Constructions of new families of nonbinary quantum codes

Giuliano G. La Guardia*
Department of Mathematics and Statistics, State University of Ponta Grossa–UEPG, 84030-900 Ponta Grossa, PR, Brazil
(Received 16 July 2009; published 28 October 2009)

Three code constructions generating new families of good nonbinary quantum codes are presented in this paper. The first two ones are derived from Hermitian self-orthogonal non-narrow-sense Bose-Chaudhuri-Hocquenghem (BCH) codes. The third one is derived from q-ary ($q\neq 2$ is a prime power) Steane's enlargement of Calderbank-Shor-Steane codes applied to Euclidean self-orthogonal non-narrow-sense BCH codes. The quantum nonbinary BCH codes presented here have parameters better than the ones available in the literature.

DOI: 10.1103/PhysRevA.80.042331 PACS number(s): 03.67.Pp

I. INTRODUCTION

The theory of quantum-error-correcting codes [1–7] has been exhaustively investigated in the literature. There are many works that deal with quantum code constructions [2–6,8–39]. However, most of them deal with constructions of binary quantum codes, while the nonbinary case has received less attention.

With respect to the construction of quantum Bose-Chaudhuri-Hocquenghem (BCH) codes, there are few works available in the literature. More specifically, in [3,19,20,33], the authors constructed binary quantum BCH codes and in [9,10,30,39], nonbinary quantum BCH codes are constructed. This fact is due to the difficulty of computing the exact dimension of this class of codes. In other words, the dimension of nonbinary (binary) BCH codes is not known.

Aly *et al.* [9,10] have constructed families of quantum BCH codes derived from Euclidean as well as Hermitian self-orthogonal codes. The procedure is based on the computation of the exact dimension of the classical narrow-sense BCH codes of length n with minimum distance $O(n^{1/2})$. Additionally, they also have established useful conditions for dual containing BCH codes. Following this approach, Ma *et al.* [30] and Xu *et al.* [39] also have constructed families of quantum BCH codes by using self-orthogonal codes.

Inspired by these latter works, we propose three constructions generating new families of good nonbinary quantum non-narrow-sense BCH codes. To construct these new families, we compute the exact dimension of the corresponding classical non-narrow-sense BCH codes used in this procedure, which is a difficult task. In other words, we derive the exact dimension of certain families of non-narrow-sense BCH codes by showing useful properties of their cyclotomic cosets, providing the exact dimension of the corresponding quantum codes. In fact, cyclotomic cosets are the key to the proposed constructions.

The first construction generates new families of quantum codes with parameters

(i) $[\![n,n-4(c-2)-2,d\geq c]\!]_q$,
where $n=q^4-1$ and $3\leq c\leq q^2$.

The second one generates new families of quantum codes with parameters

(i) $[\![n,n-2mc-2,d\geq c+2]\!]_q$
for all $1\leq c\leq q^2-2$,
(ii) $[\![n,n-2m(q^2-1)-2,d\geq q^2+2]\!]_q$,
(iii) $[\![n,n-2m(c-1)-2,d\geq c+2]\!]_q$
for all $q^2+1\leq c\leq 2q^2-2$, and
(iv) $[\![n,n-4m(q^2-1)-2,d\geq 2q^2+2]\!]_q$,
where $n=q^{2m}-1$, $q\geq 4$ is a prime power,
and $m=\mathrm{ord}_n(q^2)\geq 3$.

The third construction generates new families of quantum codes with parameters

(i) $[\![n,n-m(2c-1)-2,d\geq c+2]\!]_q$, for all $1\leq c\leq q-2$;
(ii) $[\![n,n-m(2q-3)-2,d\geq q+1]\!]_q$,
(iii) $[\![n,n-m(2q-1)-1,d\geq q+3]\!]_q$,
(iv) $[\![n,n-m(2c-4)-2,d\geq c+2]\!]_q$,
(v) $[\![n,n-m(4q-8)-2,d\geq 2q]\!]_q$
(vi) $[\![n,n-m(4q-5)-2,d\geq 2q+2]\!]_q$ where $q+1<c<2q-2$;
where $n=q^m-1$, $q\geq 4$, and $m=\mathrm{ord}_n(q)\geq 3$.

The proposed families have parameters better than the ones available in [9,10] and also better than the ones derived from q-ary Steane's construction (Corollary 4 in [25]) when applied to narrow-sense BCH codes. More specifically, fixing the length and the minimum distance, the new codes have dimension greater than the dimension of the quantum codes mentioned above.

This paper is organized as follows. In Sec. II, basic concepts on cyclic codes are revised. In Sec. III, the constructions being proposed are presented: Sec. III A shows how to construct new quantum codes of length q^4-1 over F_{q^2} derived from Hermitian construction; Sec. III B shows how to construct new families of quantum codes of arbitrary length by means of the Hermitian construction; and in Sec. III C, new families of quantum codes derived from q-ary Steane's construction applied to suitable non-narrow-sense BCH codes are constructed. In Sec. IV, the parameters of the new quantum codes are compared with the ones shown in [9,10] and also compared with the ones derived from q-ary Steane's construction when applied to narrow-sense BCH codes. Finally, in Sec. V, the final remarks are draw.

II. BACKGROUND

This section presents a review of cyclic codes for the purpose of this paper. For more details, we refer the reader to [6,10,39–41].

*gguardia@uepg.br

Notation. We consider that $q \neq 2$ is a prime power, F_q is a finite field with q elements, n denotes the code length [we always assume that $\gcd(n,q)=1$ in the Euclidean case and that $\gcd(n,q^2)=1$ in the Hermitian case], $m=\mathrm{ord}_n(q)$ is the multiplicative order of q mod n, the equivalence $\equiv$ is considered mod n, Z_i denotes the defining set of a code C_i (in particular, Z is the defining set of a code C), $\mathbb{C}_{[a]}$ denotes the cyclotomic coset containing a, where a is not necessarily the smallest number in the coset $\mathbb{C}_{[a]}$, $C^{\perp}$ denotes the Euclidean dual of C, and $C^{\perp_H}$ denotes the Hermitian dual of C.

