Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.12785/amis/080337

Some Hermitian Dual Containing BCH Codes and New Quantum Codes

*Yuena Ma**, *Fangchi Liang and Luobin Guo*

School of Science, Air Force Engineering University, Xi'an, Shaanxi 710051, P. R. China

Received: 8 Jun. 2013, Revised: 13 Oct. 2013, Accepted: 14 Oct. 2013
Published online: 1 May. 2014

Abstract: Let $q = 3l+2$ be a prime power. Maximal designed distances of imprimitive Hermitian dual containing q^2-ary narrow-sense (NS) BCH codes of length $n = \frac{(q^6-1)}{3}$ and $n = 3(q^2-1)(q^2+q+1)$ are determined. For each given n, non-narrow-sense (NNS) BCH codes which achieve such maximal designed distances are presented, and a series of NS and NNS BCH codes are constructed and their parameters are computed. Consequently, many families of q-ary quantum BCH codes are derived from these BCH codes. Some of these quantum BCH codes constructed from NNS BCH codes have better parameters than those quantum BCH codes available in the literature, and some others are new ones.

Keywords: Cyclotomic coset, BCH (Bose-Chaudhuri-Hocquenghem) code, Hermitian dual containing code, Quantum BCH code

1 Introduction

Quantum codes are powerful tool for fighting against noise in quantum communication and quantum computation. The most widely studied class of quantum codes are stabilizer (or additive) quantum codes, which can be constructed from classical codes with certain self-orthogonal (or dual containing) properties [1]-[4]. Many papers discussed dual containing conditions of BCH codes and construction of quantum codes from classical BCH codes. Steane [5] gave a simple criterion to decide the condition under which a binary primitive narrow-sense (NS) BCH code containing its Euclidean dual code, for given code length and designed distance. Aly *et.al* in [6] and [7] generalized Steane's result to primitive and non-primitive NS BCH codes over F_q or F_{q^2} with respect to Euclidean and Hermitian duality, and constructed many quantum BCH codes. In 2009, La Guardia [8] showed that there are dual containing primitive non-narrow-sense (NNS) BCH codes having better parameters than that of NS BCH codes, he constructed many good non-binary quantum codes from these NNS BCH codes. Paper [12]-[15] make further study on construction of quantum codes from (NS or NNS) BCH codes via Hermitian construction or Steane construction.

In this paper, let $q = 3l+2$, we give maximal designed distances of Hermitian dual containing non-primitive BCH codes of length $n = \frac{(q^6-1)}{3}$ and $n = 3(q^2-1)(q^2+q+1)$, determine parameters of some NS and NNS BCH codes, and construct many good non-binary quantum BCH codes from Hermitian dual containing NS and NNS BCH codes.

This paper is organized as follows. In Sec.2, basic concepts on q^2-cyclotomic cosets and BCH codes are reviewed. In Sec.3 and Sec.4, necessary and sufficient conditions of Hermitian dual containing NS BCH code of length n and their maximal designed distance δ_{new} are given, several families of Hermitian dual containing NNS BCH codes of length n with designed distance $\delta \leq \delta_{new}$ are presented. At the same time, many new quantum BCH codes are constructed from these NS and NNS BCH codes. Finally, the paper is concluded with a discussion in Sec.5.

2 Preliminaries

In this section, we will review some basic knowledge on cyclotomic cosets and BCH codes for the purpose of this paper. For more details, we refer the reader to [9,10] .

It is well known that there is a close relationship between cyclotomic cosets and cyclic codes, see [9,11].

* Corresponding author e-mail: mayuena2013@163.com

This suggests us to use q^2-cyclotomic cosets of modulo n to characterize BCH codes over $\mathbf{F}_{q^2}$, see [14].

Definition 2.1.[14] If $gcd(q,n) = 1$, the q^2-cyclotomic coset of modulo n containing x is defined by

$$C_x = \{x, xq^2, x(q^2)^2, ..., x(q^2)^{k-1}\}(\text{mod} n),$$

where k is the smallest positive integer such that $(q^2)^k x \equiv x(\text{mod} n)$.

Definition 2.2.[14] Let n, q, C_x be as in definition 2.1. If $n - qx \in C_x$, C_x is called a skew symmetric coset, otherwise skew asymmetric. The skew asymmetric coset come in pairs C_x and $C_{-qx} = C_{n-qx}$, and is denoted as (C_x, C_{-qx}).

A cyclic code of length $n = q^{2m} - 1$ over $\mathbf{F}_{q^2}$ is called a BCH code with designed distance δ if its generator polynomial is of the form

$$g(x) = \prod_{z \in T}(x - \xi^z), T = C_b \cup C_{b+1} \cup \cdots \cup C_{b+\delta-2},$$

where C_x denotes the q^2-cyclotomic coset of modulo n containing x, ξ is a primitive element of $\mathbf{F}_{q^{2m}}$ and $m = ord_n(q^2)$ is the multiplicative order of q^2 modulo n, given by [7]. Such a BCH code also defined in terms of its defining set, see following Definition 2.3.

Definition 2.3.[9, 10] Let $gcd(q,n) = 1$. If ξ is a primitive n-th root of unity in some field containing $\mathbf{F}_{q^2}$, $T = C_b \cup C_{b+1} \cup \cdots \cup C_{b+\delta-2} = T_{[b,b+\delta-2]}$, the cyclic code of length n with defining set T is called a BCH code of designed distance δ. If $b = 1$, $\mathscr{C}$ is called a narrow-sense BCH code, otherwise non-narrow-sense. If $n = q^{2m} - 1$, $\mathscr{C}$ is called primitive, otherwise called non-primitive.

Lemma 2.1.[7] If $gcd(q,n) = 1$, $\mathscr{C}$ is a cyclic code over $\mathbf{F}_{q^2}$ with defining set T, $\mathscr{C}^{\perp_h} \subseteq \mathscr{C}$ if and only if $T \cap T^{-q} = \emptyset$, where $T^{-q} = \{-qt(\text{mod} n) \mid t \in T\}$.

