International Journal of Theoretical & Applied Sciences, 9(2): 314-319(2017)

ISSN No. (Print): 0975-1718
ISSN No. (Online): 2249-3247

On the Construction of Non Primitive Narrow Sense Quantum BCH Codes

Divya Taneja
Yadavindra College of Engineering,
Punjabi University Guru Kashi Campus, Talwandi Sabo, Punjab, India.

(Corresponding author: Divya Taneja)
(Received 25 July , 2017, accepted 14 October, 2017)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: Quantum codes can be constructed by BCH codes containing their Euclidean or Hermitian duals. In this paper new classes of classical non – primitive narrow sense BCH codes of even length $< 2(q^{m/2} + 1)$ containing their Euclidean duals codes are constructed. Further, the bound on the designed distance and the dimension of Euclidean dual containing BCH codes of length $n = \frac{(q-1)(q^3+1)}{q+1}$ and $n = \frac{(q+1)(q^3-1)}{q-1}$ are derived. Efficacy of these results made it possible to find the Quantum BCH codes using CSS construction.

Keywords: Euclidean dual containing codes, cyclotomic cosets, Bose-Chaudhuri-Hocquenghem codes (BCH codes), quantum codes.

I. INTRODUCTION

Quantum error correcting codes are affective aid to fight against inexorable errors during the quantum information processing. Many classes of self- orthogonal or dual containing classical codes have been used to design good quantum codes [1-10]. One of the important classes of classical cyclic codes is the Bose- Chaudhuri – Hocquenghem codes [16-18] which have been recently used to construct many classes of quantum codes. For a given code length and designed distance the condition under which a binary narrow-sense primitive BCH code contains its dual was given in [6]. These results were further generalised to narrow sense primitive as well as non primitive BCH codes over finite field F_q and F_{q^2}in [7,8]. The exact dimensions of BCH codes for a given range of designed distance were determined in [5, 8], [11-15], [23-25].

In particular [8], determined the dimensions and bounds on the minimum distance of these codes by employing the properties of cyclotomic q-cosets and q^2 cosets and hence many good quantum codes were constructed. In addition [8] proved the sufficient condition for a narrow sense BCH code to contain its dual, according to which the designed distance δ should be in the range $2 \le \delta \le \lfloor \kappa \rfloor$, where $\kappa = \frac{n}{q^m-1}\left(q^{\lceil m/2 \rceil} - 1 - (q-1)[m\ odd]\right)$ and for codes with even order this bound becomes $2 \le \delta \le \frac{n}{q^{m/2}+1}$. In [5] the new codes construction were shown to have better dimension than the one constructed in [8] for a fixed length and designed distance. G. G. La Guardia [13] constructed quantum BCH codes of length n a factor of $q-1$ where $ord_n(q) = 2$ andalso codes of prime length where $ord_n(q) = 2$. In [14] some new properties of cyclotomic cosets were discussed for length $q^m - 1$ based on which the bounds on designed distance and dimension of cyclic codes were determined. The authors in [15] improved the bounds on the designed distance of narrow sense and non narrow sense quantum BCH codes of length $n = \frac{q^6-1}{3}$ and $n = 3(q^2-1)(q^2+q+1)$. In [24] quantum BCH codes of length $n = \frac{q^4-1}{2}$ and $n = \frac{q^4-1}{q-1}$ were constructed with improved parameters. For length $n = q^{2m} + 1$, the maximum designed distance of Hermitian dual-containing constacyclic BCH codes was found in [25].

In extension to these works, two new classes of dual containing BCH codes are constructed. The bound on the designed distance has been found. Thus using CSS construction the two new classes of quantum BCH codes of length $n = \frac{(q+1)(q^3-1)}{q-1}$ and $n = \frac{(q-1)(q^3+1)}{q+1}$ are constructed. The maximum designed distance of these codes is found to be large and hence generating good parameters of the resulting quantum codes. Most of the authors ([5], [14-15], [23]) have improved the parameters derived by [8]. Thus codes of length $n < 2(q^{m/2} + 1)$ with even order were not considered. Since the length of the codes considered in this paper is $< 2(q^{m/2} + 1)$ and of even length with $ord_n(q) = 6$, so the codes generated in this manuscript are new.