The following results can be found in [41]. The minimal polynomial over F_q of $\beta \in F_{q^m}$ is the monic polynomial of smallest degree, $M(x)$, with coefficients in F_q such that $M(\beta)=0$. Irreducible polynomials can be obtained in the following way: $x^{q^m}-x$=product of all monic irreducible polynomials over F_q, whose degree divides m.

Cyclotomic cosets are the key to the quantum code constructions being proposed:

Definition II.1. The q-ary cyclotomic coset mod n containing an element s is defined by $\mathbb{C}_s=\{s, sq, sq^2, sq^3, \ldots, sq^{m_s-1}\}$, where m_s is the smallest positive integer such that $sq^{m_s} \equiv s \bmod n$.

If C is a cyclic code of length n over F_q, there is only one monic polynomial $g(x)$ [$g(x)$ is a factor of x^n-1] with minimal degree in C; $g(x)$ is the generator polynomial of C. The dimension of C equals $n-r$, where $r=\partial(g(x))$ is the degree of $g(x)$.

The BCH bound theorem. Let C be a cyclic code with generator polynomial $g(x)$ such that, for some integers $b \geq 0$, $\delta \geq 1$, and $\alpha \in F_{q^m}$, we have $g(\alpha^b)=g(\alpha^{b+1})=\cdots=g(\alpha^{b+\delta-2})=0$, that is, the code has a sequence of $\delta-1$ consecutive powers of α as zeros. Then the minimum distance of C is, at least, δ.

A cyclic code of length n over F_q is a BCH code of designed distance δ if, for some integer $b \geq 0$,

$$g(x) = \text{l.c.m.}\{M^{(b)}(x), M^{(b+1)}(x), \ldots, M^{(b+\delta-2)}(x)\},$$

that is, $g(x)$ is the monic polynomial of smallest degree over F_q having $\alpha^b, \alpha^{b+1}, \ldots, \alpha^{b+\delta-2}$ as zeros. If $n=q^m-1$ then the BCH code is called primitive and if $b=1$ it is called narrow sense. From the BCH bound theorem, the minimum distance of BCH codes is greater than or equal to their designed distance δ.

BCH codes [42–44] are a well-studied class of good classical codes. Recently, works concerning the dimension and minimum distance of BCH codes as well as sufficient (in some cases, necessary and sufficient conditions) condition for (Euclidean and Hermitian) dual containing BCH codes were presented [9,10,30,39,45,46].

The following lemma gives necessary and sufficient conditions under which a cyclic code contains its Euclidean dual:

Lemma II.1. (Lemma 1 in [10]) Assume that $\gcd(q,n)=1$. A cyclic code of length n over F_q with defining set Z contains its Euclidean dual code if and only if $Z \cap Z^{-1}=\emptyset$, where $Z^{-1}=\{-z \bmod n \,|\, z \in Z\}$.

If C is a linear code of length n over F_{q^2}, its Hermitian dual code is defined by

$$C^{\perp_H}=\{y \in F_{q^2}^n | y^q \cdot x = 0 \text{ for all } x \in C\},$$

where $y^q=(y_1^q, \ldots, y_n^q)$ denotes the conjugate of the vector $y=(y_1, \ldots, y_n)$.

Lemma II.2 gives necessary and sufficient conditions under which a cyclic code contains its Hermitian dual:

Lemma II.2. (Lemma 13 in [10]) Assume that $\gcd(q,n)=1$. A cyclic code of length n over F_{q^2} with defining set Z contains its Hermitian dual code if and only if $Z \cap Z^{-q}=\emptyset$, where $Z^{-q}=\{-qz \bmod n \,|\, z \in Z\}$.

III. CODE CONSTRUCTIONS

In this section we present the quantum code constructions being proposed. We deal with non-narrow-sense BCH codes containing their Euclidean as well as their Hermitian duals. For the purpose of this paper let us recall the well-known Hermitian construction:

Lemma III.1. (Hermitian construction) (Lemma 17c in [10]) If there exists a classical linear $[n,k,d]_{q^2}$ code D such that $D^{\perp_H} \subset D$, 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.

A. Construction I: Codes of length q^4-1 over F_{q^2}

In this section we apply the Hermitian construction in order to construct new families of quantum codes. The main result is Theorem III.1. It asserts the existence of new families of quantum codes with parameters $[\![n, n-4(q^2-2)-2, d \geq q^2]\!]_q$, consequently, the existence of new quantum codes with parameters $[\![n, n-4(c-2)-2, d \geq c]\!]_q$, where $3 \leq c \leq q^2-1$. We begin by showing a useful lemma:

Lemma III.2. Let $n=q^4-1$, where $q \geq 3$ is a prime power, and consider the first q^2-1 q^2-ary cyclotomic cosets mod n given by

$$\mathbb{C}_{[q^2+1]},$$

$$\mathbb{C}_{[q^2+2]}=\{q^2+2, \quad 1+2q^2\},$$

$$\vdots$$

$$\mathbb{C}_{[2q^2-1]}=\{2q^2-1, \quad 1+(q^2-1)q^2\}.$$

Then the following results hold:

(a) $\mathbb{C}_{[q^2+1]}$ contains only one element;

(b) each one of the other cosets contains two elements; and

(c) each one of these cyclotomic cosets are distinct.

Proof: We begin by observing that the inequality $n>1+(q^2-1)q^2$ is true.

(a) Since $(q^2+1)q^2 \equiv q^2+1$ holds, the result follows.

