entropy

MDPI

Article

Some New Quantum BCH Codes over Finite Fields

Lijuan Xing and Zhuo Li *

The State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China; ljxing@mail.xidian.edu.cn

* Correspondence: lizhuo@xidian.edu.cn

Abstract: Quantum error correcting codes (QECCs) play an important role in preventing quantum information decoherence. Good quantum stabilizer codes were constructed by classical error correcting codes. In this paper, Bose–Chaudhuri–Hocquenghem (BCH) codes over finite fields are used to construct quantum codes. First, we try to find such classical BCH codes, which contain their dual codes, by studying the suitable cyclotomic cosets. Then, we construct nonbinary quantum BCH codes with given parameter sets. Finally, a new family of quantum BCH codes can be realized by Steane's enlargement of nonbinary Calderbank-Shor-Steane (CSS) construction and Hermitian construction. We have proven that the cyclotomic cosets are good tools to study quantum BCH codes. The defining sets contain the highest numbers of consecutive integers. Compared with the results in the references, the new quantum BCH codes have better code parameters without restrictions and better lower bounds on minimum distances. What is more, the new quantum codes can be constructed over any finite fields, which enlarges the range of quantum BCH codes.

Keywords: quantum stabilizer codes; BCH codes; cyclotomic cosets; dual codes

Citation: Xing, L.; Li, Z. Some New Quantum BCH Codes over Finite Fields. *Entropy* **2021**, *23*, 712. https://doi.org/10.3390/e23060712

Academic Editor: Pavan Hosur

Received: 11 May 2021
Accepted: 31 May 2021
Published: 3 June 2021

1. Introduction

QECCs are important tools to prevent quantum information from decoherence in quantum computations and quantum communications. After the fundamental research for QECCs [1–3], more and more good results have been proposed to improve the quantum codes.

There were relationships between quantum codes and classical self-orthogonal codes over finite fields [4–6]. The construction of binary quantum BCH codes was based on classical additive codes over GF(4) [4]. The conclusions in [4] could be generalized to all the nonbinary primitive quantum BCH codes over finite fields [7]. Aly et al. extended Steane's results [8] to narrow-sense (not necessarily primitive) BCH codes with certain distances over GF(q) [5]. Nonbinary quantum codes with better code parameters were obtained by CSS construction [9]. Steane's enlargement construction was generalized from binary quantum codes to q-ary quantum codes [10]. Moreover, two families of nonbinary quantum codes were presented by the Hermitian construction [11]. Some quantum codes could be constructed by negacyclic codes [12,13] and constacyclic codes [14,15]. Good nonbinary quantum codes were constructed by corresponding cyclotomic cosets with given parameters [16]. The designed quantum BCH codes were obtained with given code lengths [9,16–20].

However, quantum coding theory is aimed at finding codes with given parameter sets and optimizing the code parameters. The construction of quantum BCH codes is studied in this paper. First, we try to find such classical BCH codes which contain their dual codes by studying the suitable cyclotomic cosets. The suitable cyclotomic cosets are proven to have the highest numbers of consecutive integers in defining sets and compute the dimensions of quantum BCH codes correctly. Then, we can construct nonbinary quantum BCH codes with given parameter sets. Finally, a new family of quantum BCH

codes can be realized by Steane's enlargement of nonbinary Calderbank-Shor-Steane (CSS) codes and Hermitian construction.

This paper is organized as follows. The basic theory of classical BCH codes is defined in Section 2. New families of quantum BCH codes by Steane's enlargement of CSS construction are constructed in Section 3. New families of quantum BCH codes by Hermitian construction generated by classical BCH codes over F_{q^2} are shown in Section 4. The results are compared with corresponding references in Section 5.

2. Preliminaries

The finite field is denoted by F_q with q elements, where q is a prime power. A linear code of length n over F_q is a subspace of F_q^n.

Definition 1. Given two vectors $\mathbf{x}, \mathbf{y} \in F_q^n$, the Euclidean inner product over F_q is defined as follows: $\langle \mathbf{x}, \mathbf{y} \rangle_E = x_0 y_0 + x_1 y_1 + \ldots + x_{n-1} y_{n-1}$.

Similarly, given two vectors $\mathbf{x}, \mathbf{y} \in F_{q^2}^n$, the Hermitian inner product over F_{q^2} is defined as follows: $\langle \mathbf{x}, \mathbf{y} \rangle_H = x_0 y_0^q + x_1 y_1^q + \ldots + x_{n-1} y_{n-1}^q$.

We define $\gcd(n,q)=1$ in this paper. The smallest positive integer m_0 in $q^{m_0} \equiv 1 \bmod n$ is called the multiplicative order of q modulo n and is denoted by $m_0 = \mathrm{ord}_n(q)$. Namely, $n \mid q^{m_0} - 1$ holds.

If C is an $[n,k,d]$ code over F_q, the Euclidean dual code of C is defined as follows: $C^{\perp E} = \left\{ \mathbf{x} \in F_q^n \mid \langle \mathbf{x}, \mathbf{y} \rangle_E = 0 \text{ for all } \mathbf{y} \in C \right\}$.

If C is an $[n,k,d]$ code over F_{q^2}, the Hermitian dual code of C is defined as follows: $C^{\perp \mathrm{H}} = \left\{ \mathbf{x} \in F_{q^2}^n \mid \langle \mathbf{x}, \mathbf{y} \rangle_H = 0 \text{ for all } \mathbf{y} \in C \right\}$.

The classic BCH code is a family of well-studied cyclic codes. Many explicit constructions of classical BCH codes [21] and QECCs [5] have been proposed so far. They can all be characterized by the cyclotomic cosets. Let $\varphi[i] = \{ iq^z \bmod n \mid z \in \mathbb{Z} \}$ denote the q-ary cyclotomic coset of i modulo n.

