

## On Quantum and Classical BCH Codes

Salah A. Aly, *Student Member, IEEE*,  
 Andreas Klappenecker, *Member, IEEE*, and Pradeep Kiran Sarvepalli

**Abstract**—Classical Bose–Chaudhuri–Hocquenghem (BCH) codes that contain their (Euclidean or Hermitian) dual codes can be used to construct quantum stabilizer codes; this correspondence studies the properties of such codes. It is shown that a BCH code of length  $n$  can contain its dual code only if its designed distance  $\delta = O(\sqrt{n})$ , and the converse is proved in the case of narrow-sense codes. Furthermore, the dimension of narrow-sense BCH codes with small design distance is completely determined, and – consequently – the bounds on their minimum distance are improved. These results make it possible to determine the parameters of quantum BCH codes in terms of their design parameters.

**Index Terms**—Bose–Chaudhuri–Hocquenghem (BCH) codes, dimension, dual codes, minimum distance, quantum codes.

### I. INTRODUCTION

The Bose–Chaudhuri–Hocquenghem (BCH) codes [3], [4], [7], [11] are a well-studied class of cyclic codes that have found numerous applications in classical and more recently in quantum information processing. Recall that a cyclic code of length  $n$  over a finite field  $\mathbf{F}_q$  with  $q$  elements, and  $\gcd(n, q) = 1$ , is called a BCH code with designed distance  $\delta$  if its generator polynomial is of the form

$$g(x) = \prod_{z \in Z} (x - \alpha^z), \quad Z = C_b \cup \dots \cup C_{b+\delta-2},$$

where  $C_x = \{xq^k \bmod n \mid k \in \mathbf{Z}, k \geq 0\}$  denotes the  $q$ -ary cyclotomic coset of  $x$  modulo  $n$ ,  $\alpha$  is a primitive element of  $\mathbf{F}_{q^m}$ , and  $m = \text{ord}_n(q)$  is the multiplicative order of  $q$  modulo  $n$ . Such a code is called primitive if  $n = q^m - 1$ , and narrow-sense if  $b = 1$ .

An attractive feature of a (narrow-sense) BCH code is that one can derive many structural properties of the code from the knowledge of the parameters  $n$ ,  $q$ , and  $\delta$  alone. Perhaps the most well-known facts are that such a code has minimum distance  $d \geq \delta$  and dimension  $k \geq n - (\delta - 1)\text{ord}_n(q)$ . In this correspondence, we will show that a necessary condition for a narrow-sense BCH code which contains its Euclidean dual code is that its designed distance  $\delta = O(qn^{1/2})$ . We also derive a sufficient condition for dual containing BCH codes. Moreover, if the codes are primitive, these conditions are same. These results allow us to derive families of quantum stabilizer codes. Along the way, we find new results concerning the minimum distance and dimension of classical BCH codes.

To put our results into context, we give a brief overview of related work. This correspondence was motivated by problems concerning quantum BCH codes; specifically, our goal was to derive the parameters of the quantum codes as a function of the design parameters. Examples of certain binary quantum BCH codes have been given by many authors, see, for example, [5], [8], [10], [19]. Steane [18] gave a simple criterion to decide when a binary narrow-sense primitive BCH

Manuscript received April 13, 2006; revised October 31, 2006. This work was supported by the National Science Foundation CAREER award CCF 0347310, the National Sciences Foundation under Grants CCF 0218582 and CCF 0622201, and a Texas A&M TITF initiative.

The authors are with the Department of Computer Science, Texas A&M University, College Station, TX 77843 USA (e-mail: salah@cs.tamu.edu; klappi@cs.tamu.edu; pradeep@cs.tamu.edu).

Communicated by A. Winter, Associate Editor for Quantum Information Theory.

Digital Object Identifier 10.1109/TIT.2006.890730

code contains its dual, given the design distance and the length of the code. We generalize Steane’s result in various ways, in particular, to narrow-sense (not necessarily primitive) BCH codes over arbitrary finite fields with respect to Euclidean and Hermitian duality. These results allow one to derive quantum BCH codes; however, it remains to determine the dimension, purity, and minimum distance of such quantum codes.

The dimension of a classical BCH code can be bounded by many different standard methods, see [2], [12], [15] and the references therein. An upper bound on the dimension was given by Shparlinski [17], see also [14, Ch. 17]. More recently, the dimension of primitive narrow-sense BCH codes of designed distance  $\delta < q^{\lceil m/2 \rceil} + 1$  was apparently determined by Yue and Hu [22], according to [21]. We generalize their result and determine the dimension of narrow-sense BCH codes that are not necessarily primitive for a certain range of designed distances. As desired, this result allows us to explicitly obtain the dimension of the quantum codes without computation of cyclotomic cosets.

The purity and minimum distance of a quantum BCH code depend on the minimum distance and dual distance of the associated classical code. In general, it is a difficult problem to determine the true minimum distance of BCH codes, see [6]. A lower bound on the dual distance can be given by the Carlitz-Uchiyama-type bounds when the number of field elements is prime, see, for example, [15, page 280] and [20]. Many authors have determined the true minimum distance of BCH codes in special cases, see, for instance, [16], [21].

This paper also extends our previous work on *primitive* narrow-sense BCH codes [1], simplifies some of the proofs and generalizes many of the results to the nonprimitive case.

### Notation

We denote the ring of integers by  $\mathbf{Z}$  and the finite field with  $q$  elements by  $\mathbf{F}_q$ . We use the bracket notation of Iverson and Knuth that associates to  $[statement]$  the value 1 if *statement* is true, and 0 otherwise. For instance, we have  $[k \text{ even}] = k - 1 \bmod 2$  and  $[k \text{ odd}] = k \bmod 2$  for an integer  $k$ . The Euclidean dual code  $C^\perp$  of a code  $C \subseteq \mathbf{F}_q^n$  is given by  $C^\perp = \{y \in \mathbf{F}_q^n \mid x \cdot y = 0 \text{ for all } x \in C\}$ , while the Hermitian dual of  $C \subseteq \mathbf{F}_{q^2}^n$  is defined as  $C^{\perp h} = \{y \in \mathbf{F}_{q^2}^n \mid y^q \cdot x = 0 \text{ for all } x \in C\}$ . We denote a narrow-sense BCH code of length  $n$  over  $\mathbf{F}_q$  with designed distance  $\delta$  by  $BCH(n, q; \delta)$ , and we omit the parameter  $q$  if the finite field is clear from the context.

### II. EUCLIDEAN DUAL CODES

Recall that one can construct quantum stabilizer codes using classical codes that contain their duals. In this section, our goal is to find such classical codes. Steane showed that a primitive, narrow-sense, binary BCH code of length  $2^m - 1$  contains its dual if and only if its designed distance  $\delta$  satisfies  $\delta \leq 2^{\lceil m/2 \rceil} - 1$ , see [18]. We generalize this result in various ways.

*Lemma 1:* Let  $C$  be a cyclic code of length  $n$  over the finite field  $\mathbf{F}_q$  such that  $\gcd(n, q) = 1$ , and let  $Z$  be the defining set of  $C$ . The code  $C$  contains its Euclidean dual code if and only if  $Z \cap Z^{-1} = \emptyset$ , where  $Z^{-1}$  denotes the set  $Z^{-1} = \{-z \bmod n \mid z \in Z\}$ .