(b) We show that each one of the cosets $\mathbb{C}_{[q^2+2]}, \ldots, \mathbb{C}_{[2q^2-1]}$ has exactly two elements. In fact, if $q^2+j \equiv 1+jq^2$, where $j=2, \ldots, q^2-1$ since $1+jq^2<n$, one obtains $q^2+j=1+jq^2$ and so $j-1=(j-1)q^2$, which is a contradiction.

(c) It is clear that coset $\mathbb{C}_{[q^2+1]}$ is distinct of the other cosets since it has only one element. Assume that $\mathbb{C}_{[q^2+i]} = \mathbb{C}_{[q^2+j]}$, where $2 \le i,j \le q^2-1$, $i \ne j$. Then either $q^2+i \equiv q^2+j$ or $q^2+i \equiv (q^2+j)q^2$ is true, where $2 \le i,j \le q^2-1$. Since $2q^2-1 < q^4-1$ and $1+(q^2-1)q^2 < q^4-1$ hold, it implies that $q^2+i=q^2+j$ or $q^2+i=1+jq^2$ hold. The first case implies that $i=j$, a contradiction, and in the second case one has $q^2 | i-1$, which is a contradiction. Therefore, each one of the cyclotomic cosets is distinct. □

From now on, we show Theorem III.1, the main result of this section:

Theorem III.1. Let $n=q^4-1$, where $q \ge 3$ is a prime power. Then there exist quantum codes with parameters $[\![n, n-4(q^2-2)-2, d \ge q^2]\!]_q$.

Proof: Let C be the cyclic code generated by the product of the minimal polynomials

$$M^{(q^2+1)}(x)M^{(q^2+2)}(x) \ldots M^{(q^2+j)}(x),$$

$1 \le j \le q^2-1$. We first show that C is Hermitian self-orthogonal. Seeking a contradiction, we assume that $Z \cap Z^{-q} \ne \emptyset$. Then there exist i and j, where $1 \le i,j \le q^2-1$, such that $\mathbb{C}_{[q^2+j]} = \mathbb{C}_{[-q(q^2+i)]}$ and so

$$q^2 + j \equiv -q(q^2+i)q^{2k},$$

where $0 \le k \le 1$.

If $k=0$ then $q^3+qi+q^2+j < q^4-1$, and so $q^2+j=-q^3-qi$, which is a contradiction.

Assume that $k=1$. Since $\gcd(q^2,n)=1$ and $q^4 \equiv 1 \bmod n$ hold, it follows that

$$q^2 + j \equiv -q^3(q^2+i) \Rightarrow q^5 + q^3 i \equiv -(q^2+j) \Rightarrow q + q^3 i \equiv -(q^2+j),$$

where $1 \le i,j \le q^2-1$.

If $i < q$ then $iq^3+q+q^2+j < q^4-1$, and so $q+q^3i=-(q^2+j)$, which is a contradiction.

If $i \ge q$, from the division algorithm one has $i=lq+r$, where $0 \le r \le q-1$. We also have $1 \le l \le q-1$, so

$$q + q^3 i = q + q^3(lq+r) \equiv q + l + q^3 r.$$

Computing $q+l+q^3r+q^2+j$ one obtains

$$q + l + q^3 r + q^2 + j < q^3(q-1) + 2q + 2q^2 = q^4 - q^3 + 2q + 2q^2.$$

Since $q^3 > 2q^2+2q+1$, it follows that $q+l+q^3r+q^2+j < q^4-1$, and so $q+l+q^3r=-q^2-j$, which is a contradiction. Therefore C is Hermitian self-orthogonal.

Since the defining set of C contains the sequence $q^2+1, q^2+2, \ldots, 2q^2-1$, it follows from the BCH bound theorem that its minimum distance is greater than or equal to q^2.

Next we compute the dimension of the corresponding quantum code. From Lemma III.2, the defining set of C has $2(q^2-2)+1$ elements. We know that the degree of the generator polynomial of a cyclic code equals the cardinality of its defining set [see Eq. (1)]. Thus the degree of the generator polynomial of C equals $2(q^2-2)+1$; hence C has dimension $n-2(q^2-2)-1$ and, consequently, their parameters are given by $[n, n-2(q^2-2)-1, d \ge q^2]_{q^2}$. From Lemma III.1, there exists an $[\![n, 2k-n, \ge d]\!]_q$ stabilizer code derived from a classical linear $[n,k,d]_{q^2}$ code. Therefore, there exists an $[\![n, n-4(q^2-2)-2, d \ge q^2]\!]_q$ stabilizer code, as required. □

Corollary III.1 generates new families of good quantum codes:

Corollary III.1. Let $n=q^4-1$, where $q \ge 3$ is a prime power. Then there exist quantum codes with parameters $[\![n, n-4(c-2)-2, d \ge c]\!]_q$, where $3 \le c \le q^2-1$.

Proof: Let C be the cyclic code generated by the product of the minimal polynomials

$$M^{(q^2+1)}(x)M^{(q^2+2)}(x) \ldots M^{(q^2+c-1)}(x).$$

Proceeding similarly as in the proof of Theorem III.1, the result follows. □

In order to show how the proposed construction works we give an example:

Example III.1. Let $m=2$ and $q=3$; then $n=80$. Consider C be the cyclic code generated by the product of the minimal polynomials

$$M^{(10)}(x)M^{(11)}(x).$$

From the BCH bound theorem, the minimum distance of C is greater than or equal to 3. Its dimension equals $80-3=77$; so it has parameters $[80,77,d \ge 3]_9$. We know that C is Hermitian self-orthogonal (see the proof of Theorem III.1). Applying the Hermitian construction one has an $[\![80,74,d \ge 3]\!]_3$ quantum code.