Definition 2. A BCH code C over F_q with length n and designed distance δ is a cyclic code. The defining set is denoted by $Z = \bigcup_{i=b}^{b+\delta-2} \varphi[i]$. If $n = q^{m_0} - 1$, it is called a primitive BCH code. If $b = 1$, it is called a narrow-sense BCH code.

The minimal polynomial over F_q of β is the lowest degree monic polynomial $M(x)$, with coefficients from F_q such that $M(\beta) = 0$. If $\beta = \alpha^i$ for a fixed primitive n-th root of unity $\alpha \in F_{q^{m_0}}$, then the minimal polynomial of β over F_q is denoted by $M^{(i)}(x) = \prod_{j \in \varphi[i]} (x - \alpha^j)$. The dimension of the BCH code is computed as $k = n - |Z|$. The minimum distance of the BCH code is at least δ based on the BCH bound [22]. A thorough theory of classic BCH codes is discussed in [21].

Steane's enlargements of the CSS construction and Hermitian construction are widely used in quantum stabilizer codes. To proceed further, let us review some useful results as follows.

Theorem 1 [5,10].

(1) If there exists a classical linear $[n,k_1,d_1]_q$ code C such that $C^{\perp E} \subseteq C$, and C can be enlarged to a classical linear $[n,k_1',d_1']_q$ code C' where $k_1'-k_1 \geq 2$, then there exists an $[[n,k_1'+k_1-n,d \geq \min \{d_1,\lceil \frac{q+1}{q} d_1' \rceil\}]]_q$ stabilizer code;

(2) If there exists a classical linear $[n,k_1,d_1]_{q^2}$ code D such that $D^{\perp H} \subseteq D$, then there exists an $[[n,2k_1-n,d \geq d_1]]_q$ stabilizer code.

We construct quantum stabilizer codes using classic codes which contain their dual codes. An important lemma is generalized in [5].

Lemma 1 [5]. Let q be a prime power and n be an integer such that $\gcd(n,q)=1$:

(1) A cyclic code of length n over F_q with a defining set Z contains its Euclidean dual code if and only if $Z \bigcap Z^{-1} = \varnothing$, where $Z^{-1} = \{-z \ mod \ n \mid z \in Z\}$;

(2) A cyclic code of length *n* over F_{q^2} with a defining set Z contains its Hermitian dual code if and only if $Z \bigcap Z^{-q} = \varnothing$, where $Z^{-q} = \{-qz \ mod \ n \mid z \in Z\}$.

3. Steane's Construction

Suppose $n = r(q^m - 1)$ and $\mathrm{ord}_n(q) = 2m$. If $r = 1$, then $q^m \equiv 1 \bmod n$. We only consider the case where $r > 1$.

Lemma 2. If $1 < i < rq^{\lceil \frac{m}{2} \rceil}$, $\varphi[i]$ has m elements if and only if $r \mid i$; $\varphi[i]$ has $2m$ elements if $r \nmid i$.

Proof. If $r \mid i$, we obtain $r(q^m-1) \mid i(q^m-1) \Rightarrow i(q^m-1) \equiv 0 \bmod n \Rightarrow iq^m \equiv i \bmod n$.

If $m = 1$, we obtain $iq \equiv i \bmod n$; therefore, $\varphi[i]$ has one element. Now, let us discuss the case where $m > 1$. Assume that $\varphi[i]$ has m_i elements, where $m_i \mid m$. If m is even, then $1 < m_i \leq \frac{m}{2}$; if m is odd, then $1 < m_i \leq \frac{m}{3}$. We have $iq^{m_i} \equiv i \bmod n \Rightarrow n \mid i(q^{m_i}-1) \Rightarrow r\frac{q^m-1}{q^{m_i}-1} \mid i$. Since $1 \leq i \leq rq^{\lceil \frac{m}{2} \rceil} < r\frac{q^m-1}{q^{m_i}-1}$, it has a contradiction. Therefore, $\varphi[i]$ has m elements.

Conversely, if $\varphi[i]$ has m elements, we obtain $iq^m \equiv i \bmod n \Rightarrow n \mid i(q^m-1) \Rightarrow r \mid i$. If $r \nmid i$, assume that $\varphi[i]$ has m_i elements, where $m_i \mid m$. We have $iq^{m_i} \equiv i \bmod n$. Since $r\frac{q^m-1}{q^{m_i}-1} \mid i$, it has a contradiction. Finally, lemma 2 follows.

3.1. m Is Even

Let us consider the case where m is even first. The following theorem contributes to choosing cyclotomic cosets.

Lemma 3. If *i* is an integer such that $r(q^{\frac{m}{2}}-1) \mid i$, then $\varphi[i] = \varphi[-i]$.

Proof. Supposing that m is even, we have $n = r(q^{\frac{m}{2}}-1)(q^{\frac{m}{2}}+1)$. If $r(q^{\frac{m}{2}}-1) \mid i$, we obtain $i(q^{\frac{m}{2}}+1) \equiv 0 \bmod n \Rightarrow iq^{\frac{m}{2}} \equiv -i \bmod n \Rightarrow \varphi[i] = \varphi[-i]$.

According to Steane's construction, quantum BCH codes can be generated by Euclidean dual-containing classical BCH codes, with the selected cosets in the range of

$\varphi[(k\text{-}1)r(q^{\frac{m}{2}}-1)+1] \sim \varphi[kr(q^{\frac{m}{2}}-1)-1]$, $1 \le k \le q^{\frac{m}{2}}+1$. However, some cosets are not disjointed in this range. Therefore, we should choose the cosets carefully.