*Proof:* See [9, Theorem 2]. See also [12, Theorem 4.4.11].  $\square$

Let us first consider narrow-sense BCH codes of length  $n$  such that the multiplicative order of  $q$  modulo  $n$  equals 1; for example, Reed–Solomon codes belong to this class of codes. We can avoid some special cases in our subsequent arguments by treating this case separately. Furthermore, the next lemma nicely illustrates the proof technique that will be used throughout this section, so it can serve as a warm-up exercise.

**Lemma 2:** Suppose that  $q$  is a power of a prime and  $n$  is a positive integer such that  $q \equiv 1 \pmod n$ . We have  $\mathcal{BCH}(n, q; \delta)^\perp \subseteq \mathcal{BCH}(n, q; \delta)$  if and only if the designed distance  $\delta$  is in the range  $2 \leq \delta \leq \delta_{\max} = \lfloor (n+1)/2 \rfloor$ .

*Proof:* The defining set  $Z$  of  $\mathcal{BCH}(n, q; \delta)$  is given by  $Z = \{1, \dots, \delta - 1\}$ , since  $q$  has multiplicative order 1 modulo  $n$ , and therefore all cyclotomic cosets are singleton sets. If  $\mathcal{BCH}(n, q; \delta)^\perp \subseteq \mathcal{BCH}(n, q; \delta)$ , then by Lemma 1,  $Z \cap Z^{-1} = \emptyset$ . If  $x \in Z$ , then  $n - x \notin Z$  and  $n - x > x$ ; hence,  $\delta_{\max} \leq \lfloor (n+1)/2 \rfloor$ . Conversely, if  $\delta \leq \lfloor (n+1)/2 \rfloor$ , then

$$\begin{aligned} \min Z^{-1} &= \min\{n-1, \dots, n-\delta+1\} = n-\delta+1 \\ &\geq n - \lfloor (n+1)/2 \rfloor + 1 = \lceil (n+1)/2 \rceil \geq \delta_{\max}; \end{aligned}$$

hence,  $Z \cap Z^{-1} = \emptyset$  and Lemma 1 implies that  $\mathcal{BCH}(n, q; \delta)^\perp \subseteq \mathcal{BCH}(n, q; \delta)$ .  $\square$

If the multiplicative order  $m$  of  $q$  modulo  $n$  is larger than 1, then the defining set of the code has a more intricate structure, so proofs become more involved. The next theorem gives a sufficient condition on the designed distances for which the dual code of a narrow-sense BCH code is self-orthogonal.

**Theorem 3:** Suppose that  $m = \text{ord}_n(q)$ . If the designed distance  $\delta$  is in the range  $2 \leq \delta \leq \delta_{\max} = \lfloor \kappa \rfloor$ , where

$$\kappa = \frac{n}{q^m - 1} (q^{\lceil m/2 \rceil} - 1 - (q-2)[m \text{ odd}]) \quad (1)$$

then  $\mathcal{BCH}(n, q; \delta)^\perp \subseteq \mathcal{BCH}(n, q; \delta)$ .

*Proof:* It suffices to show that

$$\mathcal{BCH}(n, q; \delta_{\max})^\perp \subseteq \mathcal{BCH}(n, q; \delta_{\max})$$

holds, since  $\mathcal{BCH}(n, q; \delta)$  contains  $\mathcal{BCH}(n, q; \delta_{\max})$ , and the claim follows from these two facts.

Seeking a contradiction, we assume that  $\mathcal{BCH}(n, q; \delta_{\max})$  does not contain its dual. Let  $Z = C_1 \cup \dots \cup C_{\delta_{\max}-1}$  be the defining set of  $\mathcal{BCH}(n, q; \delta_{\max})$ . By Lemma 1,  $Z \cap Z^{-1} \neq \emptyset$ , which means that there exist two elements  $x, y \in \{1, \dots, \delta_{\max}-1\}$  such that  $y \equiv -xq^j \pmod n$  for some  $j \in \{0, 1, \dots, m-1\}$ , where  $m$  is the multiplicative order of  $q$  modulo  $n$ . Since  $\text{gcd}(q, n) = 1$  and  $q^m \equiv 1 \pmod n$ , we also have  $x \equiv -yq^{m-j} \pmod n$ . Thus, exchanging  $x$  and  $y$  if necessary, we can even assume that  $j$  is in the range  $0 \leq j \leq \lfloor m/2 \rfloor$ . It follows from (1) that

$$\begin{aligned} 1 \leq xq^j &\leq (\delta_{\max} - 1)q^j \\ &\leq \frac{n}{q^m - 1} (q^m - q^j - q^j(q-2)[m \text{ odd}]) - q^j \\ &< n, \end{aligned}$$

for all  $j$  in the range  $0 \leq j \leq \lfloor m/2 \rfloor$ . Since  $1 \leq xq^j < n$  and  $1 \leq y < n$ , we can infer from  $y \equiv -xq^j \pmod n$  that  $y = n - xq^j$ . But this implies

$$\begin{aligned} y &\geq n - xq^{\lfloor m/2 \rfloor} \\ &\geq n - \frac{n}{q^m - 1} (q^m - q^{\lfloor m/2 \rfloor} \\ &\quad - q^{\lfloor m/2 \rfloor} (q-2)[m \text{ odd}]) + q^{\lfloor m/2 \rfloor} \\ &= \frac{n}{q^m - 1} (q^{\lfloor m/2 \rfloor} - 1 + q^{\lfloor m/2 \rfloor} (q-2)[m \text{ odd}]) \\ &\quad + q^{\lfloor m/2 \rfloor} \\ &\geq \delta_{\max} \end{aligned}$$

contradicting the fact that  $y < \delta_{\max}$ .  $\square$

Now we will derive a necessary condition on the design distance of narrow-sense, nonprimitive BCH codes that contain their duals.

**Theorem 4:** Suppose that  $m = \text{ord}_n(q)$ . If the designed distance  $\delta$  exceeds  $\delta_{\max} = \lfloor qn^{1/2} \rfloor$ , then  $\mathcal{BCH}(n, q; \delta)^\perp \not\subseteq \mathcal{BCH}(n, q; \delta)$ .