B. Construction II: Hermitian non-narrow-sense BCH codes

In this section we present the second quantum code construction being proposed, which is also based on non-narrow-sense BCH codes. As we shall see, this construction generates new families of good stabilizer codes derived from Hermitian self-orthogonal codes. The first result of this section establishes the q^2-ary cosets containing only one element:

Lemma III.3. Let $n=q^{2m}-1$, where $q \ne 2$ and $m = \mathrm{ord}_n(q^2) \ge 3$. If $s=\sum_{i=0}^{m-1}(q^2)^i$ then the q^2-ary coset $\mathbb{C}_{[s]}$ has only one element.

Proof: We know that $\gcd(q^2,n)=1$ and $q^{2m} \equiv 1 \bmod n$. Applying these facts to the expression $[\sum_{i=0}^{m-1}(q^2)^i]q^{2j}$, where $0 \le j \le m-1$ and $m=\mathrm{ord}_n(q^2)$, one has

$$\begin{aligned} sq^{2j} &= \left(\sum_{i=0}^{m-1}(q^2)^i\right)q^{2j} = q^{2j}(q^2)^{(m-1)} + q^{2j}(q^2)^{(m-2)} + \cdots \\ &+ q^{2j}q^2 + q^{2j} = q^{2j}q^{2m}q^{-2} + q^{2j}q^{2m}q^{-4} + \cdots \\ &+ q^{2j}q^{2m}q^{(-2j+2)} + q^{2j}q^{2m}q^{-2j} + q^{2j}q^{2m}q^{(-2j-2)} \\ &+ q^{2j}q^{2m}q^{(-2j-4)} + \cdots + q^{2j}q^2 + q^{2j} \equiv q^{2j}q^{-2} + q^{2j}q^{-4} \\ &+ \cdots + q^{2j}q^{(-2j+2)} + q^{2j}q^{-2j} + q^{(2m-2)} + q^{(2m-4)} + \cdots \\ &+ q^{2j}q^2 + q^{2j} = (q^2)^{(m-1)} + (q^2)^{(m-2)} + \cdots + (q^2)^{(j+1)} \\ &+ (q^2)^j + (q^2)^{(j-1)} + (q^2)^{(j-2)} + \cdots + q^2 + 1 = \sum_{i=0}^{m-1}(q^2)^i \\ &= s, \end{aligned}$$

as desired. □

Lemma III.4 asserts that each one of the q^2-ary cosets of the forms $\mathbb{C}_{[s+i]}$ and $\mathbb{C}_{[s-j]}$, where $1 \le i,j \le q^2-1$, is distinct among them:

Lemma III.4. Suppose that $n=q^{2m}-1$, where $q \neq 2$ and $m=\mathrm{ord}_n(q^2) \ge 3$. Let $s=\sum_{i=0}^{m-1}(q^2)^i$. Then the following hold:

(a) each one of the q^2-ary cosets $\mathbb{C}_{[s+i]}$ is distinct, where $1 \le i \le q^2-1$;

(b) each one of the q^2-ary cosets $\mathbb{C}_{[s-j]}$ is distinct, where $1 \le j \le q^2-1$; and

(c) the cosets of the form $\mathbb{C}_{[s+i]}$ is distinct of each one of the cosets $\mathbb{C}_{[s-j]}$, where $1 \le i,j \le q^2-1$.

Proof:

(a) Assume there exist i,j, where $i \neq j$ and $1 \le i,j \le q^2-1$, such that $\mathbb{C}_{[s+i]}=\mathbb{C}_{[s+j]}$. Then there exists $0 \le t \le m-1$ such that $s+i \equiv (s+j)q^{2t}$. From Lemma III.3 one has $sq^{2t} \equiv s$. Moreover, since $\gcd(q^2,n)=1$ and $q^{2m} \equiv 1 \bmod n$ are true, it follows that

$$s+i \equiv (s+j)q^{2t} \equiv s+jq^{2t} \Rightarrow i \equiv jq^{2t}.$$

Since $1 \le i,j \le q^2-1$, it follows that $jq^{2t} < q^{2m}-1$, and so

$$i \equiv jq^{2t} \Rightarrow i = jq^{2t}.$$

If $t=0$ then $i=j$ and if $t \ge 1$ the equality $i=jq^{2t}$ does not hold, which is a contradiction. Thus, for $i \neq j$, it follows that $\mathbb{C}_{[s+j]} \neq \mathbb{C}_{[s+i]}$.

(b) Analogous to the previous item.

(c) Assume that $\mathbb{C}_{[s+i]}=\mathbb{C}_{[s-j]}$, where $1 \le i,j \le q^2-1$. Then there exists $0 \le t \le m-1$, such that $s+i \equiv (s-j)q^{2t}$. Similarly, one has

$$s+i \equiv (s-j)q^{2t} \equiv s-jq^{2t} \Rightarrow i \equiv -jq^{2t}.$$

Since $m \ge 3$, we know that

$$i+jq^{2t} \le (q^2-1)(q^{2m-2}+1) < q^{2m}-1,$$

and so $i=-jq^{2t}$, which is a contradiction.

Therefore, for each $i \neq j$, where $1 \le i,j \le q^2-1$, it implies that $\mathbb{C}_{[s+i]} \neq \mathbb{C}_{[s-j]}$, as desired. □

In the following, we show that each one of the cosets $\mathbb{C}_{[s+i]}$ and $\mathbb{C}_{[s-j]}$, where $1 \le i,j \le q^2-1$, has cardinality m:

Lemma III.5. Assume $n=q^{2m}-1$, where $q \ge 4$ and $m=\mathrm{ord}_n(q^2) \ge 3$. Let $s=\sum_{i=0}^{m-1}(q^2)^i$. Then the following hold:

(a) the cosets of the form $\mathbb{C}_{[s+i]}$, where $1 \le i \le q^2-1$, contain m elements;

(b) the cosets of the form $\mathbb{C}_{[s-j]}$ contain m elements, where $1 \le j \le q^2-1$.