This paper is planned as follows. Section 2 consists of the basic concepts, terminology and some known results. In section 3 and 4 construction of two families of non primitive, narrow sense classical BCH codes is presented by studying their respective cyclotomic sets. The bound on the designed distance and the dimension of the resulting codes has been found. In Section 5 quantum codes are constructed from these families and their parameters are compared with those existing in literature. Finally Section 6 consists of the conclusion part.

II. PRELIMINARIES

This section consists of the basic notations and the known results necessary for the construction of the paper.
In this paper q denotes a prime power and a finite field with q elements is denoted by F_q. For an $[n,k,d]_q$ code C, its Euclidean dual code is denoted by$C^{\perp}$. Here $\gcd(n,q) = 1$ and $m = ord_n(q)$ denotes the multiplicative order of q modulo n. The q - coset modulo n containing x is defined by $C_x = \{x, qx, q^2x \ldots, q^{k-1}x\}$ where k is the smallest positive integer such that $(q^k - 1)x \equiv 0 \ mod \ n$.
A BCH code C of length n over a finite field F_q is a cyclic code whose generator polynomial is of the form $g(x) = lcm\{M^{(b)}(x), M^{(b+1)}(x), \ldots, M^{(b+\delta-2)}(x)\}$, i.e. $g(x)$ is the monic polynomial of smallest degree over F_q having $\alpha^b, \alpha^{b+1}, \ldots, \alpha^{b+\delta-2}$ as zeros where α is a primitive element of F_{q^m} and $M^{(i)}(x)$ denotes the minimal polynomial of $\alpha^i \in F_{q^m}$. Since $M^{(s)}(x) = \prod_{i \in C_s}(x - \alpha^i)$ so $g(x) = \prod_{z \in Z}(x - \alpha^z), Z = \cup_{i=0}^{\delta-2} C_{b+i}$. The set Z is called the defining set of C
For $b = 1$, the code C is called narrow sense BCH code. For $n = q^m - 1$ it is called primitive or else non primitive BCH codes. Since the generator polynomial has a sequence of $\delta - 1$ consecutive powers of α as zeros, so by BCH bound for cyclic codes [23, p. 201(Th-8)] the lower bound on minimum distance of C is δ. Here δ is known as the designed distance.
Classical codes containing its dual can be used to construct quantum codes. The known results used in this context are
Lemma 2.1: [8, Lemma1] Assume that $\gcd(n,q) = 1$. A cyclic code of length n overF_q with defining set Z contains its Euclidean dual code if and only if $Z \cap Z^{-1} = \emptyset$, where $Z^{-1} = \{-z \ mod \ n \mid z \in Z\}$.
In other words a cyclic code is Euclidean dual containing if q- cyclotomic cosetsC_x and C_{-y}, $\forall x, y \in Z$, are distinct.
Theorem 2.2: [4, Corollary 21] (CSS construction)– If there exists a classical linear $[n,k,d]_q$ code such that $C^{\perp} \subseteq C$, then there exists an $[[n, 2k - n, \geq d]]_q$ stabilizer code that is pure to d. If the minimum distance of $C^{\perp}$ exceeds d, then the quantum code is pure and has minimum distance d.