Using terminology of skew symmetric coset and skew asymmetric coset pair, Lemma 2.1 can be restated as Lemma 2.2:

Lemma 2.2.[12] If $gcd(q,n) = 1$, $\mathscr{C}$ is a cyclic code over $\mathbf{F}_{q^2}$ with defining set T, $\mathscr{C}^{\perp_h} \subseteq \mathscr{C}$ if and only if each C_t is skew asymmetric and any two C_{t_1} and C_{t_2} do not form a skew asymmetric pair, where $t, t_1, t_2 \in T$.

Skew symmetric and skew asymmetric pair for q^2-cyclotomic cosets can be judged as follows.

Lemma 2.3. [12] Let $gcd(q,n) = 1$, $ord_n(q^2) = m$, $0 \leq x, y, z \leq n-1$.

(1) C_x is skew symmetric if and only if there is a $t \leq \lfloor \frac{m}{2} \rfloor$ such that $x \equiv -xq^{2t+1}(\text{mod} n)$.

(2) If $C_y \neq C_z$, (C_y, C_z) form a skew asymmetric pair if and only if there is a $t \leq \lfloor \frac{m}{2} \rfloor$ such that $y \equiv -zq^{2t+1}(\text{mod} n)$ or $z \equiv -yq^{2t+1}(\text{mod} n)$.

The following Theorem 2.4 (given in [3, 11] is well-known for constructing q-ary quantum codes from Hermitian dual containing (or self-orthogonal) codes over $\mathbf{F}_{q^2}$.

Theorem 2.4.[3, 11] If $\mathscr{C}$ is an $[n,k]$ linear code over $\mathbf{F}_{q^2}$ such that $\mathscr{C}^{\perp_h} \subseteq \mathscr{C}$, $d = min\{wt(v) : v \in \mathscr{C} \setminus \mathscr{C}^{\perp_h}\}$, then there exists an $[[n, 2k-n, d]]_q$ quantum code.

Let $\mathscr{BCH}(n, q^2; \delta)$ denote the q^2-ary NS BCH code of length n with designed distance δ. Let $[m \quad even] = m - 1(\text{mod}2)$, for instance, we have $[m \quad even] = 0$ if m is odd, otherwise $[m \quad even] = 1$. A maximal designed distances of Hermitian dual containing imprimitive BCH codes was given by [7], see Theorem 2.5. We will improve their bound in section 3 and section 4 for some special code length n.

Theorem 2.5.[7] Suppose that $m = ord_n(q^2)$, $[m \quad even] = m - 1(\text{mod}2)$ for an integer m. If the designed distance δ satisfies $2 \leq \delta \leq \delta_{max}$, where

$$\delta_{max} = \lfloor \frac{n}{q^{2m}-1}(q^{m+[m \quad even]} - 1 - (q^2-2)[m \quad even]) \rfloor$$

then $\mathscr{BCH}(n, q^2; \delta)^{\perp_h} \subseteq \mathscr{BCH}(n, q^2; \delta)$.

Notation. To simplify statement, we use $[1, n-1]$ to denote the set $\{1, 2, \cdots, n-1\}$ and call the set $\{e, e+1, \cdots, f\}$ as interval $[e, f]$.

3 BCH codes of length $n = \frac{(q^6-1)}{3}$

3.1 Dual containing BCH codes of length $n = \frac{(q^6-1)}{3}$

According to Theorem 2.5, the maximal designed distance of Hermitian dual containing NS BCH code of length $n = \frac{(q^6-1)}{3}$ given in [7] is $\delta_{max} = \lfloor \frac{q^3-1}{3} \rfloor$. In this subsection, we determine the maximal designed distance of Hermitian dual containing NS BCH code of length n is $\delta_{new} = 2\lfloor \frac{q^3-1}{3} \rfloor + 1 = 2\delta_{max} + 1$. And show that there is dual containing NNS BCH code with such maximal designed distance δ_{new}.

Theorem 3.1. Let $n = \frac{(q^6-1)}{3}$, $\delta_{new} = 2\lfloor \frac{q^3-1}{3} \rfloor + 1 = 2\delta_{max} + 1$. Then the following hold:

(1) The maximal designed distance of dual containing NS BCH codes of length n is δ_{new}.

(2) A NS BCH code of length n with designed distance δ contains its Hermitian dual code if and only if $\delta \leq \delta_{new}$.

Proof. For $q = 3l + 2$, we know $3 | (q^3 + 1)$, so let $r = \frac{1}{3}(q^3 + 1)$, then $n = \frac{(q^6-1)}{3} = (q^3 - 1)r$. We will prove a NS BCH code with designed distance $\delta \leq \delta_{new} = 2r - 1$ contains its dual code. It is enough to show, for $x, y \in [1, 2r-2] = [1, 2\lfloor \frac{q^3-1}{2} \rfloor] = [1, 2\delta_{max}]$, C_x is skew asymmetric and (C_x, C_y) can not form a skew asymmetric pair.

I. To prove C_x is skew asymmetric for $x \in [1, 2\lfloor \frac{q^3-1}{2} \rfloor]$. From Lemma 2.3, we only need to prove $x(q^{2t+1} + 1) \not\equiv 0(\text{mod} n)$ where $t \leq \lfloor \frac{3}{2} \rfloor$.

Case 1. For $t=0$, then $1<x(q+1)<2\lfloor\frac{q^3-1}{3}\rfloor(q+1)=(q^2-1)\cdot 2\lfloor\frac{q^2+q+1}{3}\rfloor<n$. So $x(q+1)\not\equiv 0(\bmod n)$.

Case 2. For $t=1$.

If $1\le x\le r-1$, then $1<x(q^3+1)\le(r-1)(q^3+1)$. Since $(r-1)(q^3+1)=r(q^3-1)+2(r-1)-(q^3-1)\equiv 2(r-1)-(q^3-1)(\bmod n)$, and $2(r-1)-(q^3-1)<n$, so we have $1<x(q^3+1)<n$.

If $r\le x\le 2r-2$, one can assume $x=r+b, 0\le b\le r-2$, then $x(q^3+1)=r(q^3-1)+b(q^3-1)+2(r+b)\equiv b(q^3-1)+2(r+b)(\bmod n)$, and $1<b(q^3-1)+2(r+b)\le(r-2)(q^3-1)+2r-2$. Since $(r-2)(q^3-1)+2r-2=r(q^3-1)-2(q^3-1)+2r-2\equiv -2(q^3-1)+2r-2(\bmod n)$, and $-2(q^3-1)+2r-2<n$, so we have $1<x(q^3+1)<n$.