Proof:

(a) The elements of the coset $\mathbb{C}_{[s+i]}$ are of the form $(s+i)q^{2t}$, where $0 \le t \le m-1$ and for all $1 \le i \le q^2-1$. Since $\gcd(q^2,n)=1$, $q^{2m} \equiv 1 \bmod n$, and $sq^{2t} \equiv s$, it follows that $(s+i)q^{2t} \equiv s+iq^{2t}$. Considering $0 \le t \le m-2$ one obtains

$$s+iq^{2t} < \frac{q^{2m}-1}{q^2-1} + q^{2m-2} \le \frac{q^{2m}-1}{15} + \frac{q^{2m}-1}{15} < q^{2m}-1.$$

Therefore, the first $m-1$ elements belonging to $\mathbb{C}_{[s+i]}$ are distinct for all $0 \le t \le m-2$ and $1 \le i \le q^2-1$, so the coset $\mathbb{C}_{[s+i]}$ contains m elements because $m-1 > m/2$.

(b) Analogous to the previous item. □

Lemma III.6 constructs families of Hermitian self-orthogonal classical non-narrow-sense BCH codes:

Lemma III.6. Suppose that $n=q^{2m}-1$, where $q \ge 4$ is a prime power, $\gcd(q^2,n)=1$ and $m=\mathrm{ord}_n(q^2) \ge 3$. Let $s=\sum_{i=0}^{m-1}(q^2)^i$. If C is the cyclic code generated by the product of the minimal polynomials

$$M^{(s)}(x)M^{(s+1)}(x) \ldots M^{(s+i)}(x)M^{(s-1)}(x) \ldots M^{(s-j)}(x)$$

for all $1 \le i,j \le q^2-1$, then C is Hermitian self-orthogonal.

Proof: According to Lemma II.2, it suffices to show that $Z \cap Z^{-q}=\emptyset$. Seeking a contradiction, we assume that $Z \cap Z^{-q} \neq \emptyset$. The cases with respect to the coset $\mathbb{C}_{[s]}$ are straightforward. Assume first that $\mathbb{C}_{[s+j]}=\mathbb{C}_{[-q(s+i)]}$, where $1 \le i,j \le q^2-1$. Then there exists $0 \le h \le m-1$ such that $s+j \equiv -q(s+i)q^{2h}$. Since $\gcd(q^2,n)=1$, $q^{2m} \equiv 1 \bmod n$, and $sq^{2t} \equiv s$ for all $0 \le t \le m-1$, one obtains

$$s+j \equiv -qs-qiq^{2h},$$

where $0 \le h \le m-1$.

Let us compute the expression $s+j+q(s+iq^{2h})$, where $0 \le h \le m-1$. If $h \le m-2$, it implies that

$$\begin{aligned} s+j+q(s+iq^{2h}) &\le \frac{q^{2m}-1}{q^2-1} + j + q\frac{q^{2m}-1}{q^2-1} + iq^{2m-3} \\ &\le \frac{q^{2m}-1}{q-1} + (q^2-1)(1+q^{2m-3}). \end{aligned}$$

By straightforward computation one can see that

$$\frac{q^{2m}-1}{q-1} + (q^2-1)(1+q^{2m-3}) < q^{2m}-1.$$

Since $s+j=-qs-qiq^{2h}$ does not hold, one has a contradiction.

If $h=m-1$, let us check the equivalence $s+j \equiv -q(s+i)q^{2m-2}$,

$$\begin{aligned} s+j \equiv -q(s+i)q^{2m-2} \Rightarrow j(q^2-1) &\equiv -iq^{2m-1}(q^2-1) \Rightarrow (j \\ &+ iq^{2m-1})(q^2-1) \equiv 0. \end{aligned}$$

Applying the division algorithm for i and q, it follows that $i=aq+r$, where $0 \le r < q$. Since $1 \le i \le q^2-1$ we also have $0 \le a < q$, so

$$\begin{aligned} (j+iq^{2m-1})(q^2-1) \equiv [j+(aq+r)q^{2m-1}](q^2-1) &\equiv (j+a) \\ \times(q^2-1) + r(q^2-1)q^{2m-1} &\equiv (j+a) \\ \times(q^2-1) + rq - rq^{2m-1} &\equiv 0 \Rightarrow rq^{2m-1} \\ - rq - (j+a)(q^2-1) &\equiv 0. \end{aligned}$$

If $r=0$ then $(j+a)(q^2-1) < q^{2m}-1$, hence $(j+a)(q^2-1) \not\equiv 0$. If $r>0$ then $0 < rq^{2m-1}-rq-(j+a)(q^2-1) < q^{2m}-1$, which is a contradiction.

The cases $\mathbb{C}_{[s+j]}=\mathbb{C}_{[-q(s-i)]}$, $\mathbb{C}_{[s-j]}=\mathbb{C}_{[-q(s+i)]}$, and $\mathbb{C}_{[s-j]}=\mathbb{C}_{[-q(s-i)]}$ are analogous to the previous proof. Therefore, C is Hermitian self-orthogonal as well. □

Keeping in mind Lemmas III.3–III.6 we are able to show Theorem III.2, the main result of this section:

Theorem III.2. Let $n=q^{2m}-1$, where $q \ge 4$ is a prime power and $m=\mathrm{ord}_n(q^2) \ge 3$. Then there exist quantum codes

with parameters $[\![n,n-4m(q^2-1)-2,d\geq 2q^2+2]\!]_q$.