III. BCH CODES OF LENGTH $n = \frac{(q+1)(q^3-1)}{q-1}$

In this section, for $n = \frac{(q+1)(q^3-1)}{q-1}$ by studying the properties of the q-cosets mod n we find the maximal designed distance of the dual containing narrow sense BCH codes and also find the dimension of these codes.
Now, for $n = \frac{(q+1)(q^3-1)}{q-1}$ where $q \geq 3$ is an odd prime power and $\gcd(n,q) = 1$ the following results leads us to find the parameters of dual containing BCH codes.
Lemma 3.1 The cardinality of q- ary cyclotomic coset C_x is 6, $\forall \ 1 \leq x \leq 2q, x \neq i\left(\frac{q+1}{2}\right)$ where $1 \leq i \leq 3$, and $C_{i\left(\frac{q+1}{2}\right)}$ contains three distinct elements.
Proof: Clearly or $d_n(q) = 6$. Let if possible $|C_x| < 6$ for some $1 \leq x \leq 2q$ and $x \neq i\left(\frac{q+1}{2}\right), 1 \leq i \leq 3 \Longrightarrow q^j x \equiv x \ mod \ n$ for some $0 < j < 6$. $ord_n(q) = 6$soj |6. Hence $j = 1, 2 \ or \ 3$
Case 1: When $j = 1$,$qx \equiv x \ mod \ n \Rightarrow x(q-1) \equiv 0 \ mod \ n$
But, $q - 1 \leq (q-1)x \leq 2q(q-1) < n$, leading to a contradiction.
Case 2: When $j = 2$,$q^2x \equiv x \ mod \ n \Longrightarrow x(q^2 - 1) \equiv 0 \ mod \ n$
(a) For $1 \leq x \leq q + 2$
$(q^2 - 1) \leq x(q^2 - 1) \leq (q+2)(q^2 - 1) = (q+1)(q^2 + q - 2) < n$, leading to a contradiction.
(b) For $q + 3 \leq x \leq 2q$ and $q > 3$, $x(q^2 - 1) \equiv 0 \ mod \ n \Longrightarrow x(q^2 - 1) - n \equiv 0 \ mod \ n$
$(q+1)(q-4) \leq x(q^2-1) - n \leq 2q(q^2 - 1) - (q+1)(q^2 + q + 1)$, leading to a contradiction.
For $q = 3$, it can be easily seen that $q^2x \not\equiv x \ mod \ n$
Case 3: When $j = 3$
Let *s* be an integer such that $1 \leq s \leq 4$.
For $(s-1)\left(\frac{q+1}{2}\right) + 1 \leq x < \left(\frac{q+1}{2}\right)s$,
$q^3x \equiv x \ mod \ n \Longrightarrow x(q^3 - 1) - n(x - s) \equiv 0 \ mod \ n \Longrightarrow \frac{(q^3-1)}{(q-1)}\big(-2x + s(q+1)\big) \equiv 0 \ mod \ n$
But, $0 < \frac{(q^3-1)}{(q-1)}(-2x + s(q+1)) \leq q^3 - 1 < \frac{(q+1)(q^3-1)}{q-1} = n$
hence a contradiction.
Equivalently, this means that for, $1 \leq x \leq 2q$, where $x \neq i\left(\frac{q+1}{2}\right), 1 \leq i \leq 3$, we have proved that $q^3x \not\equiv x \ mod \ n$.
Thus $|C_x| = 6, \forall \ 1 \leq x \leq 2q$ and $x \neq i\left(\frac{q+1}{2}\right), 1 \leq i \leq 3$
For $x = i\left(\frac{q+1}{2}\right), 1 \leq i \leq 3$, it can be easily verified that $|C_x| = 3$.
Lemma 3.2: $C_x \neq C_{-y}$ for $1 \leq x, y \leq 2q$.

Proof - If possible let $C_x = C_{-y} \Longrightarrow x \equiv -q^i y \ mod \ n$ where $0 \leq i \leq 5$
Case 1 If $x \equiv -q^i y \ mod \ n$ where $0 \leq i \leq 1 \Longrightarrow 2 \leq x + q^i y \leq x + qy \leq 2(q^2+q) < n$
a contradiction
Case 2 If $x \equiv -q^2 y \ mod \ n$
(a) When $1 \leq y \leq q+2$
(b) $2q^2+1 \leq x + q^2 y \leq q^2 + 4q < n$
(c) When $q+3 \leq y \leq 2q$
$2q^2 - 2q \leq x + q^2 y - n \leq q^3 - 2q^2 - 1 < n$
leading to a contradiction in both cases.
Case 3 If $x \equiv -q^3 y \ mod \ n$
Let s be an integer such that $1 \leq s \leq 4$.
For $(s-1)\left(\frac{q+1}{2}\right) + 1 \leq y \leq \left(\frac{q+1}{2}\right)s - 1$