From the above two cases, one can deduce $x(q^{2t+1}+1)\not\equiv 0(\bmod n)$. This proves C_x is skew asymmetric.

II. Next we show C_x and C_y can not form a skew asymmetric pair, so we only need to show $x+yq^{2t+1}\not\equiv 0(\bmod n)$ and $y+xq^{2t+1}\not\equiv 0(\bmod n)$ for $t=0,1$. Let $x,y\in[1,2\lfloor\frac{q^3-1}{2}\rfloor]$ and $x<y$.

Case 1. For $t=0$, it is obvious that $1<x+yq<y(q+1)<n$, $1<y+xq<y(q+1)<n$.

Case 2. For $t=1$.

If $1\le y\le r-1$, then $1<x+yq^3<y(q^3+1)\le(r-1)(q^3+1)<n$, $1<y+xq^3<y(q^3+1)<n$.

If $r\le y\le 2r-2$, let $y=r+b, 0\le b\le r-2$, then $n<x+rq^3<x+yq^3<x+(2r-2)q^3=2r(q^3-1)+2r-2q^3+x=2n-2(q^3+1)+4r<2n$. $1<y+xq^3<y+(r-1)q^3<n$ for $x\le r-1$ and $y+n<y+xq^3<y+(2r-2)q^3=2n-2(q^3+1)+4r<2n$ for $x\ge r$.

Hence, we have showed $x+yq^{2t+1}\not\equiv 0(\bmod n)$ and $y+xq^{2t+1}\not\equiv 0(\bmod n)$.

Combining the previous two cases, we know that C_x and C_y can not form a skew asymmetric pair.

According to the above discussions and Lemma 2.2, the theorem follows.

Theorem 3.1 gives the maximal designed distance of Hermitian dual containing NS BCH codes of length $n=\frac{(q^6-1)}{3}$. The following theorem will give NNS BCH codes also achieve the such maximal designed distance δ_{new}.

Let $s=\frac{(q^2+q+1)(q^2-q+1)}{3}$, $a=\frac{q+1}{3}(q^2+1)$ and $b=\frac{q-2}{3}(q^2+q+1)$. Similar to the above discussion, one can check that each C_{s+i} is skew asymmetric and any two cosets C_{s+i} and C_{s+j} do not form a skew asymmetric pair for $-a\le i,j\le b$. Thus we can easily deduce the NNS BCH code with defining set $T_{[s-a,s+b]}$ is a Hermitian dual containing BCH code of length n.

Theorem 3.2. Let $n=(q^2-1)s$, $s=\frac{(q^2+q+1)(q^2-q+1)}{3}$, $\delta_{new}=2\lfloor\frac{q^3-1}{3}\rfloor+1$, $a=\frac{q+1}{3}(q^2+1)$ and $b=\frac{q-2}{3}(q^2+q+1)$. Then the following hold:

(1) A NNS BCH code with defining set $T_{[s-a,s+b]}$ of length n is a Hermitian dual containing code of the maximal designed distance $\delta=\delta_{new}$.

(2) A NNS BCH code of length n with designed distance $\delta\le\delta_{new}$ and defining set $T_{[e,f]}\subset T_{[s-a,s+b]}$, then it contains its Hermitian dual code.

3.2 Dimensions of BCH codes of length $n=\frac{(q^6-1)}{3}$

In this subsection, we will first calculate dimensions of some dual containing NS and NNS BCH codes of length $n=\frac{(q^6-1)}{3}$. Then, in terms of these results, for each δ satisfying $2\le\delta\le\delta_{new}$, we will determine the parameters of quantum BCH codes via Hermitian construction. Before calculating dimensions of NS and NNS BCH codes of length n, we give following Lemma 3.3 and Corollary 3.4.

Lemma 3.3. Let $q=3l+2$. For $n=\frac{(q^6-1)}{3}$, $\delta_{max}=\lfloor\frac{q^3-1}{3}\rfloor$, then the following hold:

(1) If $x\in[1,2\delta_{max}]$, C_x contains three elements.

(2) If $x,y\in[1,2\delta_{max}]$ and $x<y$, then $C_x=C_y$ if and only if $y=xq^2$.

Proof. (1) Since $1\le x\le 2\lfloor\frac{q^3-1}{3}\rfloor$, thus $x<xq^2<n$ and $x\ne xq^2$, so $x,xq^2\in C_x$. Thus $|C_x|=r\ge 2$, but $r|3$, hence $|C_x|=3$.

(2) If $x<y$ and $C_x=C_y$, then $xq^2\equiv y(\bmod n)$ or $xq^4\equiv y(\bmod n)$.

First we show $xq^4\equiv y(\bmod n)$ can not hold. Since $x\in[1,2\delta_{max}]$ and $\lfloor 2\delta_{max}/\frac{(q^2-1)}{3}\rfloor=2q$, so we assume $x=i\cdot\frac{(q^2-1)}{3}+j$, where $0\le i\le 2q$ and $0\le j\le\frac{(q^2-1)}{3}-1$. If $1\le x<\frac{q^2-1}{3}$, then $1<q^4-y<xq^4-y<(\frac{q^2-1}{3})q^4-y=(\frac{q^2-1}{3})q^4-q^4-y<n$. If $x\ge\frac{q^2-1}{3}$, then $x=i\cdot\frac{q^2-1}{3}+j$ with $i\ge 1$, so we has $(i-1)n<xq^4-y=i(\frac{q^2-1}{3}+j)q^4-y=i\frac{q^6-1}{3}-i\frac{q^4-1}{3}+jq^4-y<in$. From the above facts, one can deduce $xq^4\not\equiv 0(\bmod n)$. Since $-y<xq^2-y<xq^2<n$, hence $xq^2-y\equiv 0(\bmod n)$ and $xq^2\equiv y(\bmod n)$.

We can give dimensions of dual containing NS BCH codes for $2\le\delta\le\delta_{new}$.