Theorem 2. Let $q \ge 4$ be a prime power, n be an integer such that $\gcd(n,q)=1$ and $\mathrm{ord}_n(q)=2m$. Assume that $n=r(q^m-1)$, where $1<r<q$. If $m \ge 4$, then there exists an $[[n, n-2m(2r-1)(q^{\frac{m}{2}}-q^{\frac{m}{2}-1}-1)+2m, d \ge r(q^{\frac{m}{2}}-1)]]_q$ quantum BCH code.

Proof. Since $n=r(q^m-1)$ and $\mathrm{ord}_n(q)=2m$, we have $n \mid q^{2m}-1$ and $r \mid q^m+1$. If $r=q-1$, we obtain $q-1 \mid q^m+1 \Rightarrow q^m+1=(\sum_{i=0}^{m-1} q^i)(q-1)+2$. Clearly, this is not true for the case where $q \ge 4$. We have $1<r<q-1$.

Let $C=\langle \prod_i M^{(i)}(x) \rangle$ with the defining set Z, where $rq^{\frac{m}{2}-1} \le i \le r(q^{\frac{m}{2}}-1)-1$. If $Z \cap Z^{-1} \ne \varnothing$, there exist i and j such that $iq^l \equiv -j \bmod n$, where $rq^{\frac{m}{2}-1} \le i, j \le r(q^{\frac{m}{2}}-1)-1$ and $0 \le l \le 2m-1$. We then obtain the following:

$$iq^l + j \equiv 0 \bmod n \tag{1}$$

This congruence equation contradicts the fact that $0 < iq^l + j \le n-(q^{\frac{m}{2}}-1)$ when $0 \le l \le \frac{m}{2}$. Let us consider the case where $\frac{m}{2}+1 \le l \le m$. Thus, $0 \le m-l \le \frac{m}{2}-1$, and it follows that $rq^m i + rq^{m-l} j \equiv 0 \bmod n$. Since $rq^m \equiv r \bmod n$, we have $i + jq^{m-l} \equiv 0 \bmod (q^m-1)$. Since $m \ge 4$ and $1<r<q-1$, we obtain $0 < i + q^{m-l} j \le r(q^{m-1}+q^{\frac{m}{2}}-q^{\frac{m}{2}-1}-1)-q^{\frac{m}{2}-1}-1 < q^m - q^{m-1} + q^{\frac{m}{2}+1} - 2q^{\frac{m}{2}} - q < q^m - 1$. Therefore, the congruence equation $i + jq^{m-l} \equiv 0 \bmod (q^m-1)$ is not satisfied.

When $m+1 \le l \le 2m-1$, we have $1 \le 2m-l \le m-1$. From $q^{2m} \equiv 1 \bmod n$, we can infer that

$$i + jq^{2m-l} \equiv 0 \bmod n \tag{2}$$

Obviously, it contradicts the cases where $0 \le l \le \frac{m}{2}$ and $\frac{m+1}{2} \le l \le m$. Therefore, $Z \cap Z^{-1} = \varnothing$, and C is Euclidean dual-containing.

Suppose $\varphi[i]=\varphi[j]$, where $rq^{\frac{m}{2}-1} \le i \ne j \le r(q^{\frac{m}{2}}-1)-1$. It follows that $iq^l \equiv j \bmod n$, where $1 \le l \le 2m-1$. We thus obtain the following:

$$iq^l - j \equiv 0 \bmod n \tag{3}$$

When $1 \le l \le \frac{m}{2}$, it contradicts the case where $r+1 \le iq^l - j \le r(q^m - q^{\frac{m}{2}} - q^{\frac{m}{2}-1}) - q^{\frac{m}{2}} < n.$

When $\frac{m}{2}+1 \le l \le m$, since $rq^m \equiv r \bmod n$, we have $rq^{m-l} j - ri \equiv 0 \bmod n$. Hence, $jq^{m-l} - i \equiv 0 \bmod (q^m-1)$, where $0 \le m-l \le \frac{m}{2}-1$. If $m-l=0$, we have $j-i \equiv 0 \bmod (q^m-1)$, which contradicts the fact that $0 < i \ne j < q^m-1$. If $1 \le m-l \le \frac{m}{2}-1$, we have

$$r+1 < jq^{m-l} - i < r(q^{m-1} - 2q^{\frac{m}{2}-1}) - q^{\frac{m}{2}-1} < q^m + q^{\frac{m}{2}-1} - q^{m-1} - 2q^{\frac{m}{2}} < q^m - 1.$$

Since $1<r<q-1$ and $m \ge 4$, $jq^{m-l} - i \equiv 0 \bmod (q^m-1)$ is not satisfied.

When $m+1 \le l \le 2m-1$, we have $1 \le 2m-l \le m-1$. Since $q^{2m} \equiv 1 \bmod n$, Equation (3) is transformed into $jq^{2m-l} - i \equiv 0 \bmod n$. This is similar to the cases where $1 \le l \le \frac{m}{2}$ and $\frac{m}{2}+1 \le l \le m$. To sum up, all the cosets given above are mutually disjointed.