*Proof:* Let  $n = n_0 + n_1q + \dots + n_{d-1}q^{d-1}$ , where  $0 \leq n_i \leq q-1$  and  $\delta \geq \delta_{\max} + 1$ . Then the defining set  $Z \supseteq \{1, \dots, \lfloor qn^{1/2} \rfloor\}$ . We will show that  $Z \cap Z^{-1} \neq \emptyset$ . Let

$$\begin{aligned} s &= \sum_{i=\lfloor d/2 \rfloor}^{d-1} n_i q^{i-\lfloor d/2 \rfloor} \\ s &\leq (q-1) \sum_{i=\lfloor d/2 \rfloor}^{d-1} q^{i-\lfloor d/2 \rfloor} = q^{\lceil d/2 \rceil} - 1 < q^{\lceil d/2 \rceil}. \end{aligned}$$

Since  $q^{d-1} < n < q^d$ , we have  $q^{(d+1)/2} < qn^{1/2} < q^{(d+2)/2}$ . If  $d$  is even then  $\lceil d/2 \rceil < (d+1)/2$  and if  $d$  is odd, then  $\lceil d/2 \rceil \leq (d+1)/2$ . Hence we have  $s < q^{\lceil d/2 \rceil} \leq q^{(d+1)/2} < qn^{1/2}$ . Therefore  $s \in Z$ . Now consider

$$\begin{aligned} s' &= n - sq^{\lfloor d/2 \rfloor} = \sum_{i=0}^{d-1} n_i q^i - q^{\lfloor d/2 \rfloor} \sum_{i=\lfloor d/2 \rfloor}^{d-1} n_i q^{i-\lfloor d/2 \rfloor} \\ &= \sum_{i=0}^{\lfloor d/2 \rfloor - 1} n_i q^i < q^{\lfloor d/2 \rfloor} \\ &< q^{(d+1)/2} < qn^{1/2}. \end{aligned}$$

Hence  $s' \in Z$  and by definition  $s' \in Z^{-1}$ , which implies  $Z \cap Z^{-1} \neq \emptyset$ ; by Lemma 1 it follows that  $\mathcal{BCH}(n, q; \delta)^\perp \not\subseteq \mathcal{BCH}(n, q; \delta)$ .  $\square$

The condition we just derived can be strengthened under some restrictions. Especially, if the constant  $\kappa$  in (1) is integral, then we can derive a necessary and sufficient condition as shown in the following theorem.

**Theorem 5:** We keep the notation of Theorem 4. Suppose that  $\kappa$  is integral, and that  $m \geq 2$ . We have  $\mathcal{BCH}(n, q; \delta)^\perp \subseteq \mathcal{BCH}(n, q; \delta)$  if and only if the designed distance  $\delta$  is in the range  $2 \leq \delta \leq \delta_{\max} = \kappa$ .

*Proof:* Suppose that  $\mathcal{BCH}(n, q; \delta)^\perp \subseteq \mathcal{BCH}(n, q; \delta)$ . Seeking a contradiction, we assume that  $\delta > \delta_{\max}$ ; thus,  $\delta_{\max}$  is contained in the defining set  $Z$  of  $\mathcal{BCH}(n, q; \delta)$ . If  $m$  is even, then

$$\begin{aligned} -\delta_{\max} q^{\lfloor m/2 \rfloor} &\equiv -\frac{nq^{\lfloor m/2 \rfloor}}{q^{\lfloor m/2 \rfloor} + 1} \equiv -n + \frac{n}{q^{\lfloor m/2 \rfloor} + 1} \\ &\equiv \delta_{\max} \pmod n \end{aligned}$$

hence,  $\delta_{\max} \in Z \cap Z^{-1} \neq \emptyset$ . If  $m$  is odd, then

$$\begin{aligned} -\delta_{\max} q^{\lfloor m/2 \rfloor} &\equiv -n(q^m - q^{\lfloor m/2 \rfloor} + q^{\lfloor m/2 \rfloor}) / (q^m - 1) \\ &\equiv n(q^{\lfloor m/2 \rfloor} - q^{\lfloor m/2 \rfloor} - 1) / (q^m - 1) \\ &\equiv s \pmod n. \end{aligned}$$

By definition,  $s \in Z^{-1}$ ; furthermore,  $s < \delta_{\max}$ , so  $s \in Z \cap Z^{-1} \neq \emptyset$ . In both cases,  $m$  even and odd, we found that  $Z \cap Z^{-1}$  is not empty, so  $\mathcal{BCH}(n, q; \delta)$  cannot contain its Euclidean dual code, contradiction. The converse follows from Theorem 3.  $\square$

As a consequence of Theorem 5, we have the following test for primitive narrow-sense BCH codes that contain their duals.  $\square$

*Corollary 6:* A primitive narrow-sense BCH code of length  $n = q^m - 1$ ,  $m \geq 2$ , over the finite field  $\mathbf{F}_q$  contains its Euclidean dual code if and only if its designed distance  $\delta$  satisfies

$$2 \leq \delta \leq \delta_{\max} = q^{\lceil m/2 \rceil} - 1 - (q-2)[m \text{ odd}].$$

We observe that a narrow-sense BCH code containing its Euclidean dual code must have a small designed distance ( $\delta = O(\sqrt{n})$ ), when the multiplicative order of  $q$  modulo  $n$  is greater than one. This raises the question whether one can allow larger designed distances by considering nonnarrow-sense BCH codes. Our next result shows that this is not possible, at least in the case of primitive codes.

*Theorem 7:* Let  $C$  be a primitive (not necessarily narrow-sense) BCH code of length  $n = q^m - 1$  over  $\mathbf{F}_q$  with designed distance  $\delta$ . If  $m > 1$  and  $\delta$  exceeds

$$\delta_{\max} = \begin{cases} q^{m/2} - 1, & m \equiv 0 \pmod{2}, \\ 2(q^{(m+1)/2} - q + 1), & m \equiv 1 \pmod{2}, \end{cases}$$

then  $C$  cannot contain its Euclidean dual.

*Proof:* Let the defining set of  $C$  be  $Z = C_b \cup C_{b+1} \cup \dots \cup C_{b+\delta-2}$ . We will show that if  $\delta > \delta_{\max}$  then  $Z \cap Z^{-1} \neq \emptyset$ . If  $0 \in Z$ , then  $0 \in Z^{-1}$ , so  $Z \cap Z^{-1} \neq \emptyset$ . Therefore, we can henceforth assume that  $0 \notin Z$ , which implies  $b \geq 1$  and  $b + \delta - 2 < n$ .

1) Suppose that  $m$  is even; thus,  $\delta_{\max} = q^{m/2} - 1$ . If  $\delta > \delta_{\max}$  then the defining set  $Z$  contains an element of the form  $s = \alpha \delta_{\max}$  for some integer  $\alpha$ . However

$$\begin{aligned} -s q^{m/2} &\equiv -\alpha(q^{m/2} - 1)q^{m/2} \equiv \alpha(q^{m/2} - 1) \\ &\equiv s \pmod{n}. \end{aligned}$$

Hence,  $s \in Z \cap Z^{-1} \neq \emptyset$ .

2) Suppose that  $m > 1$  is odd; thus,  $\delta_{\max} = 2q^{(m+1)/2} - 2q + 2$ . If  $\delta > \delta_{\max}$  then there exists an integer  $\alpha$  such that two multiples of  $\delta' = \delta_{\max}/2$  are contained in the range  $b \leq (\alpha - 1)\delta' < \alpha\delta' \leq b + \delta - 2$ . Since  $b \geq 1$  and  $\alpha\delta' < n$ , it follows that  $2 \leq \alpha \leq q^{(m-1)/2}$ .