Corollary 3.4. Let $n=\frac{(q^6-1)}{3}$, $\delta_{new}=2\lfloor\frac{q^3-1}{3}\rfloor+1$. If $2\le\delta\le\delta_{new}$, then a NS Hermitian dual containing BCH code has parameter $[n,n-3\lfloor(\delta-1)(1-\frac{1}{q^2})\rfloor,d\ge\delta]$.

Similar to the proof of Lemma 3.3, one can show the following lemma holds.

Lemma 3.5. Let $n=(q^2-1)s$, $s=\frac{(q^2+q+1)(q^2-q+1)}{3}$, $a=\frac{q+1}{3}(q^2+1)$ and $b=\frac{q-2}{3}(q^2+q+1)$. Then the following hold:

(1) $C_s=\{s\}$, $|C_{s+i}|=3$ for $-a<i<b$ and $i\ne 0$.

(2) If $-a\le i\le -1$, $1\le j\le b$, then $C_{s+i}\ne C_{s+j}$.

(3) If $1\le|i|<|j|$ and $C_{s+i}=C_{s+j}$, then $j=iq^2$.

La Guardia showed that there are dual containing primitive NNS BCH codes having better parameters than that of NS BCH codes, please see Reference [8]. By

Table 1. Comparison of quantum codes constructed from NNS BCH codes and NS BCH codes for $n = \frac{5^6-1}{3} = 5208$ and $2 \leq \delta \leq \delta_{max} = 41$

δ	our $[[n,K,d \geq \delta]]_5$	$[[n,K',d \geq \delta]]_5$ in [7]
2	$[[5208,5206,d \geq 2]]_5$	$[[5208,5202,d \geq 2]]_5$
3	$[[5208,5200,d \geq 3]]_5$	$[[5208,5196,d \geq 3]]_5$
4	$[[5208,5194,d \geq 4]]_5$	$[[5208,5190,d \geq 4]]_5$
5	$[[5208,5188,d \geq 5]]_5$	$[[5208,5184,d \geq 5]]_5$
$\cdots$	$\cdots$	$\cdots$
25	$[[5208,5068,d \geq 25]]_5$	$[[5208,5064,d \geq 25]]_5$
26	$[[5208,5062,d \geq 26]]_5$	$[[5208,5064,d \geq 26]]_5$
27	$[[5208,5062,d \geq 27]]_5$	$[[5208,5058,d \geq 27]]_5$
28	$[[5208,5056,d \geq 28]]_5$	$[[5208,5052,d \geq 28]]_5$
$\cdots$	$\cdots$	$\cdots$
40	$[[5208,4984,d \geq 40]]_5$	$[[5208,4980,d \geq 40]]_5$
41	$[[5208,4978,d \geq 41]]_5$	$[[5208,4974,d \geq 41]]_5$

applying the method in [8], we can compute dimensions of dual containing NNS BCH codes for $2 \leq \delta \leq \delta_{new}$.

Corollary 3.6. For $n = (q^2-1)s$, $s = \frac{(q^2+q+1)(q^2-q+1)}{3}$, $\delta_{new} = 2\lfloor \frac{q^3-1}{3} \rfloor + 1$. Let $\theta_\delta = 1 + 3\lfloor (\delta - 2)(1 - \frac{1}{q^2}) \rfloor$.

(1) If $2 \leq \delta \leq (l+1)q^2 + 1$, then $T_{[s-\delta+2,s]}$ define a NNS Hermitian dual containing BCH code of dimension $k = n - \theta_\delta$.

(2) If $(l+1)q^2 + 1 < \delta \leq (l+1)q^2 + 2 + b$, then $T_{[s-(l+1)q^2-1,s+\delta]}$ define a NNS Hermitian dual containing BCH code of dimension $k = n - \theta_\delta$.

(3) If $(l+1)q^2 + 2 + b < \delta \leq \delta_{new}$, let $j = \delta - b - (l+1)q^2 - 2$, then $T_{[s-j,s+b]}$ define a NNS Hermitian dual containing BCH code of dimension $k = n - \theta_\delta$.

According to Theorem 2.4, and the results of Corollary 3.4 and Corollary 3.6, some quantum BCH codes can be constructed from these dual containing NS and NNS BCH codes, therefore, we have following theorem.

Theorem 3.7. For $n = \frac{(q^6-1)}{3}$, $\delta_{new} = 2\lfloor \frac{q^3-1}{3} \rfloor + 1$.

(1) If $2 \leq \delta \leq \delta_{new}$, $\theta_\delta = 3\lfloor (\delta - 1)(1 - \frac{1}{q^2}) \rfloor$, then an $[[n, n - 2\theta_\delta, d \geq \delta]]_q$ quantum code can be constructed from NS BCH code.

(2) If $2 \leq \delta \leq \delta_{new}$, $\theta'_\delta = 1 + 3\lfloor (\delta - 2)(1 - \frac{1}{q^2}) \rfloor$, then an $[[n, n - 2\theta'_\delta, d \geq \delta]]_q$ quantum code can be constructed from NNS BCH code.

Remark 3.1. It is easy to check, for $2 \leq \delta \leq \delta_{new}$, except for some special cases, our quantum BCH codes constructed from NNS BCH codes are better than those constructed from q^2-ary NS BCH codes in [7] and those constructed from q-ary NS BCH codes in [13] via Steane construction, and quantum BCH codes obtained from q^2-ary NS BCH codes in [7] are better than those in [13]. For $\delta_{max} + 1 \leq \delta \leq \delta_{new}$, our quantum BCH codes constructed from NS and NNS BCH codes are all new ones. What is more, among these new quantum BCH codes, those constructed from NNS BCH codes have better parameters than those constructed from NS BCH codes. We use Table 1 and Table 2 to present evidences of these facts. Table 1 has showed that for $n = \frac{5^6-1}{3} = 5208$ and $2 \leq \delta \leq \delta_{max} = 41$, the parameters of quantum BCH codes constructed from NNS BCH are better than those constructed from NS BCH codes in [7], except the case $\delta = 26$. Table 2 has showed that for $42 = \delta_{max} + 1 \leq \delta \leq \delta_{new} = 83$ these quantum BCH codes are all new ones, and one can easily compare that the parameters of those constructed from NNS BCH codes are better than those constructed from NS BCH codes, except for $\delta = 51, 76$.