$$x \equiv -q^3 y \ mod \ n \Longrightarrow q^3 y + x - n(y-s) \equiv 0 \ mod \ n \Longrightarrow \frac{(q^3-1)}{(q-1)}\big(-2y + s(q+1)\big) + y + x \equiv 0 \ mod \ n$$

Now $2\frac{(q^3-1)}{(q-1)} \leq \frac{(q^3-1)}{(q-1)}(-2y + s(q+1)) \leq q^3 - 1$
Hence

$$2\frac{(q^3-1)}{(q-1)} + 2 \leq \frac{(q^3-1)}{(q-1)}(-2y + s(q+1)) + y + x \leq q^3 + 4q < n$$

a contradiction.
Thus $x \not\equiv -q^3 y \ mod \ n$ for $1 \leq x, y \leq 2q$.
Case 4: If $x \equiv -q^i y \ mod \ n$ where $4 \leq i \leq 5$
$\Longrightarrow -q^{6-i} x \equiv y \ mod \ n$ which is a contradiction as in Case 1 and 2.
Lemma 3.3: For $1 \leq x, y \leq 2q$ where $y < x$, $C_x = C_y$ if and only if $x = qy$.
Proof- Since two cosets are either disjoint or identical so $x = qy \Longrightarrow C_x = C_y$.
Conversely we prove that for $x \neq qy \Longrightarrow C_x \neq C_y$.
Let if possible $C_x = C_y \Longrightarrow x \equiv q^j y \ mod \ n$ for some $1 \leq j \leq 5$.
Case 1- When $j = 1$
For $1 \leq y \leq 2q, qy < n$ and $x \neq qy$, hence $x \not\equiv qy$.
Case 2- When j = 2
a. When $1 \leq y \leq q+2, x \equiv q^2 y \ mod \ n \Longrightarrow q^2 y - x \equiv 0 \ mod \ n$.
Now,$q^2 - 2q \leq q^2 y - x \leq q^2(q+2) - 2q < n$, leading to a contradiction.
b. When $q+3 \leq y \leq 2q, x \equiv q^2 y \ mod \ n \Longrightarrow q^2 y - n - x \equiv 0 \ mod \ n$.
$q^2 - 4q - 1 \leq q^2 y - n - x \leq q^3 - 2q^2 - 2q - 2 < n$, again leading to a contradiction.
Case 3- When $j = 3$
Let sbe an integer such that $1 \leq s \leq 4$.
For $(s-1)\left(\frac{q+1}{2}\right) + 1 \leq y \leq \left(\frac{q+1}{2}\right)s - 1$

$$x \equiv q^3 y \ mod \ n \Longrightarrow q^3 y - x - n(y-s) \equiv 0 \ mod \ n \Longrightarrow \frac{(q^3-1)}{(q-1)}\big(-2y + s(q+1)\big) + y - x \equiv 0 \ mod \ n$$

Now $2\frac{(q^3-1)}{(q-1)} \leq \frac{(q^3-1)}{(q-1)}(-2y + s(q+1)) \leq q^3 - 1$
Hence

$$\begin{aligned} 2\frac{(q^3-1)}{(q-1)} + 1 - 2q \leq 2\frac{(q^3-1)}{(q-1)} + (s-1)\left(\frac{q+1}{2}\right) + 1 - 2q \leq \frac{(q^3-1)}{(q-1)}(-2y + s(q+1)) + y - x \\ \leq q^3 - 1 + \left(\frac{q+1}{2}\right)s - 1 - 1 \leq q^3 + 2q - 1 < n \end{aligned}$$