The defining set  $Z$  of the code contains the element  $s = \alpha\delta'$ . The number  $s' = \alpha(q^{(m+1)/2} - q^{(m-1)/2} - 1)$  lies in the range  $0 \leq s' \leq s$  and satisfies  $-s q^{(m-1)/2} \equiv s' \pmod{n}$ , so  $s' \in Z^{-1}$ . Suppose that  $b \leq s'$ . Then  $s' \in Z$ , which implies  $Z \cap Z^{-1} \neq \emptyset$ . Suppose that  $s' < b$ . Since  $b \leq (\alpha - 1)\delta'$ , we obtain the inequality  $s' < (\alpha - 1)\delta'$ ; solving for  $\alpha$  shows that  $\alpha \geq q$ ; thus,  $q \leq \alpha \leq q^{(m-1)/2}$ . Let  $t' = (\alpha - 1)(q^{(m+1)/2} - 1) + q^{(m-1)/2} - 1$ ; it is easy to check that  $t'$  is in the range  $(\alpha - 1)\delta' \leq t' \leq \alpha\delta'$  when  $\alpha \geq q$ ; thus,  $t' \in Z$ . Further, let  $t = s - (\alpha - q + 1)$ ; since  $t \geq s - \delta'$ , we have  $t \in Z$  as well. Since  $-t q^{(m-1)/2} \equiv t' \pmod{n}$ , we can conclude that  $t' \in Z \cap Z^{-1} \neq \emptyset$ .

Therefore, we can conclude that if the designed distance of  $C$  is greater than  $\delta_{\max}$ , then  $Z \cap Z^{-1} \neq \emptyset$ , which proves the claim thanks to Lemma 1.  $\square$

### III. DIMENSION AND MINIMUM DISTANCE

While the results in the previous section are sufficient to tell us when we can construct quantum BCH codes, they are still unsatisfactory because we do not know the dimension of these codes. To this end, we determine the dimension of narrow-sense BCH codes of length  $n$  with minimum distance  $d = O(n^{1/2})$ . It turns out that these results on dimension also allow us to sharpen the estimates of the true distance of some BCH codes.

First, we make some simple observations about cyclotomic cosets that are essential in our proof.

*Lemma 8:* Let  $n$  be a positive integer and  $q$  be a power of a prime such that  $\gcd(n, q) = 1$  and  $q^{\lceil m/2 \rceil} < n \leq q^m - 1$ , where  $m = \text{ord}_n(q)$ . The cyclotomic coset  $C_x = \{xq^j \pmod{n} \mid 0 \leq j < m\}$  has cardinality  $m$  for all  $x$  in the range  $1 \leq x \leq nq^{\lceil m/2 \rceil}/(q^m - 1)$ .

*Proof:* If  $m = 1$ , then  $|C_x| = 1$  for all  $x$  and the statement is trivially true. Therefore, we can assume that  $m > 1$ . Seeking a contradiction, we suppose that  $|C_x| < m$ , meaning that there exists a divisor  $j$  of  $m$  such that  $xq^j \equiv x \pmod{n}$ , or equivalently, that  $x(q^j - 1) \equiv 0 \pmod{n}$  holds.

Suppose that  $m$  is even. The divisor  $j$  of  $m$  must be in the range  $1 \leq j \leq m/2$ . However,  $x(q^j - 1) \leq nq^{m/2}(q^{m/2} - 1)/(q^m - 1) < n$ ; hence  $x(q^j - 1) \not\equiv 0 \pmod{n}$ , contradicting the assumption  $|C_x| < m$ .

Suppose that  $m$  is odd. The divisor  $j$  of  $m$  must be in the range  $1 \leq j \leq m/3$ . Since  $q^{(m+1)/2} \leq q^{2m/3}$  for  $m \geq 3$ , we have

$$\begin{aligned} x(q^j - 1) &\leq nq^{(m+1)/2}(q^{m/3} - 1)/(q^m - 1) \\ &\leq nq^{2m/3}(q^{m/3} - 1)/(q^m - 1) < n. \end{aligned}$$

Therefore,  $x(q^j - 1) \not\equiv 0 \pmod{n}$ , contradicting the assumption  $|C_x| < m$ .  $\square$

The following observation tells us when some cyclotomic cosets are disjoint.

*Lemma 9:* Let  $n \geq 1$  be an integer and  $q$  be a power of a prime such that  $\gcd(n, q) = 1$  and  $q^{\lceil m/2 \rceil} < n \leq q^m - 1$ , where  $m = \text{ord}_n(q)$ . If  $x$  and  $y$  are distinct integers in the range  $1 \leq x, y \leq \min\{\lfloor nq^{\lceil m/2 \rceil}/(q^m - 1) - 1 \rfloor, n - 1\}$  such that  $x, y \not\equiv 0 \pmod{q}$ , then the  $q$ -ary cyclotomic cosets of  $x$  and  $y$  modulo  $n$  are distinct.

*Proof:* If  $m = 1$ , then clearly  $C_x = \{x\}$ ,  $C_y = \{y\}$  and distinct  $x, y$  implies that  $C_x$  and  $C_y$  are disjoint. If  $m > 1$ , then  $x, y \leq \lfloor nq^{\lceil m/2 \rceil}/(q^m - 1) - 1 \rfloor < n - 1$ . The set  $S = \{xq^j \pmod{n}, yq^j \pmod{n} \mid 0 \leq j \leq \lfloor m/2 \rfloor\}$  contains  $2(\lfloor m/2 \rfloor + 1) \geq m + 1$  elements, since  $q^{\lfloor m/2 \rfloor} \times \lfloor nq^{\lceil m/2 \rceil}/(q^m - 1) - 1 \rfloor < n$  and, thus, no two elements are identified modulo  $n$ . If we assume that  $C_x = C_y$ , then the preceding observation would imply that  $|C_x| = |C_y| \geq |S| \geq m + 1$ , which is impossible since the maximal size of a cyclotomic coset is  $m$ . Hence, the cyclotomic cosets  $C_x$  and  $C_y$  must be disjoint.  $\square$

With these results in hand, we can now derive the dimension of narrow-sense BCH codes.

*Theorem 10:* Let  $q$  be a prime power and  $\gcd(n, q) = 1$  with  $\text{ord}_n(q) = m$ . Then a narrow-sense BCH code of length  $q^{\lceil m/2 \rceil} < n \leq q^m - 1$  over  $\mathbf{F}_q$  with designed distance  $\delta$  in the range  $2 \leq \delta \leq \min\{\lfloor nq^{\lceil m/2 \rceil}/(q^m - 1) \rfloor, n\}$  has dimension

$$k = n - m[(\delta - 1)(1 - 1/q)]. \quad (2)$$

*Proof:* Let the defining set of  $\mathcal{BCH}(n, q; \delta)$  be  $Z = C_1 \cup C_2 \dots \cup C_{\delta-1}$ ; a union of at most  $\delta - 1$  consecutive cyclotomic cosets. However, when  $1 \leq x \leq \delta - 1$  is a multiple of  $q$ , then  $C_{x/q} = C_x$ . Therefore, the number of cosets is reduced by  $\lfloor (\delta - 1)/q \rfloor$ . By Lemma 9, if  $x, y \not\equiv 0 \pmod{q}$  and  $x \neq y$ , then the cosets  $C_x$  and  $C_y$  are disjoint. Thus,  $Z$  is the union of  $(\delta - 1) - \lfloor (\delta - 1)/q \rfloor = \lceil (\delta - 1)(1 - 1/q) \rceil$  distinct cyclotomic cosets. By Lemma 8, all these cosets have cardinality  $m$ . Therefore, the degree of the generator polynomial is  $m \lceil (\delta - 1)(1 - 1/q) \rceil$ , which proves our claim about the dimension of the code.  $\square$

As a consequence of the dimension result, we can tighten the bounds on the minimum distance of narrow-sense BCH codes generalizing a result due to Farr, see [15, p. 259].