From Lemma 2, there are $q^{\frac{m}{2}} - q^{\frac{m}{2}-1} - 1$ cosets with m elements. Since $\varphi[1]=\varphi[q^{\frac{m}{2}}], \cdots, \varphi[rq^{\frac{m}{2}-1}-2]=\varphi[rq^{\frac{m}{2}}-2q]$ and $\varphi[rq^{\frac{m}{2}-1}-1]=\varphi[rq^{\frac{m}{2}}-q]$, there are

$r(q^{\frac{m}{2}}-1)-1$ consecutive integers in Z. Therefore, we obtain $C=[n,k_1=n-m(2r-1)(q^{\frac{m}{2}}-q^{\frac{m}{2}-1}-1),d_1\geq r(q^{\frac{m}{2}}-1)]_q$ according to the BCH bound. Let $C'=\left\langle \prod_j M^{(j)}(x)\right\rangle$ and $rq^{\frac{m}{2}-1}\leq j\leq r(q^{\frac{m}{2}}-1)-2$. Since $1<r<q-1$, we have $(rq^{\frac{m}{2}-1}-1)q \leq r(q^{\frac{m}{2}}-1)-2$, and thus $\varphi[rq^{\frac{m}{2}-1}-1]=\varphi[rq^{\frac{m}{2}}-q]$. We obtain $C'=[n,k_1'=n-m(2r-1)(q^{\frac{m}{2}}-q^{\frac{m}{2}-1}-1)+2m,d_1'\geq r(q^{\frac{m}{2}}-1)-1]_q$. Since $k_1'-k_1=2m>2$, C' is an enlargement of *C*. Since $r(q^{\frac{m}{2}}-1)\leq\left\lceil\frac{q+1}{q}\right\rceil(r(q^{\frac{m}{2}}-1)-1)$, we have an $[[n,n-2m(2r-1)\left(q^{\frac{m}{2}}-q^{\frac{m}{2}-1}-1\right)+2m, d\geq r\left(q^{\frac{m}{2}}-1\right)]]_q$ quantum BCH code.

It is rather remarkable that $q\geq 4$ ensures that C' contains the highest numbers of consecutive integers. We choose $m\geq 4$ for the reason that there exist cyclotomic cosets $\varphi[i]=\varphi[-j]$ when $m=2$. The *q*-ary cyclotomic cosets proposed in Theorem 2 not only easily compute the dimensions of C and C', but also ensure C is Euclidean dual-containing. The condition $1<r<q$ ensures that the selected cosets are mutually disjointed.

Example 1. If $q=5$, $m=4$ and $r=2$, we have *n* = 1248 and $r(q^{\frac{m}{2}}-1)=48$. It is easy to compute the following 5-ary cyclotomic cosets: $\varphi[10]=\{10,50,250,2\}$, …, $\varphi[48]=\{48,240,1200,1008\}$. Obviously, $\varphi[48]=-\varphi[48]$. Let $C=<\prod_{i\in Z}M^{(i)}(x)>$ have the defining set $Z=\bigcup_{i=10}^{47}\varphi[i]$ and $C'=<\prod_{j\in Z'}M^{(j)}(x)>$ have the defining set $Z'=\bigcup_{j=10}^{46}\varphi[j]$. $C=[1248,1020,d_1\geq 48]_5$ is Euclidean dual-containing, and $C'=[1248,1028,d_1'\geq 47]_5$ is an enlargement of C. Then, we obtain an $[[1248,800,d\geq 48]]_5$ quantum BCH code.

3.2. m Is Odd

Next, we consider the case where m is odd. For simplicity, we define $Q_1=q^{\frac{m+1}{2}}-q+\lfloor\frac{r}{2}\rfloor$. If $m=1$, we have $n=r(q-1)$ and $\mathrm{ord}_n(q)=2$, which were studied in [16]. Therefore, we choose $m>1$ when *m* is odd. A few contributions are presented as follows.

Theorem 3. Let q be a prime power, n be an integer such that $\gcd(n,q)=1$ and $\mathrm{ord}_n(q)=2m$. Assume that $n=r(q^m-1)$, where $\lfloor\frac{3r}{2}\rfloor<q\leq 2r$. If $m>1$, then there exists an $[[n,n-4m(Q_1-q^{\frac{m-1}{2}})+m(\lfloor\frac{Q_1}{r}\rfloor+\lfloor\frac{Q_1-1}{r}\rfloor-2\left\lceil\frac{q^{\frac{m-1}{2}}}{r}\right\rceil),d\geq Q_1+1]]_q$ quantum BCH code.

The proof is similar to Theorem 2.

Example 2. If $q=7$, $m=3$ and $n=1368$, we have $q^{\frac{m-1}{2}}=7$ and $Q_1=44$. It is easy to compute the following 7-ary cyclotomic cosets: $\varphi[7]=\{7,49,343,1033,391,1\}$, …, $\varphi[44]=\{44,308,788\}$ and $\varphi[45]=\{45,315,837,1341,1179\}$. Obviously, $\varphi[45]=\varphi[-27]$. Meanwhile, the cosets which contain $\varphi[1]$, $\varphi[2]$, …, $\varphi[6]$ are mutually disjointed. We choose $\varphi[7]$, $\varphi[8]$, …, $\varphi[44]$ to generate $C=[1368,1170,d_1\geq 45]_7$ and $\varphi[7]$, $\varphi[8]$, …, $\varphi[43]$ to generate $C'=[1368,1173,d_1'\geq 45]_7$. Finally, we obtain an $[[1368,975,d\geq 45]]_7$ quantum BCH code.