a contradiction.
Case 4: When $j = 4, x \equiv q^4 y \ mod \ n \Longrightarrow q^2 x \equiv y \ mod \ n$. As proved in Case 2 it can be proved that this is not possible.
Case 5: When $j = 5$,$x \equiv q^5 y \ mod \ n \Longrightarrow qx \equiv y \ mod \ n$.
Here $1 \leq qx, y < n$ and $y < x$. Hence $qx \not\equiv y \ mod \ n$.
Thus the cosets are distinct.
The above discussion leads to the following theorem
Theorem 3.4: Let $n = \frac{(q+1)(q^3-1)}{q-1}$ where $q \geq 3$ is an odd prime power and $\gcd(n, q) = 1$. Then there exists narrow sense BCH code $[n, n - 6\left(\left\lceil(\delta-1)\left(1-\frac{1}{q}\right)\right\rceil - s\right) + 3s, \geq \delta]$, where s is an integer representing the number of

multiples of $\left(\frac{q+1}{2}\right)$ in the range $[1, \delta - 1]$such that $s\left(\frac{q+1}{2}\right) \leq (\delta - 1) < (\mathrm{s} + 1)\left(\frac{q+1}{2}\right)$ and $2 \leq \delta \leq \delta_{max} = 2q + 1$, containing its Euclidean dual.

Proof: From the Lemmas it is clear that the defining set Z consisting of union of the distinct cyclotomic cosests C_x for $1 \leq x \leq 2q$ contains $2q$ consecutive integers and $Z \cap Z^{-1} = \emptyset$. Thus the maximum designed distance of the dual containing BCH codes is $2q + 1$.

If $= \cup_{i=1}^{\delta-1} C_i$, then the number of distinct cosets are $\left\lceil (\delta - 1)\left(1 - \frac{1}{q}\right)\right\rceil$. Also the order of the cosets C_i where i is not a multiple of $\left(\frac{q+1}{2}\right)$ is 6 and for i a multiple of $\left(\frac{q+1}{2}\right)$, C_i contains three distinct elements. For $2 \leq \delta \leq \delta_{max} = 2q + 1$ the number of multiples of $\left(\frac{q+1}{2}\right)$ in the range $[1, \delta - 1]$ is denoted by an integer s such that $s\left(\frac{q+1}{2}\right) \leq (\delta - 1) < (\mathrm{s} + 1)\left(\frac{q+1}{2}\right)$. Thus the set Z contains $\left(6\left(\left\lceil (\delta - 1)\left(1 - \frac{1}{q}\right)\right\rceil - s\right) + 3s\right)$ distinct elements.

IV. BCH CODES OF LENGTH $n = \frac{(q-1)(q^3+1)}{q+1}$

In this section we find the bound on the maximum designed distance and the dimension of Eucledian dual containing narrow sense BCH code of length= $\frac{(q-1)(q^3+1)}{q+1}$, thus obtaining a series of BCH codes. In this context following results have been proved

Lemma 4.1 The cardinality of q- coset $mod\ n$is 6, $\forall\ 1 \leq x \leq \left(\frac{q-1}{2}\right) - 1$.

Proof: Clearly for $n = \frac{(q-1)(q^3+1)}{q+1}$, $ord_n(q) = 6$.Let if possible $|C_x| < 6$ for some $1 \leq x \leq \left(\frac{q-1}{2}\right) - 1 \Longrightarrow q^j x \equiv x\ mod\ n$ for some $0 < j < 6$. The multiplicative order of q modulo n is 6 so 6|j. Hence $j = 1, 2\ or\ 3$

Case 1: When $j = 1 or\ 2$, $q^j x \equiv x\ mod\ n \Longrightarrow x(q^j - 1) \equiv 0\ mod\ n$

But

$$x(q^j - 1) \leq x(q^2 - 1) \leq \left(\left(\frac{q-1}{2}\right) - 1\right)(q^2 - 1) \leq (q - 1)\left(\frac{q^2 - 2q - 3}{2}\right) \leq (q - 1)(q^2 - q + 1) = n$$

hence it leads to a contradiction.