*Corollary 11:* A  $\mathcal{BCH}(n, q; \delta)$  code

- 1) with length in the range  $q^{\lceil m/2 \rceil} < n \leq q^m - 1$ ,  $m = \text{ord}_n(q)$ ;
- 2) and designed distance in the range

$$2 \leq \delta \leq \min\{\lfloor nq^{\lceil m/2 \rceil}/(q^m - 1) \rfloor, n\};$$

3) such that

$$\sum_{i=0}^{\lfloor (\delta+1)/2 \rfloor} \binom{n}{i} (q-1)^i > q^{m \lceil (\delta-1)(1-1/q) \rceil}. \quad (3)$$

has minimum distance  $d = \delta$  or  $\delta + 1$ ; if  $\delta \equiv 0 \pmod{q}$ , then  $d = \delta + 1$ .

*Proof:* Seeking a contradiction, we assume that the minimum distance  $d$  of the code satisfies  $d \geq \delta + 2$ . We know from Theorem 10 that the dimension of the code is  $k = n - m \lceil (\delta - 1)(1 - 1/q) \rceil$ . If we substitute this value of  $k$  into the sphere-packing bound  $q^k \sum_{i=0}^{\lfloor (d-1)/2 \rfloor} \binom{n}{i} (q-1)^i \leq q^n$ , then we obtain

$$\begin{aligned} \sum_{i=0}^{\lfloor (\delta+1)/2 \rfloor} \binom{n}{i} (q-1)^i &\leq \sum_{i=0}^{\lfloor (d-1)/2 \rfloor} \binom{n}{i} (q-1)^i \\ &\leq q^{m \lceil (\delta-1)(1-1/q) \rceil} \end{aligned}$$

but this contradicts condition (3); hence,  $\delta \leq d \leq \delta + 1$ .

If  $\delta \equiv 0 \pmod{q}$ , then the cyclotomic coset  $C_\delta$  is contained in the defining set  $Z$  of the code because  $C_\delta = C_{\delta/q}$ . Thus, the BCH bound implies that the minimum distance must be at least  $\delta + 1$ .  $\square$

We conclude this section with a minor result on the dual distance of BCH codes which will be needed later for determining the purity of quantum codes.

*Lemma 12:* Suppose that  $C$  is a narrow-sense BCH code of length  $n$  over  $\mathbf{F}_q$  with designed distance  $2 \leq \delta \leq \delta_{\max} = \lfloor n(q^{\lceil m/2 \rceil} - 1 - (q-2)[m \text{ odd}]) / (q^m - 1) \rfloor$ , then the dual distance  $d^\perp \geq \delta_{\max} + 1$ .

*Proof:* Let  $N = \{0, 1, \dots, n-1\}$  and  $Z_\delta$  be the defining set of  $C$ . We know that  $Z_{\delta_{\max}} \supseteq Z_\delta \supset \{1, \dots, \delta-1\}$ . Therefore,  $N \setminus Z_{\delta_{\max}} \subseteq N \setminus Z_\delta$ . Further, we know that  $Z \cap Z^{-1} = \emptyset$  if  $2 \leq \delta \leq \delta_{\max}$  from Lemma 1 and Theorem 3. Therefore,  $Z_{\delta_{\max}}^{-1} \subseteq N \setminus Z_{\delta_{\max}} \subseteq N \setminus Z_\delta$ .

Let  $T_\delta$  be the defining set of the dual code. Then  $T_\delta = (N \setminus Z_\delta)^{-1} \supseteq Z_{\delta_{\max}}$ . Moreover  $\{0\} \in N \setminus Z_\delta$  and therefore  $T_\delta$ . Thus there are at least  $\delta_{\max}$  consecutive roots in  $T_\delta$ . Thus the dual distance  $d^\perp \geq \delta_{\max} + 1$ .  $\square$

#### IV. HERMITIAN DUAL CODES

Suppose that  $C$  is a linear code of length  $n$  over  $\mathbf{F}_{q^2}$ . Recall that its Hermitian dual code is defined by  $C^{\perp_h} = \{y \in \mathbf{F}_{q^2}^n \mid y^q \cdot x = 0 \text{ for all } x \in C\}$ , where  $y^q = (y_1^q, \dots, y_n^q)$  denotes the conjugate of the vector  $y = (y_1, \dots, y_n)$ .

*Lemma 13:* Assume that  $\gcd(n, q) = 1$ . A cyclic code of length  $n$  over  $\mathbf{F}_{q^2}$  with defining set  $Z$  contains its Hermitian dual code if and only if  $Z \cap Z^{-q} = \emptyset$ , where  $Z^{-q} = \{-qz \pmod{n} \mid z \in Z\}$ .

*Proof:* Let  $N = \{0, 1, \dots, n-1\}$ . If  $g(x) = \prod_{z \in Z} (x - \alpha^z)$  is the generator polynomial of a cyclic code  $C$ , then  $h^\dagger(x) = \prod_{z \in N \setminus Z} (x - \alpha^{-qz})$  is the generator polynomial of  $C^{\perp_h}$ . Thus,  $C^{\perp_h} \subseteq C$  if and only if  $g(x)$  divides  $h^\dagger(x)$ . The latter condition is equivalent to  $Z \subseteq \{-qz \mid z \in N \setminus Z\}$ , which can also be expressed as  $Z \cap Z^{-q} = \emptyset$ .  $\square$

Now similar to Theorem 3, we will derive a sufficient condition for BCH codes that contain their Hermitian duals.

*Theorem 14:* Suppose that  $m = \text{ord}_n(q^2)$ . If the designed distance  $\delta$  satisfies  $2 \leq \delta \leq \delta_{\max}$ , where

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

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

*Proof:* Since  $\mathcal{BCH}(n, q^2; \delta)$  contains  $\mathcal{BCH}(n, q^2; \delta_{\max})$ , it suffices to show that  $\mathcal{BCH}(n, q^2; \delta_{\max})^{\perp_h} \subseteq \mathcal{BCH}(n, q^2; \delta_{\max})$  holds.

