $C_2^{\perp_H} \leq C_2$ and via Hermitian construction we get $[\![65, 41, d \geq 5]\!]_7$ quantum code. See that $-7C_{7^2,65}(10) = C_{7^2,65}(5)$ and $C_{7^2,65}(10) = \{10, 25, 30, 35, 40, 55\}$. If C_3 is a cyclic code with defining set $Z_3 = C_{7^2,65}(2, 6, 10)$, then $C_3^{\perp_H} \leq C_3$ and via Hermitian construction we get $[\![65, 29, d \geq 7]\!]_7$ quantum code.

Note that $2\left|C_{q^2,n}(i)\right| = |C_{q,n}(i)|$ if $2|\,|C_{q,n}(i)|$. This fact enables us to derive quantum codes with better parameters than ones in [15].

Example 3. Let $q = 11$ and $n = 63$. In [15], La Guardia obtained a $[\![63, 39, d \geq 4]\!]_{11}$ quantum code from dual-containing cyclic codes over F_{11}. However, via Hermitian construction we get a $[\![63, 39, d \geq 7]\!]_{11}$ quantum code from the cyclic code with defining set $Z_1 = C_{11^2,63}(3, 8, 9, 10)$, which is clearly better than $[\![63, 39, d \geq 4]\!]_{11}$. In fact, via dual-containing cyclic codes over F_{11}, the best parameters with $d \geq 4$ are $[\![63, 45, d \geq 4]\!]_{11}$. Via Hermitian construction we get $[\![63, 45, d \geq 5]\!]_{11}$ quantum code from the cyclic code with defining set $Z_2 = C_{11^2,63}(3, 8, 10)$ that is better than $[\![63, 45, d \geq 4]\!]_{11}$.

5. Code comparison

As stated by La Guardia in [15], unfortunately it seems that an available source for quantum codes over large alphabets in the literature doesn't exist. Therefore, we take the parameters in Table 1 given by La Guardia in [15] as known parameters of quantum codes over large alphabets. In the Tables 2, 3 and 4, we compare our results with these parameters in [15]. In Table 2, we give the parameters of quantum codes which are better than ones listed in Table 1 in [15].

For some lengths and alphabets, we also obtain better quantum codes than the best ones that can be obtained via the construction derived in [15] and we list these parameters in Tables 3 and 4.

For instance, as the best quantum code with length 32 and least minimum distance 3 over F_9 according to the construction given in [15] is $[\![32, 22, d \geq 3]\!]_9$,

TABLE 2. A comparison between our parameters and ones in [15]

Defining set	Our quantum code	Quantum code in [15]
$C_{11^2,63}\,(3,8,9,10)$	$[\![63,39,d\geq 7]\!]_{11}$	$[\![63,39,d\geq 4]\!]_{11}$
$C_{11^2,63}\,(3,8,10)$	$[\![63,45,d\geq 5]\!]_{11}$	$[\![63,39,d\geq 4]\!]_{11}$
$C_{27^2,35}\,(1,2,3,4)$	$[\![35,19,d\geq 5]\!]_{27}$	$[\![35,19,d\geq 4]\!]_{27}$

TABLE 3. A comparison of quantum codes of length 32 over F_9

d	Quantum code in [15]	Our quantum code	Defining set
$d\geq 3$	$[\![32,22,d\geq 3]\!]_9$	$[\![32,26,d\geq 3]\!]_9$	$C_{9^2,32}\,(1,2)$
$d\geq 4$	$[\![32,18,d\geq 4]\!]_9$	$[\![32,24,d\geq 4]\!]_9$	$C_{9^2,32}\,(2,3,4)$
$d\geq 5$	$[\![32,10,d\geq 5]\!]_9$	$[\![32,20,d\geq 5]\!]_9$	$C_{9^2,32}\,(1,2,3,4)$
$d\geq 6$	$[\![32,8,d\geq 6]\!]_9$	$[\![32,18,d\geq 6]\!]_9$	$C_{9^2,32}\,(4,5,6,7,8)$

TABLE 4. A comparison of quantum codes of length 35 over F_{13}

d	Quantum code in [15]	Our quantum code	Defining set
$d\geq 4$	$[\![35,19,d\geq 4]\!]_{13}$	$[\![35,23,d\geq 4]\!]_{13}$	$C_{13^2,35}\,(1,2,3)$
$d\geq 5$	$[\![35,11,d\geq 5]\!]_{13}$	$[\![35,19,d\geq 5]\!]_{13}$	$C_{13^2,35}\,(1,2,3,4)$

we obtain a $[\![32,26,d\geq 3]\!]_9$ quantum code from cyclic codes over F_{9^2} via Hermitian construction. We list more parameters of quantum codes with length 32 over F_9 in Table 3.