Proof: Let C be the cyclic code generated by the product of the minimal polynomials

$$M^{(s)}(x)M^{(s+1)}(x)\ldots M^{(s+q^2-1)}(x)M^{(s-1)}(x)\ldots M^{(s-q^2+1)}(x).$$

It is easy to see that the element $s-q^2$ belongs to the coset $\mathbb{C}_{[s-1]}$ and the element $s+q^2$ belongs to $\mathbb{C}_{[s+1]}$. Then the defining set of C contains the sequence of consecutive integers $s-q^2,s-q^2+1,\ldots,s-1,s,s+1,\ldots,s+q^2-1,s+q^2$. From the BCH bound theorem, the minimum distance of C is greater than or equal to $2q^2+2$.

It is known that if $i\in\mathbb{C}_s$ then

$$M^{(i)}(x)=\prod_{j\in\mathbb{C}_s}(x-\alpha^j). \tag{1}$$

Equation (1) means that degree of the minimal polynomial $M^{(i)}(x)$ equals the cardinality of the coset $\mathbb{C}_s$, and so the degree of the generator polynomial of a cyclic code equals the cardinality of its defining set. From Lemmas III.4 and III.5 and from Eq. (1), we know that the dimension of code C equals $n-2m(q^2-1)-1$. Thus C has parameters $[n,n-2m(q^2-1)-1,d\geq 2q^2+2]_{q^2}$. From Lemma III.6, C is Hermitian self-orthogonal. Applying the Hermitian construction, an $[\![n,n-4m(q^2-1)-2,d\geq 2q^2+2]\!]_q$ quantum code is constructed. □

Corollary III.2 also constructs new families of good quantum codes:

Corollary III.2. Let $n=q^{2m}-1$, where $q\geq 4$ is a prime power and $m=\mathrm{ord}_n(q^2)\geq 3$. Then there exist quantum codes with parameters

(1) $[\![n,n-2mc-2,d\geq c+2]\!]_q$, where $1\leq c<q^2-1$,

(2) $[\![n,n-2m(q^2-1)-2,d\geq q^2+2]\!]_q$, and

(3) $[\![n,n-2m(c-1)-2,d\geq c+2]\!]_q$ for all $q^2+1\leq c\leq 2q^2-2$.

Proof:

(1) Let C' be the cyclic code generated by the product of the minimal polynomials

$$M^{(s)}(x)M^{(s+1)}(x)\ldots M^{(s+i)}(x)$$

for all $1\leq i<q^2-1$. From the BCH bound theorem, the minimum distance of C is greater than or equal to $i+2$. Again, from Lemmas III.4 and III.5 and since the degree of the generator polynomial of a cyclic code equals the cardinality of its defining set, the dimension of code C equals $n-mi-1$. Thus C has parameters $[n,n-mi-1,d\geq i+2]_{q^2}$. From Lemma III.6, C is Hermitian self-orthogonal. Applying the Hermitian construction an $[\![n,n-2mi-2,d\geq i+2]\!]_q$ quantum code is constructed for all $1\leq i<q^2-1$.

(2) Let C'' be the cyclic code generated by the product of the minimal polynomials

$$M^{(s)}(x)M^{(s+1)}(x)\ldots M^{(s+q^2-1)}(x).$$

We know that element $s+q^2$ belongs to the q^2-ary coset $\mathbb{C}_{[s+1]}$; from the BCH bound theorem, the minimum distance of C is greater than or equal to q^2+2. Its dimension is equal to $n-m(q^2-1)-1$; C has parameters $[n,n-m(q^2-1)-1,d\geq q^2+2]_{q^2}$ and it is Hermitian self-orthogonal. Applying the Hermitian construction one has an $[\![n,n-2m(q^2-1)-2,d\geq q^2+2]\!]_q$ quantum code.

(3) Let C''' be the cyclic code generated by the product of the minimal polynomials

$$M^{(s)}(x)M^{(s-1)}(x)\ldots M^{(s-j)}(x)M^{(s+1)}(x)\ldots M^{(s+q^2-1)}(x),$$

where $1\leq j<q^2-1$. From the BCH bound theorem, C has minimum distance greater than or equal to $j+q^2+2$. Its dimension equals $n-m(j+q^2-1)-1$. Set $j+q^2=c$. Thus the corresponding quantum code has parameters $[\![n,n-2m(c-1)-2,d\geq c+2]\!]_q$ for all $q^2+1\leq c\leq 2q^2-2$.

The proof is complete. □

We finish this section by presenting an illustrative example:

Example III.2. Consider $m=3$, $q=4$; so $n=4095$. Proceeding similarly as in the proof of Theorem III.2, we have constructed quantum codes with parameters $[\![4095,4087,d\geq 3]\!]_4$, $[\![4095,4081,d\geq 4]\!]_4$, $[\![4095,4075,d\geq 5]\!]_4$, $[\![4095,4069,d\geq 6]\!]_4$, $[\![4095,4063,d\geq 7]\!]_4$, $[\![4095,4057,d\geq 8]\!]_4$, and so on.

C. Construction III: Euclidean non-narrow-sense BCH codes

In this section we construct new families of good q-ary quantum codes derived from q-ary Steane's construction applied to certain families of non-narrow-sense BCH codes. In order to do this, we show suitable properties concerning their cyclotomic cosets as well as the fact that they are Euclidean self-orthogonal. We start by showing three useful lemmas:

Lemma III.7. Assume $n=q^m-1$, $q\neq 2$, $m=\mathrm{ord}_n(q)\geq 3$, and $s=\sum_{i=0}^{m-1}q^i$. Then the q-ary coset $\mathbb{C}_{[s]}$ has only one element.