Corollary 1. Let q be a prime power, n be an integer such that $\gcd(n,q)=1$ and $\mathrm{ord}_n(q)=2m$. Assume that $n=r(q^m-1)$ and $m>1$:

(1) If $r < q < \lfloor \frac{3r}{2} \rfloor$ or $q > 2r$, then there exists an $[[n, n-4m(q^{\frac{m+1}{2}} - q^{\frac{m-1}{2}} - q) + m(\lfloor \frac{q^{\frac{m+1}{2}} - q - 1}{r} \rfloor + \lfloor \frac{q^{\frac{m+1}{2}} - q - 2}{r} \rfloor - 2\lceil \frac{q^{\frac{m-1}{2}} - 1}{r} \rceil), d \geq q^{\frac{m+1}{2}} - q]]_q$ quantum BCH code;

(2) If $q < r \leq 2q - 4$, then there exists an $[[n, n-4m(rq^{\frac{m-1}{2}} - rq^{\frac{m-3}{2}} + \lfloor \frac{r}{2} \rfloor) + 2m(q^{\frac{m-1}{2}} - q^{\frac{m-3}{2}} - 1), d \geq rq^{\frac{m-1}{2}} - q + \lfloor \frac{r}{2} \rfloor + 1]]_q$ quantum BCH code;

(3) If $2q - 3 \leq r \leq \frac{q^2+1}{2}$ and $m = 3$, then there exists an $[[n, n-12(rq - r - q) + 3(2q - \lfloor \frac{q+2}{r} \rfloor - \lfloor \frac{q+1}{r} \rfloor - 2), d \geq rq - q]]_q$ quantum BCH code;

(4) If $2q - 3 \leq r \leq q^2 - q + 1$ and $m = 5$, then there exists an $[[n, n-20(rq^2 - rq - q) + 5(2q^2 - 2q - \lfloor \frac{q+2}{r} \rfloor - \lfloor \frac{q+2}{r} \rfloor), d \geq rq^2 - q]]_q$ quantum BCH code;

(5) If $2q - 3 \leq r < q^2$ and $m \geq 7$, then there exists an $[[n, n-4m(rq^{\frac{m-1}{2}} - rq^{\frac{m-3}{2}} - q) + m(2q^{\frac{m-1}{2}} - 2q^{\frac{m-3}{2}} - \lfloor \frac{q+1}{r} \rfloor - \lfloor \frac{q+2}{r} \rfloor), d \geq rq^{\frac{m-1}{2}} - q]]_q$ quantum BCH code.

Proof. We only listed the range of q-ary cyclotomic cosets to generate C and C'. The reminder proof is similar to Theorem 2.

(1) Let $C = \langle \prod_i M^{(i)}(x) \rangle$, where $q^{\frac{m-1}{2}} - 1 \leq i \leq q^{\frac{m+1}{2}} - q - 1$. Let $C' = \langle \prod_j M^{(j)}(x) \rangle$, where $q^{\frac{m-1}{2}} - 1 \leq j \leq q^{\frac{m+1}{2}} - q - 2$;

(2) Let $C = \langle \prod_i M^{(i)}(x) \rangle$, where $rq^{\frac{m-3}{2}} \leq i \leq rq^{\frac{m-1}{2}} - q + \lfloor \frac{r}{2} \rfloor$. Let $C' = \langle \prod_j M^{(j)}(x) \rangle$, where $rq^{\frac{m-3}{2}} \leq j \leq rq^{\frac{m-1}{2}} - q + \lfloor \frac{r}{2} \rfloor - 1$;

(3) Let $C = \langle \prod_i M^{(i)}(x) \rangle$, where $r - 1 \leq i \leq rq - q - 1$. Let $C' = \langle \prod_j M^{(j)}(x) \rangle$, where $r - 1 \leq j \leq rq - q - 2$;

(4) Let $C = \langle \prod_i M^{(i)}(x) \rangle$, where $rq - 1 \leq i \leq rq^2 - q - 1$. Let $C' = \langle \prod_j M^{(j)}(x) \rangle$, where $rq - 1 \leq j \leq rq^2 - q - 2$;

(5) Let $C = \langle \prod_i M^{(i)}(x) \rangle$, where $rq^{\frac{m-3}{2}} - 1 \leq i \leq rq^{\frac{m-1}{2}} - q - 1$. Let $C' = \langle \prod_j M^{(j)}(x) \rangle$, where $rq^{\frac{m-3}{2}} - 1 \leq j \leq rq^{\frac{m-1}{2}} - q - 2$.

4. Hermitian Construction

Let us focus on classic BCH codes over F_{q^2}. Suppose $n = r(q^{2m} - 1)$ and $\mathrm{ord}_n(q^2) = 2m$. We choose $r > 1$ for the reason that we have $q^{2m} \equiv 1 \bmod n$ when $r = 1$.

Lemma 4. If $1 \leq i \leq rq^m$, $\varphi[i]$ has m elements if and only if $r \mid i$, and $\varphi[i]$ has $2m$ elements if $r \nmid i$.

The proof is similar to Lemma 2.

Lemma 5. Let m_o be the odd factor of m and m_e be the even factor of m:

(1) If $r\frac{q^{2m}-1}{q^{m_o}+1} \mid i$, then $\varphi[i] = -q\varphi[i]$;

(2) If $r\frac{q^{2m}-1}{q^{m_e}+1} \mid i$, then $\varphi[i] = -q\varphi[qi]$.

Proof. (1) Since $n = r(q^{2m} - 1)$, we have $n = r\frac{q^{2m}-1}{q^{m_o}+1}(q^{m_o} + 1)$. If $r\frac{q^{2m}-1}{q^{m_o}+1} \mid i$, we have $i(q^{m_o} + 1) \equiv 0 \bmod n \Rightarrow i \equiv -qq^{m_o - 1} i \bmod n$. When m_o is odd, we obtain $\varphi[i] = -q\varphi[i]$. (2)

Since $n = r(q^{2m}-1)$, we have $n = r\frac{q^{2m}-1}{q^{m_e}+1}(q^{m_e}+1)$. If $r\frac{q^{2m}-1}{q^{m_e}+1} \mid i$, we have $i \equiv -qq^{m_e-2}qi \bmod n$. When m_e is even, we obtain $\varphi[i] = -q\varphi[qi]$.