Furthermore, as the best quantum code with length 35 and least minimum distance 4 over F_{13} according to the construction given in [15] is $[\![35,19,d\geq 4]\!]_{13}$, we get a $[\![35,23,d\geq 4]\!]_{13}$ quantum code from cyclic codes over F_{13^2} via Hermitian construction. We list more parameters of quantum codes with length 35 over F_{13} in Table 4.

Moreover, as an illustration of Proposition 4.2, we derive some quantum codes that can not be obtained via the construction given in [15] and we list the parameters of these quantum codes in Table 5.

6. Conclusion

We obtain a condition for a q^2-cyclotomic coset to contain at least three consecutive elements and give a construction for a class of quantum MDS codes. Furthermore, by making use of cyclic codes over higher alphabet F_{q^2} instead of F_q and Hermitian construction, we get better quantum codes than quantum codes derived in [15] and tabulate their parameters in Tables 2, 3, 4 and 5.

TABLE 5. List of some quantum codes that can not be obtained via the construction given in [15]

n	q	m	Quantum code	Defining set
17	7	2	$[[17,1,d\geq 4]]_7$	$C_{7^2,17}\,(3)$
25	13	5	$[[25,5,d\geq 3]]_{13}$	$C_{13^2,25}\,(2)$
25	13	5	$[[25,1,d\geq 4]]_{13}$	$C_{13^2,25}\,(1,10)$
29	11	7	$[[29,1,d\geq 5]]_{11}$	$C_{11^2,29}\,(1)$
37	19	9	$[[37,1,d\geq 5]]_{19}$	$C_{19^2,37}\,(1)$
37	23	3	$[[37,25,d\geq 3]]_{23}$	$C_{23^2,37}\,(1)$
37	23	3	$[[37,13,d\geq 5]]_{23}$	$C_{23^2,37}\,(1,9)$
37	23	3	$[[37,1,d\geq 6]]_{23}$	$C_{23^2,37}\,(1,5,9)$
41	7	5	$[[41,1,d\geq 6]]_7$	$C_{7^2,41}\,(3)$
41	27	2	$[[41,33,d\geq 3]]_{27}$	$C_{27^2,41}\,(4)$
41	27	2	$[[41,25,d\geq 4]]_{27}$	$C_{27^2,41}\,(3,4)$
41	27	2	$[[41,17,d\geq 5]]_{27}$	$C_{27^2,41}\,(2,3,4)$
41	32	1	$[[41,37,d\geq 2]]_{32}$	$C_{32^2,41}\,(1)$
41	32	1	$[[41,33,d\geq 3]]_{32}$	$C_{32^2,41}\,(1,2)$
41	32	1	$[[41,29,d\geq 4]]_{32}$	$C_{32^2,41}\,(1,2,3)$
53	23	1	$[[53,49,d\geq 2]]_{23}$	$C_{23^2,53}\,(1)$
53	23	1	$[[53,45,d\geq 3]]_{23}$	$C_{23^2,53}\,(1,2)$
53	23	1	$[[53,41,d\geq 4]]_{23}$	$C_{23^2,53}\,(1,2,3)$
53	23	1	$[[53,37,d\geq 5]]_{23}$	$C_{23^2,53}\,(1,2,3,4)$
53	23	1	$[[53,33,d\geq 6]]_{23}$	$C_{23^2,53}\,(1,2,3,4,5)$
53	23	1	$[[53,29,d\geq 7]]_{23}$	$C_{23^2,53}\,(1,2,3,4,5,6)$
61	32	3	$[[61,49,d\geq 3]]_{32}$	$C_{32^2,61}\,(1)$
61	32	3	$[[61,37,d\geq 5]]_{32}$	$C_{32^2,61}\,(1,12)$
61	32	3	$[[61,25,d\geq 7]]_{32}$	$C_{32^2,61}\,(2,7,11)$
65	7	3	$[[65,53,d\geq 3]]_7$	$C_{7^2,65}\,(2)$
65	7	3	$[[65,41,d\geq 5]]_7$	$C_{7^2,65}\,(2,6)$
65	7	3	$[[65,29,d\geq 7]]_7$	$C_{7^2,65}\,(2,6,10)$
73	17	6	$[[73,49,d\geq 5]]_{17}$	$C_{17^2,73}\,(4)$
73	17	6	$[[73,25,d\geq 7]]_{17}$	$C_{17^2,73}\,(4,13)$

References

[1] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli, *On quantum and classical BCH codes*, IEEE Trans. Inform. Theory **53** (2007), no. 3, 1183–1188.