Proof: This proof is similar to that of Lemma III.3. In fact, since $\gcd(q,n)=1$ and $q^m\equiv 1 \bmod n$ one has

$$\begin{aligned} sq^j &= \left(\sum_{i=0}^{m-1}q^i\right)q^j = q^jq^{(m-1)}+q^jq^{(m-2)}+\cdots+q^jq^{(m-j)} \\ &\quad + q^jq^{[m-(j+1)]}+q^jq^{[m-(j+2)]}+\cdots+q^jq^{[m-(m-1)]}+q^jq^{(m-m)} \\ &\equiv q^{(j-1)}+q^{(j-2)}+\cdots+q^{[j-(j-1)]}+1+q^{(m-1)}+q^{(m-2)}+\cdots \\ &\quad + q^{(j+1)}+q^j=\sum_{i=0}^{m-1}q^i=s, \end{aligned}$$

where $1\leq j\leq m-1$ and $m=\mathrm{ord}_n(q)$, that is, $sq^j\equiv s$ for all $0\leq j\leq m-1$. Therefore, the q-ary coset $\mathbb{C}_{[s]}$ has only one element. □

Lemma III.8. Suppose that $n=q^m-1$, where $q\geq 3$ and $m=\mathrm{ord}_n(q)\geq 3$. Let s given as above. Then the following hold:

(a) each one of the q-ary cosets $\mathbb{C}_{[s+i]}$ is distinct, where $1\leq i\leq q-1$;

(b) each one of the q-ary cosets $\mathbb{C}_{[s-j]}$ are distinct, where $1\leq j\leq q-1$; and

(c) the cosets of the form $\mathbb{C}_{[s+i]}$ are distinct of each one of the cosets $\mathbb{C}_{[s-j]}$, where $1\leq i,j\leq q-1$.

Proof:

(a) Assume there exist i,j, where $i\neq j$ and $1\leq i,j\leq q-1$, such that $\mathbb{C}_{[s+i]}=\mathbb{C}_{[s+j]}$. Then there exists $0\leq t\leq m-1$, such that $s+i\equiv(s+j)q^t$. From Lemma III.7 one has $sq^t\equiv s$. More-

over, since $\gcd(q,n)=1$ and $q^m \equiv 1 \bmod n$, it follows that

$$s+i \equiv (s+j)q^t \equiv s+jq^t \Rightarrow i \equiv jq^t.$$

Since $1 \leq i,j \leq q-1$, it follows that $jq^t < q^m-1$, and so

$$i \equiv jq^t \Rightarrow i = jq^t.$$

If $t=0$ then $i=j$ and if $t \geq 1$ the equality $i=jq^t$ does not hold, which is a contradiction. Thus, for $i \neq j$, one has $\mathbb{C}_{[s+j]} \neq \mathbb{C}_{[s+i]}$.

(b) Analogous to the previous item.

(c) Assume that $\mathbb{C}_{[s+i]}=\mathbb{C}_{[s-j]}$, where $1 \leq i,j \leq q-1$. Then there exists $0 \leq t \leq m-1$, such that $s+i \equiv (s-j)q^t$. Similarly, one has

$$s+i \equiv (s-j)q^t \equiv s-jq^t \Rightarrow i \equiv -jq^t.$$

Since $m \geq 3$, we know that

$$i+jq^t \leq (q-1)(q^{m-1}+1) < q^m-1,$$

and so $i=-jq^t$, which is a contradiction.

Thus, for each $i \neq j$, one concludes that $\mathbb{C}_{[s+i]} \neq \mathbb{C}_{[s-j]}$, as required. □

Lemma III.9. Suppose that $n=q^m-1$, $q \geq 4$, $m=\mathrm{ord}_n(q) \geq 3$, and s is given as above. Then the following hold:

(a) the cosets of the form $\mathbb{C}_{[s+i]}$, where $1 \leq i \leq q-1$, have m elements;

(b) the cosets of the form $\mathbb{C}_{[s-j]}$ have m elements, where $1 \leq j \leq q-1$.

Proof:

(a) The elements of the coset $\mathbb{C}_{[s+i]}$ are of the form $(s+i)q^t$, where $0 \leq t \leq m-1$ and $1 \leq i \leq q-1$. Since $\gcd(q,n)=1$, $q^m \equiv 1 \bmod n$, and $sq^t \equiv s$, it follows that $(s+i)q^t \equiv s+iq^t$. Considering $0 \leq t \leq m-2$ one obtains

$$s+iq^t < \frac{q^m-1}{q-1}+q^{m-1} < \frac{q^m-1}{3}+\frac{q^m-1}{3} < q^m-1.$$

This means that the first $m-1$ elements belonging to $\mathbb{C}_{[s+i]}$ are distinct for all $0 \leq t \leq m-2$ and for all $1 \leq i \leq q-1$; so $\mathbb{C}_{[s+i]}$ contains m elements because $m-1 > m/2$.

(b) Analogous to the previous item. □

We next show Lemma III.10 that generates families of Euclidean self-orthogonal non-narrow-sense BCH codes:

Lemma III.10. Suppose that $n=q^m-1$, $q \geq 4$, $m=\mathrm{ord}_n(q) \geq 3$, and $s=\sum_{i=0}^{m-1} q^i$. If C is the cyclic code generated by the product of the minimal polynomials

$$M^{(s)}(x)M^{(s+1)}(x) \ldots M^{(s+j)}(x)M^{(s-1)}(x) \ldots M^{(s-j)}(x),$$

where $1 \leq j \leq q-1$, then C is Euclidean self-orthogonal.

Proof: See Appendix. □

Let us recall the following result in [25]:

Corollary III.3. (Corollary 4 in [25]) Assume we have an $[N_0,K_0]$ linear code L which contains its Euclidean dual, $L^{\perp} \leq L$, and which can be enlarged to an $[N_0,K_0']$ linear code L', where $K_0' \geq K_0+2$. Then there exists a quantum symplectic code with parameters $[\![N_0, K_0+K_0'-N_0, d \geq \min\{d, \lceil \frac{q+1}{q} d' \rceil\}]\!]$, where $d=w(L \backslash L'^{\perp})$ and $d'=w(L' \backslash L^{\perp})$.