4.1. m Is Odd

Corollary 2. Let m be an integer. If $r(q^m-1) \mid i$, then $\varphi[i] = -q\varphi[i]$.

Theorem 4. Let q be a prime power and n be an integer such that $\gcd(n, q^2) = 1$ and $\mathrm{ord}_n(q^2) = 2m$. Assume that $n = r(q^{2m}-1)$, where $1 < r < q$. If $m > 1$, then there exists an $[[n, n-2m(2r-1)(q^m - q^{m-2}-1), d \geq r(q^m-1)]]_q$ quantum BCH code.

Proof. Let $D = \left\langle \prod_i M^{(i)}(x) \right\rangle$ with the defining set Z, where $rq^{m-2} \leq i \leq r(q^m-1)-1$. If $Z \cap Z^{-q} \neq \varnothing$, there exist values i and j such that $iq^{2l} \equiv -qj \bmod n$, where $rq^{m-2} \leq i, j \leq r(q^m-1)-1$ and $0 \leq 2l \leq 4m-2$. Thus, we obtain

$$iq^{2l} + jq \equiv 0 \bmod n \tag{4}$$

First, let us consider the case where $2l = 0$. Equation (4) transforms into $i + qj \equiv 0 \bmod n$. This contradicts the fact that $0 < iq^{2l-1} + j \leq n - (q^m+1) < n$.

When $2 \leq 2l \leq m+1$, since $\gcd(n, q^2) = 1$, Equation (4) transforms into $iq^{2l-1} + j \equiv 0 \bmod n$. This contradicts the fact that $0 < iq^{2l-1} + j \leq n - (q^m+1) < n$.

When $m+3 \leq 2l \leq 2m$, since $rq^{2m} \equiv r \bmod n$, Equation (4) transforms into

$$i + jq^{2m-2l+1} \equiv 0 \bmod (q^{2m}-1) \tag{5}$$

We obtain $i + q^{2m-2l+1}j \leq r(q^{2m-2} - q^{m-2} + q^m - 1) - q^{m-2} - 1 < q^{2m} - 1$, and the congruence of Equation (5) is not satisfied.

When $2m+2 \leq 2l \leq 4m-2$, we have $3 \leq 4m-2l+1 \leq 2m-1$. From $q^{4m} \equiv 1 \bmod n$, it can be inferred that $i + jq^{4m-2l+1} \equiv 0 \bmod n$. Obviously, this contradicts the cases where $0 \leq 2l \leq m+1$ and $m+3 \leq 2l \leq 2m$. Therefore, $Z \cap Z^{-q} = \varnothing$, and D is Hermitian dual-containing.

Similar to Theorem 2, the cosets $\varphi[rq^{m-2}]$, …, $\varphi[r(q^m-1)-2]$ and $\varphi[r(q^m-1)-1]$ are mutually disjointed. From Lemma 4, there are $q^m - q^{m-2} + 1$ cosets with m elements. Since $\varphi[1] = \varphi[q^{m-1}]$, …, $\varphi[rq^{m-2}-2] = \varphi[rq^m - 2q^2]$ and $\varphi[rq^{m-2}-1] = \varphi[rq^m - q^2]$, there are $r(q^m-1)-1$ consecutive integers in Z. Therefore, we obtain $D = [n, n-m(2r-1)(q^m - q^{m-2}-1), d_1 \geq r(q^m-1)]_{q^2}$. Then, an $[[n, n-2m(2r-1)(q^m - q^{m-2}-1), d \geq r(q^m-1)]]_q$ quantum BCH code can be obtained by a Hermitian construction.

It is rather remarkable that the q^2–ary cyclotomic cosets proposed in Theorem 4 can easily compute the dimensions of the BCH codes. The condition $1 < r < q$ ensures that the selected cosets are mutually disjointed. Furthermore, the cosets contain the highest numbers of consecutive integers.

Theorem 5. Let q be a prime power, n be an integer such that $\gcd(n, q) = 1$ and $\mathrm{ord}_n(q^2) = 2m$, Assume that $n = r(q^{2m}-1)$, where $q < r < 2q$. If $m > 1$, then there exists an $[[n, n-4m\ (q^{m+1} - q^{m-1} + r) + 2m(\left\lfloor \frac{q^{m+1}-1}{r} \right\rfloor - \left\lfloor \frac{q^{m-1}+1}{r} \right\rfloor + 4),\ d \geq q^{m+1} + r)]]_q$ quantum BCH code.

The proof is similar to Theorem 4.

Example 3. If $q=7$, $m=3$ and $n=1176480$, it is easy to compute the following 49-ary cosets: $\varphi[50]=\{50,2450,120050\}$, …, $\varphi[2410]=\{2410,118090,1080490\}$. Let $D=<\prod_{i=50}^{2410}M^{(i)}(x)>$, where $D=[1176480,1163025,d_1\geq 2411]_{49}$ is Hermitian dual-containing. Then, we obtain an $[[1176480,1149570,d\geq 2411]]_7$ quantum BCH code.

4.2. m Is Even

Now, we consider the case where m is even. A few contributions are presented as follows.

Corollary 3. When letting λ be an integer such that $0\leq\lambda\leq r\frac{(q^m-1)(q-1)}{q^{m-1}+1}$, we have $\varphi[r(q^m-1)+\lambda q^{m-1}]=\varphi[-q(rq(q^m-1)-\lambda)]$. In particular, when letting i be an integer such that $r(q^m-1)\,|\,i$, we have $\varphi[i]=-q\varphi[qi]$.