Table 2. Comparison of new quantum codes $[[n,K,d \geq \delta]]_5$ constructed from NNS BCH codes and $[[n,K',d \geq \delta]]_5$ constructed from NS BCH codes for $n = \frac{5^6-1}{3} = 5208$ and $42 \leq \delta \leq \delta_{new} = 83$

δ	$[[n,K,d \geq \delta]]_5$	$[[n,K',d \geq \delta]]_5$
42	$[[5208,4972,d \geq 42]]_5$	$[[5208,4968,d \geq 42]]_5$
43	$[[5208,4966,d \geq 43]]_5$	$[[5208,4962,d \geq 43]]_5$
44	$[[5208,4960,d \geq 44]]_5$	$[[5208,4956,d \geq 44]]_5$
45	$[[5208,4954,d \geq 45]]_5$	$[[5208,4950,d \geq 45]]_5$
$\cdots$	$\cdots$	$\cdots$
50	$[[5208,4924,d \geq 50]]_5$	$[[5208,4920,d \geq 50]]_5$
51	$[[5208,4918,d \geq 51]]_5$	$[[5208,4920,d \geq 51]]_5$
52	$[[5208,4918,d \geq 52]]_5$	$[[5208,4914,d \geq 52]]_5$
53	$[[5208,4912,d \geq 53]]_5$	$[[5208,4908,d \geq 53]]_5$
$\cdots$	$\cdots$	$\cdots$
75	$[[5208,4780,d \geq 75]]_5$	$[[5208,4776,d \geq 75]]_5$
76	$[[5208,4774,d \geq 76]_5$	$[[5208,4776,d \geq 76]]_5$
77	$[[5208,4774,d \geq 77]_5$	$[[5208,4770,d \geq 77]]_5$
78	$[[5208,4768,d \geq 78]_5$	$[[5208,4764,d \geq 78]]_5$
$\cdots$	$\cdots$	$\cdots$
83	$[[5208,4738,d \geq 83]_5$	$[[5208,4734,d \geq 83]]_5$

4 BCH codes of length $n = 3(q^2-1)(q^2+q+1)$

According to Theorem 2.5, the maximal designed distance of Hermitian dual containing NS BCH code of length $n = 3(q^2-1)(q^2+q+1)$ given in [7] is $\delta_{max} = 3q + 2$. In this section, we will first determine the maximal designed distance of Hermitian dual containing NS BCH code of length n is $\delta_{new} = \frac{q^3+3q+2}{2}$. And then show that there is a dual containing NNS BCH code of such designed distance δ_{new}. Finally, some quantum BCH codes will be constructed from these dual containing BCH codes via Hermitian construction.

4.1 Dual containing BCH codes of length $n = 3(q^2-1)(q^2+q+1)$

In this subsection, we will present the maximal designed distance of Hermitian dual containing NS BCH code of length n is $\delta_{new} = \frac{q^3+3q+2}{2}$.

Theorem 4.1. Let $n = 3(q^2 - 1)(q^2 + q + 1)$, $\delta_{new} = \frac{q^3+3q+2}{2}$. Then:

(1) The maximal designed distance of dual containing NS BCH codes of length n is δ_{new}.

(2) A NS BCH code of length n with designed distance δ contains its Hermitian dual code if and only if $\delta \leq \delta_{new}$.

Proof. Let $r = 3(q+1)$, $a = \frac{(q^2-q+1)}{3}$, then $n = r(q^3 - 1) = \frac{(q^6-1)}{a}$. Now similar to the discussions of Theorem 3.1, there exists two cases:

Case I. Firstly, we prove C_x is skew asymmetric for $x \in [1, \delta_{new} - 1]$.

(1) It is not difficult to check $1 < x(q+1) < n$.

(2) Let $x = kr + b, 0 \leq b \leq r-1$, then $x(q^3+1) = (kr + b)(q^3+1) = kr(q^3+1) + b(q^3+1) = kr(q^3-1) + b(q^3 + 1) + 2kr \equiv b(q^3+1) + 2kr(\mathrm{mod}n)$.

If $0 \leq b \leq r-2$, then $1 < b(q^3+1) + 2kr \leq (r-2)(q^3+1) + 2kr < n - 2(q^3+1) + 2kr < n$.

If $b = r-1$, from $x < \delta_{new} - 1$ and $\delta_{new} - 1 = \frac{q^3+3q}{2} - 1 = \frac{(q+1)(q-2)}{6} r + (r-3)$, we know $k \leq \frac{(q+1)(q-2)}{6} - 1$. So we has $1 < (r-1)(q^3+1) + 2kr = n - (q^3+1) + 2(k + 1)r \leq n - (q^3+1) - (q+1)^2(q-2) < n$.

Combining (1) and (2), we derive $x(q^{2t+1}+1) \not\equiv 0(\mathrm{mod}n)$, hence C_x is asymmetric.

Case II. Secondly, let $x, y \in [1, \delta_{new} - 1]$ and $x < y$, we prove C_x and C_y can not form a skew asymmetric pair. We only need to show that: for $t = 0, 1$, there must be $x + yq^{2t+1} \not\equiv 0(\mathrm{mod}n)$ and $y + xq^{2t+1} \not\equiv 0(\mathrm{mod}n)$.

(1) For $t = 0$, then $1 < x + yq < y(q+1) < n$ and $1 < y + xq < y(q+1) < n$. Hence $x + yq \not\equiv 0(\mathrm{mod}n)$ and $y + xq \not\equiv 0(\mathrm{mod}n)$.

(2) For $t = 1$, let $y = kr + b, 0 \leq b \leq r-1$, then $x + yq^3 < y(q^3+1) = y(q^3-1) + 2y = (kr+b)(q^3-1) + 2(kr+b) \equiv b(q^3-1) + 2(kr+b)(\mathrm{mod}n)$.

If $0 \leq b \leq r-2$, then $b(q^3-1) + 2(kr+b) \leq (r-2)(q^3-1) + 2(k+1)r - 4 = r(q^3-1) - 2(q^3+1) + 2(k+1)r = n - 2(q^3+1) + 2(k + 1)r \leq n - 2(q^3+1) + (q+1)^2(q-2) < n$.