Case 2: When $j = 3$,

$x(q^3 - 1) \equiv 0\ mod\ n \Longrightarrow x(q^3 - 1) - nx \equiv 0\ mod\ n \Longrightarrow x[2q(q - 1)] \equiv 0\ mod\ n$

Now $2q(q - 1) \leq x[2q(q - 1)] \leq 2q(q - 1)\left(\frac{q-1}{2} - 1\right) = (q - 1)(q^2 - 3q)$

$\leq (q - 1)(q^2 - q + 1) = n$

which is a contradiction.

Thus $|C_x| = 6, \forall\ 1 \leq x \leq \left(\frac{q-1}{2}\right) - 1$.

Lemma 4.2- $C_x \neq C_{-y}$ for $1 \leq x, y \leq \left(\frac{q-1}{2}\right) - 1$.

Proof - If possible let $C_x = C_{-y}$ for some $1 \leq x, y \leq \left(\frac{q-1}{2}\right) - 1 \Longrightarrow x \equiv -q^i y\ mod\ n$ where $0 \leq i \leq 5$

Case 1 If $x \equiv -q^i y\ mod\ n$ where $0 \leq i \leq 2 \Longrightarrow 2 \leq x + q^i y \leq x + q^2 y \leq (q^2 + 1)\left(\frac{q-3}{2}\right) < n$ a contradiction

Case 2 If$x \equiv -q^3 y\ mod\ n$. Since $q^3 y \equiv (2q^2 - 2q + 1)y$ and

$(2q^2 - 2q + 1) \leq (2q^2 - 2q + 1)y \leq (2q^2 - 2q + 1)\left(\frac{q-3}{2}\right)$

$2(q^2 - q + 1) \leq \mathrm{x} + (2q^2 - 2q + 1)y \leq (q^2 - q + 1)(q - 3) < n$

contradicting our assumption.

Case 3: If $x \equiv -q^i y\ mod\ n$ where $4 \leq i \leq 5 \Longrightarrow -q^{6-i} x \equiv y\ mod\ n$ which is again a contradiction as in Case 1.

Lemma 4.3 –All cosets are distinct in the range $[1, \left(\frac{q-1}{2}\right) - 1]$.

Proof- Let if possible $C_x = C_y$ for some$1 \leq x, y \leq \left(\frac{q-1}{2}\right) - 1$where $x \neq y \Longrightarrow x \equiv q^j y\ mod\ n$ for some $1 \leq j \leq 5$. For $1 \leq x \leq \left(\frac{q-1}{2}\right) - 1, q^j x < n, 0 \leq j \leq 2$.Hence $x \not\equiv q^j y\ mod\ n$ for $1 \leq j \leq 2$. Also for $4 \leq j \leq 5$, $x \equiv q^j y\ mod\ n \Longrightarrow q^{6-j} x \equiv y\ mod\ n$ which is not possible as earlier.

If possible let $x \equiv q^3 y\ mod\ n \equiv (q^3 y - ny)\ mod\ n \equiv (2q^2 - 2q + 1)y\ mod\ n$

Now $2q(q - 1) \leq (2q^2 - 2q + 1)y \leq (2q^2 - 2q + 1)\left(\frac{q-1}{2} - 1\right)$

$= (q - 1)\left(q^2 - 3q + \frac{1}{2}\right) < (q - 1)(q^2 - q + 1) = n$

and $1 \leq x \leq \left(\frac{q-1}{2}\right) - 1$. Hence it leads to a contradiction. Thus the cosets are distinct.

As consequences of these results we have the following theorem.

Theorem 4.4: Let $n = \frac{(q-1)(q^3+1)}{q+1}$ where $q \geq 5$ is an odd prime power and $\gcd(n,q) = 1$. Then there exists a BCH code $[n, n-6(\delta-1), \geq \delta]$, where $2 \leq \delta \leq \delta_{max} = \frac{q-1}{2}$, containing its Euclidean dual.