Proof. Since $rq^{2m}\equiv r \bmod n$, we have

$$(r(q^m-1)+\lambda q^{m-1})q^m\equiv rq^{2m}-rq^{3m}+\lambda q^{2m-1}\equiv -q(rq(q^m-1)-\lambda)q^{2m-2} \bmod n$$

If m is even, clearly, we obtain $\varphi[r(q^m-1)+\lambda q^{m-1}]=\varphi[-q(rq(q^m-1)-\lambda)]$. In the condition of $rq(q^m-1)-\lambda\geq r(q^m-1)+\lambda q^{m-1}$, we obtain $0\leq\lambda\leq r\frac{(q^m-1)(q-1)}{q^{m-1}+1}$. According to Corollary 3, if $r(q^m-1)\,|\,i$, we have $\varphi[i]=-q\varphi[qi]$.

Therefore, we should choose the q^2-ary cyclotomic cosets properly to ensure the cyclic code is Hermitian dual-containing.

Theorem 6. Let q be a prime power, n be an integer such that $\gcd(n,q^2)=1$ and $\mathrm{ord}_n(q^2)=2m$. Assume that $n=r(q^{2m}-1)$, where $1<r<q$. Then, there exists an $[[n,n-2m(2r-1)(q^m-q^{m-2}),\ d\geq rq^m+1]]_q$ quantum BCH code.

The proof is similar to Theorem 4.

Example 4. If $q=3$, $m=4$, $r=2$ and $n=13120$, we choose $\varphi[19]$ to $\varphi[162]$ as the 9-ary cyclotomic cosets, which are mutually disjointed, to generate *D*. Obviously, $Z\cap Z^{-3}=\varnothing$, where *Z* is the defining set of *D*. Then, $D=[13120,12256,d\geq 163]_9$ is Hermitian dual-containing. Thus, we can construct an $[[13120,11392,d\geq 163]]_3$ quantum BCH code.

5. Comparison and Conclusions

In this section, we give some comparisons to corresponding references.

Aly et al. constructed quantum BCH codes over F_q with classic non-primitive narrow-sense BCH codes and F_{q^2} with classic primitive narrow-sense BCH codes [5]. In this paper, we designed quantum BCH codes with classic non-primitive, non-narrow-sense BCH codes. In [5], Aly et al. designed an $[[n,n-4m\lceil(\delta-1)(1-1/q)\rceil,d\geq\delta]]_q$ quantum BCH code, where $2\leq\delta\leq\delta_{\max}\leq r\frac{q^m-1}{q^m+1}<r$. If $r\frac{q^m-1}{q^m+1}<2$, a quantum BCH code does not exist. Therefore, we could not obtain quantum codes with $r=2$ in [5]. In this paper, we designed quantum BCH codes without this restriction. For example, if $q=5$, $m=4$ and $r=2$, we can construct an $[[1248,800,d\geq 48]]_5$ quantum BCH code, in which $\delta_{\max}=1.933<2$. Since $2\leq\delta\leq\delta_{\max}<r$, we got better lower bounds for the minimum dis-

tances than those in [5]. Meanwhile, [10] presented similar results to [5] with Steane's construction. Therefore, our results were better than those in [10], too. Table 1 shows more precise conclusions.

Table 1. Code comparison with length $n = r(q^m - 1)$.

New Quantum BCH Codes	Quantum BCH Codes in [5,10]
$[[315,195,d \geq 16]]_4$	$[[315,279,d \geq 4]]_4$
$[[1248,800,d \geq 48]]_5$	—
$[[1368,975,d \geq 45]]_7$	$[[1368,1344,d \geq 3]]_7$
$[[1533,1158,d \geq 56]]_8$	$[[1533,1521,d \geq 2]]_8$
$[[2736,2142,d \geq 54]]_7$	$[[2736,2664,d \geq 7]]_7$
$[[4599,3831,d \geq 69]]_8$	$[[4599,4515,d \geq 8]]_8$
$[[4800,3824,d \geq 96]]_7$	—

In [17], by letting $n = r(q^3 - 1)$ and $m = \mathrm{ord}_n(q^2) = 3$, quantum BCH codes were constructed with classic non-primitive, narrow-sense and non-narrow-sense BCH codes. However, in [17], quantum BCH codes could only be constructed with a fixed length n for $q = 3l + 2$. In this paper, we extended the construction to a larger range of n over any finite field F_q.

In [23], non-binary primitive quantum BCH codes were constructed when $m = \mathrm{ord}_n(q)$=2 and $m = \mathrm{ord}_n(q^2)$=2. In this paper, we designed nonbinary, non-primitive quantum BCH codes. Moreover, we extended the results to more general cases where $m > 3$.

The earlier work of this paper was conducted in [20]. In [20], we discussed the construction of quantum BCH codes with multiplicative order $m = 2$ when the code lengths were $n = r(q+1)$ over F_q and $n = r(q^2+1)$ over F_{q^2}. We also considered the situation where $m = 3$ and when the code lengths were $n = r(q-1)$ over F_q and $n = r(q^2 - 1)$ over F_{q^2}. In this paper, we discussed more general cases. We enlarged the multiplicative order to any even integers. Moreover, we extended the construction to a larger range of code lengths with $n = r(q^m - 1)$ over F_q and $n = r(q^{2m} - 1)$ over F_{q^2}, where m denotes the integers.

In this paper, a new family of quantum BCH codes was constructed by Steane's construction and Hermitian construction. By studying the suitable cyclotomic cosets, we tried to find such classic BCH codes which contained their dual codes. Then, we constructed nonbinary quantum BCH codes with given parameter sets. We have proven that the cyclotomic cosets are good tools to study quantum BCH codes. The defining sets contained the highest numbers of consecutive integers. Compared with the results in the references, the new quantum BCH codes had better code parameters without restrictions and better lower bounds for the minimum distances. What is more, the new quantum codes can be constructed over any finite fields, which enlarges the range of quantum BCH codes.