Seeking a contradiction, we assume that  $\mathcal{BCH}(n, q^2; \delta_{\max})$  does not contain its dual. Let  $Z = C_1 \cup C_2 \cup \dots \cup C_{\delta_{\max}-1}$  be the defining set of  $\mathcal{BCH}(n, q^2; \delta_{\max})$ . By Lemma 13,  $Z \cap Z^{-q} \neq \emptyset$ , which means that there exist two elements  $x, y \in \{1, \dots, \delta_{\max} - 1\}$  such that  $y = -xq^{2j+1} \pmod{n}$  for some  $j \in \{0, 1, \dots, m-1\}$ , where  $m = \text{ord}_n(q)$ . Since  $\gcd(q, n) = 1$  and  $q^{2m} \equiv 1 \pmod{n}$ , we also have  $y \equiv -xq^{2m-2j-1} \pmod{n}$ , so we can assume without loss of generality that  $j$  lies in the range  $0 \leq j \leq \lfloor (m-1)/2 \rfloor$ . It follows that

$$\begin{aligned} xq^{2j+1} &\leq (\delta_{\max} - 1)q^{2j+1} \\ &= \frac{nq^{2j+1}}{q^{2m} - 1} (q^{m + [m \text{ even}]} - 1 - (q^2 - 2)[m \text{ even}]) - q^{2j+1} \\ &< n \end{aligned}$$

holds for all  $j$  in the range  $0 \leq j \leq \lfloor (m-1)/2 \rfloor$ .

Since  $1 \leq xq^{2j+1} < n$ , the congruence  $y \equiv -xq^{2j+1} \pmod{n}$  implies that  $y = n - xq^{2j+1}$ . Therefore,  $y \geq n - (\delta_{\max} - 1)q^{2\lfloor (m-1)/2 \rfloor + 1}$ , which is equivalent to

$$\begin{aligned} y \geq n - \frac{nq^{2\lfloor (m-1)/2 \rfloor + 1}}{q^{2m} - 1} (q^{m + [m \text{ even}]} - 1 \\ - (q^2 - 2)[m \text{ even}]) + q^{2\lfloor (m-1)/2 \rfloor + 1}. \end{aligned}$$

If  $m$  is odd, this yields

$$\begin{aligned} y \geq n - \frac{nq^m}{q^{2m} - 1} (q^m - 1) + q^m \\ = \frac{n}{q^{2m-1}} (q^m - 1) + q^m \geq \delta_{\max}. \end{aligned}$$

Similarly, if  $m$  is even, then

$$\begin{aligned} y \geq \frac{n}{q^{2m} - 1} (q^{m+1} - q^{m-1} - 1) + q^{m-1} \\ \geq \delta_{\max}. \end{aligned}$$

Both cases contradict the assumption  $0 \leq y < \delta_{\max}$ . Therefore, we can conclude that  $\mathcal{BCH}(n, q; \delta_{\max})$  contains its Hermitian dual code.  $\square$

Arguing as in Theorem 4, we can show that a BCH code must have its designed distance  $\delta = O(q^{2n^{1/2}})$  if it contains its Hermitian dual. As the arguments are very similar we illustrate it for a simpler case as shown in the following lemma.

*Lemma 15:* Let  $C \subseteq \mathbf{F}_{q^2}^n$  be a nonnarrow-sense, nonprimitive BCH code of length  $n \equiv 0 \pmod{q^m + 1}$ , where  $m = \text{ord}_n(q^2)$ . If its design distance  $\delta \geq \delta_{\max} = n/(q^m + 1)$ , then  $C$  cannot contain its Hermitian dual.

*Proof:* The defining set  $Z = C_b \cup \dots \cup C_{b+\delta-2}$  contains  $\{b, \dots, b + \delta - 2\}$ . If  $\delta > \delta_{\max} = n/(q^m + 1)$ , then there exists an element  $s = \alpha \delta_{\max} \in Z$  for some positive integer  $\alpha$ . Then  $-qs(q^2)^{(m-1)/2} \equiv -\alpha n q^m / (q^m + 1) \equiv \alpha n / (q^m + 1) \equiv s \pmod{n}$ . Therefore,  $Z \cap Z^{-q} \neq \emptyset$ ; hence,  $C$  cannot contain its Hermitian dual code.  $\square$

Finally, we conclude this section on Hermitian duals by proving as in the Euclidean case nonnarrow-sense BCH codes that contain their Hermitian duals cannot have too large design distances.

*Theorem 16:* Let  $C \subseteq \mathbf{F}_{q^2}^n$  be a primitive (not necessarily narrow-sense) BCH code of length  $n = q^{2m} - 1$ ,  $m = \text{ord}_n(q)$ , and designed distance  $\delta$ . If  $\delta$  exceeds

$$\delta_{\max} = \begin{cases} q^m - 1, & \text{if } m \text{ is odd} \\ 2(q^{m+1} - q^2 + 1), & \text{if } m \neq 2 \text{ is even} \end{cases}$$

then  $C$  cannot contain its Hermitian dual code.

*Proof:* Suppose that the defining set of  $C$  is given by  $Z = C_b \cup \dots \cup C_{b+\delta-2}$ , where  $C_x = \{xq^{2j} \pmod{n} \mid j \in \mathbf{Z}\}$ , and that  $\delta > \delta_{\max}$ . Seeking a contradiction, we assume that  $C^{\perp_h} \subseteq C$ , which means that

$Z \cap Z^{-q} = \emptyset$ . It follows that  $0 \notin Z$ , for otherwise  $0 \in Z \cap Z^{-q}$ ; therefore,  $b \geq 1$  and  $b + \delta - 2 < n$ .

If  $m$  is odd, then there exists an integer  $\alpha$  such that  $b \leq \alpha \delta_{\max} \leq b + \delta - 2$ . We have  $-q\alpha\delta_{\max}q^{m-1} \equiv \alpha(1 - q^m)q^m \equiv \alpha(q^m - 1) \equiv \alpha\delta_{\max} \pmod{n}$ ; thus,  $\alpha\delta_{\max} \in Z \cap Z^{-q} \neq \emptyset$ .

If  $m > 2$  is even and  $\delta > \delta_{\max} = 2q^{m+1} - 2q^2 + 2$ , then there exists an integer  $\alpha$  such that two multiples of  $\delta' = \delta_{\max}/2$  are contained in the range  $b \leq (\alpha - 1)\delta' < \alpha\delta' \leq b + \delta - 2$ . Since  $b \geq 1$  and  $\alpha\delta' < n$ , it follows that  $2 \leq \alpha \leq q^{m-1}$  (which holds only if  $m > 2$ ).

Clearly  $s = \alpha\delta' \in Z$ . Let  $s' \equiv -qsq^{m-2} \pmod{n}$ , so  $s' \in Z^{-q}$ , then  $1 \leq s' = \alpha(q^{m+1} - q^{m-1} - 1) \leq s$  for  $m > 2$ .

Suppose that  $b \leq s'$ . Then  $s' \in Z$ , which implies  $Z \cap Z^{-q} \neq \emptyset$ .