If $b = r-1$, then $b(q^3-1) + 2(kr+b) = (r-1)(q^3 - 1) + 2(k+1)r - 2r(q^3-1) - (q^3+1) + 2(k+1)r = n - (q^3+1) + 2(k+1)r < n$.

Summarizing the discussions of (1) and (2), we have proved that any two C_x and C_y do not form a skew asymmetric pair.

From Case I and Case II, we know that if $x, y \in [1, \delta_{new} - 1]$, any C_x is skew asymmetric and any two C_x and C_y do not form a skew asymmetric pair.

According to the above discussions and Lemma 2.2, the theorem follows.

Arguing as in Theorem 4.1, we can show that there are also Hermitian dual containing NNS BCH codes whose designed distance is δ_{new}.

Let $s = 3(q^2 + q + 1)$, $\gamma = \frac{q-2}{3}$, $u = \frac{1}{2}(-q^3 + 6q^2 + 9q + 6)$ and $v = (q-4)(q^2+q+1) - 1$. Similar to the above discussions, one can check that each $C_{\gamma s+i}$ is skew asymmetric and any two cosets $C_{\gamma s+i}$ and $C_{\gamma s+j}$ do not form a skew asymmetric pair for $-a \leq i, j \leq b$. Thus we easily deduce the NNS BCH code with defining set $T_{[\gamma s-u, \gamma s+v]}$ is a Hermitian dual containing BCH code of length n.

Theorem 4.2. Let $n = (q^2-1)s$, $s = 3(q^2+q+1)$, $\gamma = \frac{q-2}{3}$, $\delta_{new} = \frac{q^3+3q+2}{2}$, $u = \frac{1}{2}(-q^3 + 6q^2 + 9q + 6)$ and $v = (q-4)(q^2+q+1) - 1$. Then:

(1) A NNS BCH code with defining set $T_{[\gamma s-u, \gamma s+v]}$ of length n is a Hermitian dual containing code of maximal designed distance $\delta = \delta_{new}$.

(2) A NNS BCH code of length n with designed distance $\delta \leq \delta_{new}$ and defining set $T_{[e,f]} \subset T_{[\gamma s-u, \gamma s+v]}$, then it contains its Hermitian dual code.

4.2 Dimensions of BCH codes of length $n = 3(q^2-1)(q^2+q+1)$

In this subsection, we will determine dimensions of some dual containing NS BCH codes and NNS BCH codes for $n = 3(q^2-1)(q^2+q+1)$. To simplify calculation, we restrict the designed distance δ of BCH codes with $2 \leq \delta \leq mq^2 + 1$, and construct new quantum BCH codes via Hermitian construction. Similar to the discussions of subsection 3.2, one can easily deduce the following Lemma 4.3 and Lemma 4.4, so all proofs of Lemma 4.3 and Lemma 4.4 are omitted.

Lemma 4.3. Let $n = 3(q^2 - 1)(q^2 + q + 1)$, $\delta_{new} = \frac{q^3+3q+2}{2}$, then the following hold:

(1) If $x \in [1, \delta_{new} - 1]$, C_x contains three elements.

(2) If $x, y \in [1, \delta_{new} - 1]$ and $x < y$, then $C_x = C_y$ if and only if $y = xq^2$.

Lemma 4.4. Let $n = 3(q^2-1)(q^2+q+1)$, $s = 3(q^2 + q + 1)$, $\gamma = \frac{q-2}{3}$ $u = \frac{1}{2}(-q^3 + 6q^2 + 9q + 6)$ and $v = (q - 4)(q^2+q+1) - 1$. Then the following hold:

(1) $C_{\gamma s} = \{\gamma s\}$, $|C_{\gamma s+i}| = 3$ for $-u < i < v$ and $i \neq 0$.

(2) If $-u \leq i \leq -1, 1 \leq j \leq v$, then $C_{\gamma s+i} \neq C_{\gamma s+j}$.

(3) If $1 \leq |i| \leq \lfloor \frac{q}{3} \rfloor$, then $C_{\gamma s+iq^2} = C_{\gamma s+i}$.

According to Lemma 4.3 and Lemma 4.4, the dimensions of some Hermitian dual containing NS BCH codes and NNS BCH codes can be computed as in Theorem 4.5 and Theorem 4.6, respectively.

Theorem 4.5. Let $n = 3(q^2-1)(q^2+q+1)$, $\theta_\delta = 3\lfloor(\delta - 1)(1 - \frac{1}{q^2})\rfloor$ for $2 \leq \delta \leq mq^2 + 1$ where $m = \lfloor \frac{q}{3} \rfloor$. Then:

(1) There is an $[n, n - \theta_\delta, d \geq \delta]$ Hermitian dual containing NS BCH code.

(2) An $[[n, n - 2\theta_\delta, d \geq \delta]]_q$ quantum code can be constructed from NS BCH code.

Proof. (1) From Theorem 4.1, we know that $T_{[1,\delta_{new}-1]}$ defines a Hermitian dual containing NS BCH code. If $[1, f] \subset [1, \delta_{new} - 1]$, then $T_{[1,f]}$ defines a Hermitian dual containing NS BCH code. For $2 \leq \delta \leq mq^2 + 1$, let $f \leq \delta - 1$, the NS BCH code $\mathscr{C}$ with defining set $T_{[1,\delta-1]}$

is a Hermitian dual containing BCH code of designed distance δ. From Lemma 4.3, we know that $\theta_\delta = |T_{[1,\delta-1]}| = 3\lfloor(\delta-1)(1-\frac{1}{q^2})\rfloor$. Hence, $\mathscr{C} = [n, n-\theta_\delta, d \geq \delta]$.

(2) According to (1) and Theorem 2.4, then (2) follows.

Theorem 4.6 Let $n = 3(q^2-1)(q^2+q+1)$, $\theta_\delta = 1+3\lfloor(\delta-2)(1-\frac{1}{q^2})\rfloor$ for $2 \leq \delta \leq mq^2+1$ where $m = \lfloor\frac{q}{3}\rfloor$.Then:

(1) There is an $[n, n-\theta_\delta, d \geq \delta]$ Hermitian dual containing NNS BCH code.

(2) An $[[n, n-2\theta_\delta, d \geq \delta]]_q$ quantum code can be constructed from NNS BCH code.