[2] A. Ashikhmin and E. Knill, *Nonbinary quantum stabilizer codes*, IEEE Trans. Inform. Theory **47** (2001), no. 7, 3065–3072.

[3] N. Aydin, I. Siap, and D. K. Ray-Chaudhuri, *The structure of 1-generator quasi-twisted codes and new linear codes*, Des. Codes Cryptogr. **24** (2001), no. 3, 313–326.

[4] J.-Z. Chen, J.-P. Li, and J. Lin, *New optimal asymmetric quantum codes derived from negacyclic codes*, Internat. J. Theoret. Phys. **53** (2014), no. 1, 72–79.

[5] J. Gao and Y. Wang, *Quantum codes derived from negacyclic codes*, Internat. J. Theoret. Phys. **57** (2018), no. 3, 682–686.
[6] L. Hu, Q. Yue, and X. Zhu, *New quantum MDS code from constacyclic codes*, Chin. Ann. Math. Ser. B **37** (2016), no. 6, 891–898.
[7] L. Jin, H. Kan, and J. Wen, *Quantum MDS codes with relatively large minimum distance from Hermitian self-orthogonal codes*, Des. Codes Cryptogr. **84** (2017), no. 3, 463–471.
[8] L. Jin, S. Ling, J. Luo, and C. Xing, *Application of classical Hermitian self-orthogonal MDS codes to quantum MDS codes*, IEEE Trans. Inform. Theory **56** (2010), no. 9, 4735–4740.
[9] L. Jin and C. Xing, *A construction of new quantum MDS codes*, IEEE Trans. Inform. Theory **60** (2014), no. 5, 2921–2925.
[10] X. Kai and S. Zhu, *New quantum MDS codes from negacyclic codes*, IEEE Trans. Inform. Theory **59** (2013), no. 2, 1193–1197.
[11] X. Kai, S. Zhu, and P. Li, *Constacyclic codes and some new quantum MDS codes*, IEEE Trans. Inform. Theory **60** (2014), no. 4, 2080–2086.
[12] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, *Nonbinary stabilizer codes over finite fields*, IEEE Trans. Inform. Theory **52** (2006), no. 11, 4892–4914.
[13] A. Krishna and D. V. Sarwate, *Pseudocyclic maximum-distance-separable codes*, IEEE Trans. Inform. Theory **36** (1990), no. 4, 880–884.
[14] G. G. La Guardia, *New quantum MDS codes*, IEEE Trans. Inform. Theory **57** (2011), no. 8, 5551–5554.
[15] ———, *Quantum codes derived from cyclic codes*, Int. J. Theor. Phys. **56** (2017), no. 8, 2479–2484.
[16] G. G. La Guardia and M. M. S. Alves, *On cyclotomic cosets and code constructions*, Linear Algebra Appl. **488** (2016), 302–319.
[17] S. Li, M. Xiong, and G. Ge, *Pseudo-cyclic codes and the construction of quantum MDS codes*, IEEE Trans. Inform. Theory **62** (2016), no. 4, 1703–1710.
[18] J. Qian and L. Zhang, *Improved constructions for nonbinary quantum BCH codes*, Internat. J. Theoret. Phys. **56** (2017), no. 4, 1355–1363.
[19] ———, *Improved constructions for quantum maximum distance separable codes*, Quantum Inf. Process. **16** (2017), no. 1, Art. 20.
[20] P. W. Shor, *Scheme for reducing decoherence in quantum memory*, Phys. Rev. A **52** (1995), no. 4, 2493–2496.
[21] J. Yuan, S. Zhu, X. Kai, and P. LI, *On the construction of quantum constacyclic codes*, Des. Codes Cryptogr. **85** (2017), no. 1, 179–190.
[22] G. Zhang and B. Chen, *New quantum MDS codes*, Int. J. Quantum Inf. **12** (2014), no. 4, 1450019, 10 pp.

Emre Kolotoğlu
Department of Mathematics
Yildiz Technical University
Esenler 34220, Turkey
Email address: kolot@yildiz.edu.tr

Mustafa Sari
Department of Mathematics
Yildiz Technical University
Esenler 34220, Turkey
Email address: musari@yildiz.edu.tr