Suppose that  $s' < b$ . Since  $b \leq (\alpha - 1)\delta'$ , we obtain the inequality  $s' < (\alpha - 1)\delta'$ ; solving for  $\alpha$  shows that  $\alpha \geq q^2$ ; thus,  $q^2 \leq \alpha \leq q^{m-1}$ . Let  $t' = (\alpha - 1)(q^{m+1} - 1) + q^{(m-1)/2} - 1$ ; it is easy to check that  $t'$  is in the range  $(\alpha - 1)\delta' \leq t' \leq \alpha\delta'$  when  $\alpha \geq q^2$ ; thus,  $t' \in Z$ . Further, let  $t = s - (\alpha - q^2 + 1)$ ; since  $t \geq s - \delta'$ , we have  $t \in Z$  as well. Since  $-qtq^{m-2} \equiv t' \pmod{n}$ , we can conclude that  $t' \in Z \cap Z^{-q} \neq \emptyset$ . Hence, by Lemma 13 we conclude that  $C$  cannot contain its Hermitian dual if its design distance exceeds  $\delta_{\max}$ .  $\square$

## V. FAMILIES OF QUANTUM BCH CODES

In this section, we will study the construction of (nonbinary) quantum BCH codes. Calderbank, Shor, Rains, and Sloane outlined the construction of binary quantum BCH codes in [5]. Grassl, Beth and Pellizari developed the theory further by formulating a nice condition for determining which BCH codes can be used for constructing quantum codes [8], [9]. The dimension and the purity of the quantum codes constructed were determined by numerical computations. Steane simplified it further for the special case of binary narrow-sense primitive BCH codes [18] and gave a very simple criterion based on the design distance alone. Very little was done with respect to the nonprimitive and nonbinary quantum BCH codes.

In this section, we show how the developed results from the previous sections help us to generalize the previous work on quantum codes and give very simple conditions based on design distance alone. Further, we give precisely the dimension and tighten results on the purity of the quantum codes. But, first we review the methods of constructing quantum codes from classical codes.

*Lemma 17 (Quantum Code Constructions):*

- If there exists classical linear codes  $C_1 \subseteq C_2 \subseteq \mathbf{F}_q^n$ , then there exists an  $[[n, k_2 - k_1, d]]_q$  quantum code where  $d = \min \text{wt}\{(C_2 \setminus C_1) \cup (C_1^\perp \setminus C_2^\perp)\}$ .
- If there exists a classical linear  $[n, k, d]_q$  code  $C$  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 stabilizer code is pure and has minimum distance  $d$ .
- If there exists a classical linear  $[n, k, d]_{q^2}$  code  $D$  such that  $D^{\perp h} \subseteq D$ , then there exists an  $[[n, 2k - n, \geq d]]_q$  stabilizer code that is pure to  $d$ . If the minimum distance  $d^{\perp h}$  of  $D^{\perp h}$  exceeds  $d$ , then the stabilizer code is pure and has minimum distance  $d$ .

*Proof:* See, for instance, [13] for the proofs. Part a) is commonly referred to as the CSS construction [13, Lemma 20] and b) is a special case of a); part c) is the Hermitian code construction [13, Corollary 19].  $\square$

*Theorem 18:* Let  $m = \text{ord}_n(q) \geq 2$ , where  $q$  is a power of a prime and  $\delta_1, \delta_2$  are integers such that  $2 \leq \delta_1 < \delta_2 \leq \delta_{\max}$  where

$$\delta_{\max} = \frac{n}{q^m - 1}(q^{\lceil m/2 \rceil} - 1 - (q - 2)[m \text{ odd}]),$$

then there exists a quantum code with parameters

$$[[n, m(\delta_2 - \delta_1 - \lfloor (\delta_2 - 1)/q \rfloor + \lfloor (\delta_1 - 1)/q \rfloor), \geq \delta_1]]_q$$

pure to  $\delta_2$ .

*Proof:* By Theorem 10, there exist BCH codes  $\mathcal{BCH}(n, q; \delta_i)$  with the parameters  $[n, n - m(\delta_i - 1) + m\lfloor (\delta_i - 1)/q \rfloor, \geq \delta_i]_q$  for  $i \in \{1, 2\}$ . Further,  $\mathcal{BCH}(n, q; \delta_2) \subset \mathcal{BCH}(n, q; \delta_1)$ . Hence, by the CSS construction there exists a quantum code with the parameters

$$[[n, m(\delta_2 - \delta_1 - \lfloor (\delta_2 - 1)/q \rfloor + \lfloor (\delta_1 - 1)/q \rfloor), \geq \delta_1]]_q.$$

The purity follows due to the fact that  $\delta_2 > \delta_1$  and Lemma 12 by which the dual distance of either BCH code is  $\geq \delta_{\max} + 1 > \delta_2$ .  $\square$

When the BCH codes contain their duals, then we can derive the following codes. Note that these cannot be obtained as a consequence of Theorem 18.

*Theorem 19:* Let  $m = \text{ord}_n(q)$  where  $q$  is a power of a prime and  $2 \leq \delta \leq \delta_{\max}$ , with

$$\delta_{\max} = \frac{n}{q^m - 1}(q^{\lceil m/2 \rceil} - 1 - (q - 2)[m \text{ odd}])$$

then there exists a quantum code with parameters

$$[[n, n - 2m\lceil (\delta - 1)(1 - 1/q) \rceil, \geq \delta]]_q$$

pure to  $\delta_{\max} + 1$

*Proof:* Theorems 3 and 10 imply that there exists a classical BCH code with parameters  $[n, n - m\lceil (\delta - 1)(1 - 1/q) \rceil, \geq \delta]_q$  which contains its dual code. By Lemma 17 b) an  $[n, k, d]_q$  code that contains its dual code implies the existence of the quantum code with parameters  $[[n, 2k - n, \geq d]]_q$ . The purity follows from Lemma 12 by which the dual distance  $\geq \delta_{\max} + 1 > \delta$ .  $\square$

Before we can construct quantum codes via the Hermitian construction, we will need the following lemma.

*Lemma 20:* Suppose that  $C$  is a primitive, narrow-sense BCH code of length  $n = q^{2m} - 1$  over  $\mathbf{F}_{q^2}$  with designed distance  $2 \leq \delta \leq \delta_{\max} = q^{m + \lfloor m \text{ even} \rfloor} - 1 - (q^2 - 2)[m \text{ even}]$ , then the dual distance  $d^\perp \geq \delta_{\max} + 1$ .

*Proof:* The proof is analogous to the one of Lemma 12; just keep in mind that the defining set  $Z_\delta$  is invariant under multiplication by  $q^2$  modulo  $n$ .  $\square$

*Theorem 21:* Let  $m = \text{ord}_n(q^2) \geq 2$  where  $q$  is a power of a prime and  $2 \leq \delta \leq \delta_{\max} = \lfloor n(q^m - 1)/(q^{2m} - 1) \rfloor$ , then there exists a quantum code with parameters

$$[[n, n - 2m\lceil (\delta - 1)(1 - 1/q^2) \rceil, \geq \delta]]_q$$

that is pure up to  $\delta_{\max} + 1$ .

*Proof:* It follows from Theorems 10 and 14 that there exists a primitive, narrow-sense  $[n, n - 1 - m\lceil (\delta - 1)(1 - 1/q^2) \rceil, \geq \delta]_{q^2}$  BCH code that contains its Hermitian dual code. By Lemma 17c) a classical  $[n, k, d]_{q^2}$  code that contains its Hermitian dual code implies the existence of an  $[[n, 2k - n, \geq d]]_q$  quantum code. By Lemma 20 the quantum code is pure to  $\delta_{\max} + 1$ .  $\square$

In the above theorem, quantum codes can also be constructed when the design distance exceeds the given value of  $\delta_{\max}$ , however we do not have exact knowledge of the dimension in all those cases, hence we have not included them to keep the theorem precise.