Proof. (1) From Theorem 4.2, we know that $T_{[\gamma s-u, \gamma s+v]}$ defines a Hermitian dual containing NNS BCH code. If $[e,f] \subset [\gamma s-u, \gamma s+v]$, then $T_{[e,f]}$ defines a Hermitian dual containing NNS BCH code. Now we construct a suitable subinterval $[e,f]$ of $[\gamma s-u, \gamma s+v]$ and get the desired Hermitian dual containing NNS BCH code. For $2 \leq \delta \leq mq^2+1$, let $f = \gamma s, e = \gamma s - \delta + 2$, then the NNS BCH code $\mathscr{C}$ with defining set $T_{[\gamma s-\delta+2, \gamma s]}$ is a Hermitian dual containing BCH code of designed distance δ. From Lemma 4.4, we know that $\theta_\delta = |T_{[\gamma s-\delta+2,\gamma s]}| = 1+3\lfloor(\delta-2)(1-\frac{1}{q^2})\rfloor$. Hence, $\mathscr{C} = [n, n-\theta_\delta, d \geq \delta]$.

Hence, According to (1) and Theorem 2.4, then (2) follows.

Table 3. Comparison of quantum codes constructed from NNS BCH code and NS BCH code for $n = \frac{(8^6-1)}{19} = 13797$ and $2 \leq \delta \leq \delta_{max} = 26$

δ	our $[[n,K,d \geq \delta]]_8$	$[[n,K',d \geq \delta]]_8$ in [13]
2	$[[13797, 13795, d \geq 2]]_8$	$[[13797, 13791, d \geq 2]]_8$
3	$[[13797, 13789, d \geq 3]]_8$	$[[13797, 13779, d \geq 3]]_8$
4	$[[13797, 13783, d \geq 4]]_8$	$[[13797, 13767, d \geq 4]]_8$
5	$[[13797, 13777, d \geq 5]]_8$	$[[13797, 13755, d \geq 5]]_8$
6	$[[13797, 13771, d \geq 6]]_8$	$[[13797, 13743, d \geq 6]]_8$
7	$[[13797, 13765, d \geq 7]]_8$	$[[13797, 13731, d \geq 7]]_8$
$\cdots$	$\cdots$	$\cdots$
24	$[[13797, 13663, d \geq 24]]_8$	$[[13797, 13551, d \geq 24]]_8$
25	$[[13797, 13657, d \geq 25]]_8$	$[[13797, 13545, d \geq 25]]_8$
26	$[[13797, 13651, d \geq 26]]_8$	$[[13797, 13533, d \geq 26]]_8$

Remark 4.1 For $2 \leq \delta \leq \delta_{max}$, we have constructed many quantum BCH codes from Hermitian dual containing NS and NNS BCH codes via Hermitian construction. The quantum BCH codes constructed from Hermitian dual containing NNS BCH codes are better than those in [7, 13]. Similar to Table1, one can show that quantum BCH codes constructed from NNS BCH codes are better than those constructed from NS BCH codes in [7]. So we only to show quantum BCH codes constructed from NNS BCH codes are better than those in [13], for details see Table 3. Table 3 has showed that for $q = 8$, $2 \leq \delta \leq \delta_{max} = 26$, our quantum BCH codes constructed from NNS BCH codes are better than those in [13]. For $\delta_{max}+1 \leq \delta \leq \delta_{new}$, one can construct quantum BCH codes from NS and NNS BCH codes given in Theorem 4.1 and Theorem 4.2, and these quantum BCH codes constructed from NS and NNS BCH codes are all new. However, we only give part results in Theorem 4.5 and Theorem 4.6, the discussions of constructing quantum BCH codes constructed from NS and NNS BCH codes for all δ can be given as in Section 3, but a little complex. So we use Table 4 to give a special case for $q = 8$. Table 4 has showed that for $q = 8$ and $27 = \delta_{max}+1 \leq \delta \leq \delta_{new} = 269$, these quantum BCH codes constructed from NS and NNS BCH codes are all new. For $27 \leq \delta \leq 216$ quantum BCH codes constructed from NNS BCH codes are better than those constructed from NS BCH codes, except in the case $\delta = 65, 129, 193$. For $221 \leq \delta \leq 269$ quantum BCH codes constructed from NNS BCH codes and NS BCH codes have same parameters.

Table 4. Comparison of new quantum codes $[[n,K,d \geq \delta]]_8$ constructed from NNS BCH codes and $[[n,K^{'},d \geq \delta]]_8$ constructed from NS BCH codes for $n = \frac{8^6-1}{19} = 13797$ and $27 = \delta_{max}+1 \leq \delta \leq \delta_{new} = 269$

δ	$[[n,K,d \geq \delta]]_8$	$[[n,K',d \geq \delta]]_8$
27	$[[13797, 13645, d \geq 27]]_8$	$[[13797, 13641, d \geq 27]]_8$
28	$[[13797, 13639, d \geq 28]]_8$	$[[13797, 13635, d \geq 28]]_8$
$\cdots$	$\cdots$	$\cdots$
64	$[[13797, 13423, d \geq 64]]_8$	$[[13797, 13419, d \geq 64]]_8$
65	$[[13797, 13417, d \geq 65]]_8$	$[[13797, 13419, d \geq 65]]_8$
66	$[[13797, 13417, d \geq 66]]_8$	$[[13797, 13413, d \geq 66]]_8$
$\cdots$	$\cdots$	$\cdots$
128	$[[13797, 13045, d \geq 128]]_8$	$[[13797, 13041, d \geq 128]]_8$
129	$[[13797, 13039, d \geq 129]]_8$	$[[13797, 13041, d \geq 129]]_8$
130	$[[13797, 13039, d \geq 130]]_8$	$[[13797, 13035, d \geq 130]]_8$
$\cdots$	$\cdots$	$\cdots$
192	$[[13797, 12667, d \geq 192]]_8$	$[[13797, 12663, d \geq 192]]_8$
193	$[[13797, 12661, d \geq 193]]_8$	$[[13797, 12663, d \geq 193]]_8$
194	$[[13797, 12661, d \geq 194]]_8$	$[[13797, 12657, d \geq 194]]_8$
$\cdots$	$\cdots$	$\cdots$
216	$[[13797, 12529, d \geq 216]]_8$	$[[13797, 12525, d \geq 216]]_8$
217	$[[13797, 21523, d \geq 217]]_8$	$[[13797, 12525, d \geq 217]]_8$
218	$[[13797, 21523, d \geq 218]]_8$	$[[13797, 12525, d \geq 218]]_8$
219	$[[13797, 21523, d \geq 219]]_8$	$[[13797, 12525, d \geq 219]]_8$
220	$[[13797, 21523, d \geq 220]]_8$	$[[13797, 12523, d \geq 220]]_8$
221	$[[13797, 12517, d \geq 221]]_8$	$[[13797, 12517, d \geq 221]]_8$
$\cdots$	$\cdots$	$\cdots$
256	$[[13797, 12307, d \geq 256]]_8$	$[[13797, 12307, d \geq 256]]_8$
257	$[[13797, 12307, d \geq 257]]_8$	$[[13797, 12307, d \geq 257]]_8$
258	$[[13797, 12301, d \geq 258]]_8$	$[[13797, 12301, d \geq 258]]_8$
$\cdots$	$\cdots$	$\cdots$
268	$[[13797, 12241, d \geq 268]]_8$	$[[13797, 12241, d \geq 268]]_8$
269	$[[13797, 12235, d \geq 269]]_8$	$[[13797, 12235, d \geq 269]]_8$