V. QUANTUM BCH CODES AND CODE COMPARISON

In this section, quantum BCH codes of length$n = \frac{(q+1)(q^3-1)}{q-1}$ and $n = \frac{(q-1)(q^3+1)}{q+1}$are constructed. The constructed code parameters are compared with those available in literature and it is shown that the bounds on the maximum designed distance of the constructed codes have been improved.

Theorem 5.1: Let $n = \frac{(q+1)(q^3-1)}{q-1}$ where $q \geq 3$ is an odd prime power and $\gcd(n,q) = 1$.Then there exists quantum BCH code with parameters$\left[\left[n, n-2\left(6\left(\left\lceil(\delta-1)\left(1-\frac{1}{q}\right)\right\rceil - s\right)+3s\right), \geq \delta\right]\right]$, where s is an integer representing the number of multiples of $\left(\frac{q+1}{2}\right)$ in the range $[1, \delta-1]$such that $s\left(\frac{q+1}{2}\right) \leq (\delta-1) < (s+1)\left(\frac{q+1}{2}\right)$ and $2 \leq \delta \leq \delta_{max} = 2q+1$that is pure to δ.

Theorem 5.2: Let $n = \frac{(q-1)(q^3+1)}{q+1}$, where $q \geq 5$ is an odd prime power and $\gcd(n,q) = 1$.Then thereexists quantum BCH code with parameters $[[n, n-12(\delta-1), \geq \delta]]$, where $2 \leq \delta \leq \delta_{max} = \frac{q-1}{2}$ that is pure to δ.

The above two results are direct consequences of Theorem 3.1, 4.4 and 2.2.

Since the length of the codes considered in this paper is $< 2(q^{m/2}+1)$and of even length with $ord_n(q) = 6$, so the codes constructed are new. Moreover the maximum designed distance of the codes is large consequently we have constructed a series of quantum codes with better parameters. In Table 1 and 2 we have listed series of the new quantum codes constructed for a particular value of q.

Table 1: New quantum codes constructed from narrow sense BCH codes of length $n = \frac{(9+1)(9^3-1)}{9-1} = 910$ and $2 \leq \delta \leq \delta_{max} = 19$.

Δ	$[[n, k, d \geq \delta]]_9$
2	$[[910, 898, d \geq 2]]_9$
3	$[[910, 886, d \geq 3]]_9$
4	$[[910, 874, d \geq 4]]_9$
5	$[[910, 862, d \geq 5]]_9$
6	$[[910, 856, d \geq 6]]_9$
7	$[[910, 844, d \geq 7]]_9$
8	$[[910, 832, d \geq 8]]_9$
9	$[[910, 820, d \geq 9]]_9$
10	$[[910, 820, d \geq 10]]_9$
11	$[[910, 814, d \geq 11]]_9$
12	$[[910, 802, d \geq 12]]_9$
13	$[[910, 790, d \geq 13]]_9$
14	$[[910, 778, d \geq 14]]_9$
15	$[[910, 766, d \geq 15]]_9$
16	$[[910, 760, d \geq 16]]_9$
17	$[[910, 748, d \geq 17]]_9$
18	$[[910, 736, d \geq 18]]_9$
19	$[[910, 736, d \geq 19]]_9$

Table 2: New quantum codes constructed from narrow sense BCH codes of length $n = \frac{(25-1)(25^3+1)}{25+1} = 14424$ and $2 \leq \delta \leq \delta_{max} = 12$.

Δ	$[[n, k, d \geq \delta]]_{25}$
2	$[[14424, 14412, d \geq 2]]_{25}$
3	$[[14424, 14400, d \geq 3]]_{25}$
4	$[[14424, 14388, d \geq 4]]_{25}$
5	$[[14424, 14376, d \geq 5]]_{25}$
6	$[[14424, 14364, d \geq 6]]_{25}$
7	$[[14424, 14352, d \geq 7]]_{25}$
8	$[[14424, 14340, d \geq 8]]_{25}$
9	$[[14424, 14328, d \geq 9]]_{25}$
10	$[[14424, 14316, d \geq 10]]_{25}$
11	$[[14424, 14304, d \geq 11]]_{25}$
12	$[[14424, 14292, d \geq 12]]_{25}$

VI. CONCLUSION

The maximum designed distance and the dimension of non primitive narrow sense BCH codes of length $n = \frac{(q-1)(q^3+1)}{q+1}$ and $n = \frac{(q+1)(q^3-1)}{q-1}$ have been found." These codes generated a series of quantum codes using the CSS construction. The constructed codes seem to be new as these are not available in literature.