Author Contributions: Conceptualization, Z.L.; writing—original draft preparation, L.X. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Natural Science Foundation of China (NSFC) (61372072); Overseas Expertise Introduction Project for Discipline Innovation (111 Project) (B08038); and Fundamental Research Funds for the Central Universities.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Nielsen, M.A.; Chuang, I.; Grover, L.K. Quantum Computation and Quantum Information. *Am. J. Phys.* **2002**, *70*, 558–559, doi:10.1119/1.1463744.
2. Shor, P.W. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A* **1995**, *52*, R2493–R2496, doi:10.1103/physreva.52.r2493.
3. Steane, A. Multiple-particle interference and quantum error correction. *Proc. R. Soc. A: Math. Phys. Eng. Sci.* **1996**, *452*, 2551–2577, doi:10.1098/rspa.1996.0136.
4. Calderbank, A.; Rains, E.; Shor, P.; Sloane, N. Quantum error correction via codes over GF(4). *IEEE Trans. Inf. Theory* **1998**, *44*, 1369–1387, doi:10.1109/18.681315.
5. Aly, S.A.; Klappenecker, A.; Sarvepalli, P.K. On Quantum and Classical BCH Codes. *IEEE Trans. Inf. Theory* **2007**, *53*, 1183–1188, doi:10.1109/tit.2006.890730.
6. Hamada, M. Concatenated Quantum Codes Constructible in Polynomial Time: Efficient Decoding and Error Correction. *IEEE Trans. Inf. Theory* **2008**, *54*, 5689–5704, doi:10.1109/TIT.2008.2006416.
7. Ketkar, A.; Klappenecker, A.; Kumar, S.; Sarvepalli, P. Nonbinary Stabilizer Codes Over Finite Fields. *IEEE Trans. Inf. Theory* **2006**, *52*, 4892–4914, doi:10.1109/tit.2006.883612.
8. Steane, A. Enlargement of Calderbank-Shor-Steane quantum codes. *IEEE Trans. Inf. Theory* **1999**, *45*, 2492–2495, doi:10.1109/18.796388.
9. La Guardia, G.G. Quantum Codes Derived from Cyclic Codes. *Int. J. Theor. Phys.* **2017**, *56*, 2479–2484, doi:10.1007/s10773-017-3399-2.
10. Ling, S.; Luo, J.; Xing, C. Generalization of Steane's Enlargement Construction of Quantum Codes and Applications. *IEEE Trans. Inf. Theory* **2010**, *56*, 4080–4084, doi:10.1109/TIT.2010.2050828.
11. Hu, Q.; Zhang, G.H.; Chen, B.C. Constructions of New Nonbinary Quantum Codes. *Int. J. Theor. Phys.* **2015**, *54*, 92–99.
12. Gao, J.; Wang, Y. Quantum Codes Derived from Negacyclic Codes. *Int. J. Theor. Phys.* **2017**, *57*, 682–686, doi:10.1007/s10773-017-3599-9.
13. Chen, J.-Z.; Li, J.-P.; Lin, J. New Optimal Asymmetric Quantum Codes Derived from Negacyclic Codes. *Int. J. Theor. Phys.* **2014**, *53*, 72–79, doi:10.1007/s10773-013-1784-z.
14. Liu, Y.; Li, R.; Lv, L.; Ma, Y. A class of constacyclic BCH codes and new quantum codes. *Quantum Inf. Process.* **2017**, *16*, doi:10.1007/s11128-017-1533-y.
15. Yuan, J.; Zhu, S.; Kai, X.; Li, P. On the construction of quantum constacyclic codes. *Des. Codes Cryptogr.* **2017**, *85*, 179–190, doi:10.1007/s10623-016-0296-2.
16. La Guardia, G.G. On the Construction of Nonbinary Quantum BCH Codes. *IEEE Trans. Inf. Theory* **2014**, *60*, 1528–1535, doi:10.1109/tit.2014.2298137.
17. Ma, Y.; Liang, F.; Guo, L. Some Hermitian Dual Containing BCH Codes and New Quantum Codes. *Appl. Math. Inf. Sci.* **2014**, *8*, 1231–1237, doi:10.12785/amis/080337.
18. Ma, Z.; Lü, X.; Feng, K.; Feng, D. On Non-binary Quantum BCH Codes. In Proceedings of the International Conference on Theory and Applications of Models of Computation, Beijing, China, 15–20 May 2006; pp. 675–683.
19. Qian, J.; Zhang, L. Improved Constructions for Nonbinary Quantum BCH Codes. *Int. J. Theor. Phys.* **2017**, *56*, 1355–1363, doi:10.1007/s10773-017-3277-y.
20. Zhang, M.; Li, Z.; Xing, L.; Tang, N. Some Families of Quantum BCH Codes. *Int. J. Theor. Phys.* **2018**, *58*, 615–630, doi:10.1007/s10773-018-3959-0.
21. Macwilliams, F.J.; Sloane, N.J.A. *The Theory of Error-Correcting Codes*; North-Holland Publishing Company: Amsterdam, The Netherlands, 1977.
22. Charpin, P. *Open Problems on Cyclic Codes in Handbook of Coding Theory*; North-Holl and Publishing Company: Amsterdam, The Netherlands, 1998).
23. La Guardia, G.G. Constructions of new families of nonbinary quantum codes. *Phys. Rev. A* **2009**, *80*, 042331, doi:10.1103/physreva.80.042331.