These are not the only possible families of quantum codes that can be derived from BCH codes. As pointed out in [8], we can expand BCH codes over  $\mathbf{F}_{q^l}$  to get codes over  $\mathbf{F}_q$ . Once again the dimension and duality results of BCH codes makes it very easy to specify such codes. We will just give one example in the Euclidean case. Similar results can be derived for the Hermitian case.

**Theorem 22:** Let  $m = \text{ord}_n(q^l)$  where  $q$  is a power of a prime and  $2 \leq \delta \leq \delta_{\max}$ , with

$$\delta_{\max} = \frac{n}{q^{lm} - 1} (q^{l\lceil m/2 \rceil} - 1 - (q^l - 2)[m \text{ odd}])$$

then there exists a quantum code with parameters

$$[[ln, ln - 2lm\lceil(\delta - 1)(1 - 1/q^l)\rceil, \geq \delta]]_q$$

that is pure up to  $\delta$ .

*Proof:* By Theorem 19 there exists a quantum BCH code with parameters  $[[n, n - 2m\lceil(\delta - 1)(1 - 1/q^l)\rceil, \geq \delta]]_{q^l}$ . An  $[[n, k, d]]_{q^l}$  quantum code implies the existence of the quantum code with parameters  $[[ln, lk, \geq d]]_q$  by [13, Lemma 76] and the code follows.  $\square$

## VI. CONCLUSION

In this correspondence, we have identified the classes of BCH codes that contain their Euclidean (Hermitian) duals by a careful analysis of the cyclotomic cosets. In the process we have been able to shed more light on the structure of dual containing BCH codes. We were able to derive a formula for the dimension of narrow-sense BCH codes when the designed distance is small. These results allowed us to identify easily which classical BCH codes can be used for construct quantum codes. Further, the parameters of these quantum codes are easily specified in terms of the design distance.

## ACKNOWLEDGMENT

The authors would like to thank the referees for their comments.

## REFERENCES

- [1] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli, "Primitive quantum BCH codes over finite fields," in *Proc. IEEE Int. Symp. Inf. Theory*, Seattle, WA, 2006, pp. 1105–1108.
- [2] E. R. Berlekamp, *Algebraic Coding Theory*. New York: McGraw-Hill, 1968.
- [3] R. C. Bose and D. K. Ray-Chaudhuri, "Further results on error correcting binary group codes," *Inf. Contr.*, vol. 3, pp. 279–290, 1960.
- [4] —, "On a class of error correcting binary group codes," *Inf. Contr.*, vol. 3, pp. 68–79, 1960.
- [5] 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*, vol. 44, pp. 1369–1387, 1998.
- [6] P. Charpin, "Open problems on cyclic codes," in *Handbook of Coding Theory*. Amsterdam, The Netherlands: North-Holland, 1998, vol. I, II, pp. 963–1063.
- [7] D. Gorenstein and N. Zierler, "A class of error-correcting codes in  $p^m$  symbols," *J. Soc. Ind. Appl. Math.*, vol. 9, pp. 207–214, 1961.
- [8] M. Grassl and T. Beth, "Quantum BCH codes," in *Proc. X. Int. Symp. Theoret. Elec. Eng.*, Magdeburg, 1999, pp. 207–212.
- [9] M. Grassl, T. Beth, and T. Pellizzari, "Codes for the quantum erasure channel," *Phys. Rev. Lett. A*, vol. 56, no. 1, pp. 33–38, 1997.
- [10] M. Grassl and T. Beth, "Cyclic quantum error-correcting codes and quantum shift registers," *Proc. Royal Soc. London Series A*, vol. 456, no. 2003, pp. 2689–2706, 2000.
- [11] A. Hocquenghem, "Codes correcteurs d'erreurs," *Chiffres*, vol. 2, pp. 147–156, 1959.
- [12] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge, U.K.: Cambridge University Press, 2003.
- [13] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, "Non-binary stabilizer codes over finite fields," *IEEE Trans. Inf. Theory*, vol. 52, pp. 4892–4914, 2006.
- [14] S. Konyagin and I. Shparlinski, *Character Sums with Exponential Functions and their Applications*. Cambridge, U.K.: Cambridge University Press, 1999.
- [15] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.
- [16] W. W. Peterson and W. J. Weldon Jr., *Error-Correcting Codes*. Cambridge, MA: MIT Press, 1972.
- [17] I. E. Shparlinski, "On the dimension of BCH codes," (in Russian) *Problemy Peredachi Informatsii*, vol. 25, no. 1, pp. 77–80, 1988.
- [18] A. Steane, "Enlargement of Calderbank-Shor-Steane codes," *IEEE Trans. Inform. Theory*, vol. 45, pp. 2492–2495, 1999.
- [19] A. M. Steane, "Simple quantum error correcting codes," *Phys. Rev. Lett.*, vol. 77, pp. 793–797, 1996.
- [20] H. Stichtenoth and C. Voß, "Generalized Hamming weights of trace codes," *IEEE Trans. Inf. Theory*, vol. 40, pp. 554–558, 1994.
- [21] D.-W. Yue and G.-Z. Feng, "Minimum cyclotomic coset representatives and their applications to BCH codes and Goppa codes," *IEEE Trans. Inf. Theory*, vol. 46, pp. 2625–2628, 2000.
- [22] D.-W. Yue and Z.-M. Hu, "On the dimension and minimum distance of BCH codes over GF(q)," (in Chinese) *J. Electron.*, vol. 18, pp. 263–269, 1996.

## Generalized Bose–Lin Codes, a Class of Codes Detecting Asymmetric Errors

Irina Naydenova and Torleiv Kløve, *Fellow, IEEE*

**Abstract**—Bose and Lin introduced a class of systematic codes for detection of binary asymmetric errors. In this note, we describe a generalization to  $q$ -ary asymmetric error detecting codes. For these codes, the possible undetectable errors are characterized and the undetectable errors of minimum weight are determined.

**Index Terms**—Asymmetric channel, Bose–Lin codes, error detection.

## I. INTRODUCTION

An asymmetric channel is a channel where a transmitted symbol (from a finite ordered alphabet) never is transformed into a larger symbol during transmission. For the binary case (where the alphabet is  $\{0, 1\}$ ), 0 is never transformed but 1 may be transformed to 0.

Bose and Lin [3] introduced a class of systematic binary codes for detection of asymmetric errors (codes occurring over an asymmetric channel). The probability of undetected error for these codes was determined in [6]. The class of codes is conjectured to contain the best

Manuscript received December 6, 2005; revised October 5, 2006. The material in this correspondence was presented in part at the 4th International Workshop on Optimal Codes and Related Topics, Pamporovo, Bulgaria, June 2005.

The authors are with the Department of Informatics, University of Bergen, N-5020 Bergen, Norway (e-mail: Irina.Gancheva@ii.uib.no; Torleiv.Klove@ii.uib.no).

Communicated by M. Sudan, Associate Editor for Coding Theory. Digital Object Identifier 10.1109/TIT.2006.890776