REFERENCES

[1]. Ashikhmin and E. Knill (2001). Nonbinary quantum stabilizer codes. IEEE *Trans. Inform. Theory*, **47**(7), 3065-3072.

[2]. J. Bierbrauer and Y. Edel (2000). Quantum twisted codes. *J. Comb. Designs*, **8**(3), 174-188.

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

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

[5]. G.G. La Guardia (2009). Constructions of new families of nonbinary quantum codes. *Phys. Rev. A.*, **80**(4), 042331-1–042331-11.

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

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

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

[9]. A.R. Calderbank and P.W. Shor (1996). Good quantum error correcting codes exist. *Phys. Rev. A.,* **54**, 1098- 1105.

[10]. D. Taneja, M. Gupta, R. Narula and J.S. Bhullar (2017). Construction of new quantum MDS codes derived from constacyclic codes. *International Journal of Quantum Information*, **15**(1) 1750008 1-12.

[11]. I. E. Shparlinski (1988). On the dimension of BCH codes," (in Russian) *Problemy Peredachi Informatsii*, **25**(1), 77–80.

[12]. D.-W. Yue and Z.-M. Hu (1996). On the dimension and minimum distance of BCH codes over GF(q). (in Chinese) *J. Electron.*, **18**, 263–269.

[13]. G. G. La Guardia (2014). On the construction of nonbinary quantum BCH Codes. *IEEE Trans. Inf. Theory*, **60**(3), 1528-1535.

[14]. G. G. La Guardia and M.M.S. Alves (2016). On cyclotomic cosets and code constructions. *Linear Algebra and its Applications*, **488**, 302-319.

[15]. Y. Ma, F. Liang and L. Guo (2014). Some Hermitian Dual containing BCH codes and New Quantum Codes. *Appl. Math. Inf. Sci.*, **8**(3), 1231-1237.

[16]. R. C. Bose and D. K. Ray-Chaudhuri (1960). Further results on error correcting binary group codes. *Inf. Contr.*, **3**, 279-290.

[17]. R. C. Bose and D. K. Ray-Chaudhuri (1960). On a class of error correcting binary group codes. *Inf. Contr.*, **3**, 68-79.

[18]. A. Hocquenghem (1959). Codes correcteursd erreurs. *Chiffres*, **2**(2), 147-156.

[19]. M. Grassl and T. Beth (1999). Quantum BCH codes, in Proc. 10th Int. Symp. *Theory Electr. Eng.*, 207–212.

[20]. M. Grassl, T. Beth, and M. Rötteler (2004). On optimal quantum codes. *Int. J. Quantum Inf.*, **2**(1), 757-766.

[21]. M. Hamada (2008). Concatenated quantum codes constructible in polynomial time: Efficient decoding and error correction. *IEEE Trans. Inf. Theory*, **54**(12), 5689-5704.

[22]. Z. Ma, X. Lu, K. Feng, and D. Feng (2006). On non-binary quantum BCH codes. *LNCS*, **3959**, 675-683.

[23]. F. J. MacWilliams and N. J. A. Sloane (1977). The Theory of Error-Correcting Codes. The Netherlands: North-Holland.

[24]. Qian, J., & Zhang, L. (2017). Improved constructions for nonbinary quantum BCH codes. *International Journal of Theoretical Physics*, *56*(4), 1355-1363.

[25]. Li, R., Lv, L., & Ma, Y. (2017). A class of constacyclic BCH codes and new quantum codes. *Quantum Information Processing*, *16*(3), 66.