5 Conclusion

We have determined the maximal designed distances δ_{new} of imprimitive Hermitian dual containing q^2-ary NS BCH codes of length $n = \frac{(q^6-1)}{3}$ and $n = 3(q^2-1)(q^2+q+1)$ for $q = 3l+2$. We also presented two families of

Hermitian dual containing NNS BCH codes whose maximal designed distances achieving δ_{new}. At the same time, we calculated the dimensions of these NS and NNS BCH codes, then constructed many q-ary quantum BCH codes from these NS and NNS BCH codes. For $2 \leq \delta \leq \delta_{max}$, except for some special cases, our quantum BCH codes constructed from NNS BCH codes are better than the ones available in the literature. For $\delta_{max} + 1 \leq \delta \leq \delta_{new}$, our quantum BCH codes constructed from NS and NNS BCH codes are new ones. These new quantum BCH codes constructed from NNS BCH codes have better parameters than those constructed from NS BCH codes.

Acknowledgments

This work is supported by National Natural Science Foundation of China under Grant No.11071255 and Science Foundation for young teachers in College of Science, Air Force Engineering University. The authors are very grateful to the anonymous referees and the editors for their valuable comments and suggestions, which help to improve the manuscript significantly.

References

[1] P. W. Shor. Scheme for reducing decoherence in quantum computer memory. Phys. Rev. A, **52**, 2493-2496 (1995).

[2] A. M. Steane. Error correcting codes in quantum theory. Phys. Rev. Lett., **77**, 793-797 (1996).

[3] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane. Quantum error-correction via codes over GF(4). IEEE. Trans. Inf. Theory, **44**, 1369-1387 (1998).

[4] D. Gottesman. Stabilizer codes and quantum error correction. Ph.D. Thesis, California Institute of Technology. quant-ph/9707027, (1997).

[5] A. M. Steane. Enlargement of Calderbank-Shor-Steane quantum codes. IEEE. Trans. Inf. Theory, **45**, 2492-2495 (1999).

[6] S. A. Aly, A. Klappenecker and P. K. Sarvepalli. Primitive quantum BCH codes over finite fields. Proc. Int. Symp. Inf. Theory, ISIT, 1114-1118 (2006).

[7] S. A. Aly, A. Klappenecker and P. K. Sarvepalli. On quantum and classical BCH codes. IEEE. Trans. Inf. Theory, **53**, 1183-1188 (2007).

[8] G. G. La Guardia. Constructions of new families of nonbinary quantum codes. Phys. Rev. A, **80**, 1-11 (2009).

[9] W. C. Huffman and V. Pless. Fundamentals of error-correcting codes. Fundamentals of Error-Correcting Codes, (Cambridge University Press, Cambridge), (2003).

[10] F. J. Macwilliams and N. J. A. Sloane. The theory of error-correcting codes. Amsterdam, the Netherlands: North-Holland, (1977).

[11] A. Ketkar, A. Klappenecker, S. Kumar and P. K. Saverpalli. nonbinary stablizer codes over finite fields. IEEE. Trans. Inf. Theory, **52**, 4892-4914 (2006).

[12] R. Li, F. Zuo and Y. Liu. A study of skew symmetric q^2-cyclotomic coset and its application. Journal of Air Force Engineering University, **12**, 87-89 (2011).

[13] S. Ling, J. Luo and C. Xing. Generalization of Steane's enlargement construction of quantum codes and applications. IEEE. Trans. Inf. Theory, **56**, 4080-4084 (2010).

[14] R. Li, F. zuo and Y. Liu. Hermitian dual containing BCH codes and construction of new quantum codes. Quantum Inf. Comp., **13**, 0021-0036 (2013).

[15] Y. Liu, Y. Ma and Q. Feng. New quantum codes constructed from a class of imprimitive BCH codes. Int. J. Quantum Inf., **11**, 1-14 (2013).

Yuena Ma is currently a lecturer in School of Science, Air Force Engineering University. She received her M.Sc. in Applied Mathematics from Air Force Engineering University in 2006. Her research interests include Self-Orthogonal (or Dual Containing) Code, Additive Quantum Error-Correcting Code, Asymmetric Quantum Error-Correcting Code, Entanglement-Assisted Quantum Code ect.

Fangchi Liang is an Associate Professor in School of Science, Air Force Engineering University and is currently an Applied Mathematics Ph.D. Student at Xi'an Jiaotong University. His interests lie in the areas of Combinatorial Mathematics, Computational Security and Error- Correcting Coding Theory ect.

Luobin Guo is an Assistant Professor of School of Science, Air Force Engineering University. He received the Ph.D. in Applied Mathematics from Shaanxi Normal University in 1999. His main research interests are Numerical Methods, Coding and Cryptography, Quantum Error-Correcting Code, Algorithm Analysis and Design etc.