Theorems III.3 and III.4 are the main results of this section. They generate new families of good nonbinary quantum codes:

Theorem III.3. Let $n=q^m-1$, where $q \geq 4$ and $m=\mathrm{ord}_n(q) \geq 3$. Then there exist quantum codes with parameters $[\![n, n-m(2c-1)-2, d \geq c+2]\!]_q$ for all $1 \leq c \leq q-2$.

Proof: According to Corollary III.3, we have to construct Euclidean self-orthogonal BCH codes in order to obtain the corresponding quantum codes. For this purpose, consider C the cyclic code generated by the product of the minimal polynomials

$$M^{(s)}(x)M^{(s+1)}(x) \ldots M^{(s+i)}(x)M^{(s-1)}(x) \ldots M^{(s-j)}(x),$$

where $1 \leq i+j=c \leq q-2$. First we compute the minimum distance of C. Since its defining set contains the sequence $s-j, \ldots, s-1, s, s+1, \ldots, s+i$, from the BCH bound theorem, its minimum distance is greater than or equal to $c+2$.

We next compute the dimension of C. We know that the degree of the generator polynomial of a cyclic code equals the cardinality of its defining set. Thus, from Lemmas III.8 and III.9, C has dimension $n-mc-1$, and so it has parameters $[n, n-mc-1, d \geq c+2]_q$, where $1 \leq c \leq q-2$, $q \geq 4$, and $m=\mathrm{ord}_n(q) \geq 3$. Moreover, from Lemma III.10, C is Euclidean self-orthogonal.

Let C' be the cyclic code generated by the product of the minimal polynomials

$$M^{(s)}(x)M^{(s+1)}(x) \ldots M^{(s+i)}(x)M^{(s-1)}(x) \ldots M^{(s-j+1)}(x).$$

C' is an enlargement of C and has parameters $[n, n-m(c-1)-1, d' \geq c+1]_q$. Applying Corollary III.3 to C and C', since $\lceil \frac{q+1}{q} d' \rceil$ is, at least, $c+2$, then there exist quantum codes with parameters $[\![n, n-m(2c-1)-2, d \geq c+2]\!]_q$ for all $1 \leq c \leq q-2$. This completes the proof. □

Theorem III.4. Suppose that $n=q^m-1$, where $q \geq 4$ and $m=\mathrm{ord}_n(q) \geq 3$. Then there exist quantum codes with parameters

(a) $[\![n, n-m(2q-3)-2, d \geq q+1]\!]_q$,
(b) $[\![n, n-m(2q-1)-1, d \geq q+3]\!]_q$,
(c) $[\![n, n-m(2c-4)-2, d \geq c+2]\!]_q$,
(d) $[\![n, n-m(4q-8)-2, d \geq 2q]\!]_q$, and
(e) $[\![n, n-m(4q-5)-2, d \geq 2q+2]\!]_q$,

where $q+1 < c < 2q-2$.

Proof:

(a) Consider the cyclic code C generated by the product of the minimal polynomials

$$M^{(s)}(x)M^{(s+1)}(x) \ldots M^{(s+q-1)}(x)$$

and C' generated by the product of the minimal polynomials

$$M^{(s)}(x)M^{(s+1)}(x) \ldots M^{(s+q-2)}(x).$$

By Lemma III.10, C is Euclidean self-orthogonal. From the BCH bound theorem, the minimum distance of C is greater than or equal to $q+2$ because $s+q$ belongs to the coset $\mathbb{C}_{[s+1]}$. Similarly, from the BCH bound theorem, the minimum distance of C' is greater than or equal to q so, applying Corollary III.3, the corresponding quantum code has minimum distance greater than or equal to $q+1$ because $\lceil \frac{q+1}{q} d' \rceil = (\frac{q+1}{q})q = q+1$.

From Lemmas III.8 and III.9, C has dimension $k=n-m(q-1)-1$ and C' has dimension $k'=n-m(q-2)-1$. Applying Corollary III.3, it follows that the corresponding quantum code has dimension $n-m(2q-3)-2$. Then there ex-

ist quantum codes with parameters $[\![n, n-m(2q-3)-2, d \geq q+1]\!]_q$.

(b) Consider C generated by the product of the minimal polynomials

$$M^{(s-1)}(x)M^{(s)}(x)M^{(s+1)}(x)\ldots M^{(s+q-1)}(x)$$

and C' generated by the product of the minimal polynomials

$$M^{(s+1)}(x)\ldots M^{(s+q-1)}(x).$$

Again, by Lemma III.10, C is Euclidean self-orthogonal. From the BCH bound theorem, the minimum distance d of C is greater than or equal to $q+3$ and the minimum distance of C' is greater than or equal to $q+1$. We know that $\lceil \frac{q+1}{q} d' \rceil = \lceil \frac{q+1}{q}(q+1) \rceil = q+3$. Proceeding similarly as in the proof above, one has an $[\![n, n-m(2q-1)-1, d \geq q+3]\!]_q$ stabilizer code.

(c) Let C be the cyclic code generated by the product of the minimal polynomials

$$M^{(s)}(x)M^{(s+1)}(x)\ldots M^{(s+q-1)}(x)M^{(s-1)}(x)\ldots M^{(s-j)}(x)$$

and C' be the cyclic code generated by the product of the minimal polynomials

$$M^{(s)}(x)M^{(s+1)}(x)\ldots M^{(s+q-1)}(x)M^{(s-1)}(x)\ldots M^{(s-j+2)}(x),$$

where $j \geq 3$. Lemma III.10 asserts that C is Euclidean self-orthogonal. Proceeding as above, one can show that C has parameters $[n, n-m(c-1)-1, d \geq c+2]_q$ and C' has parameters $[n, n-m(c-3)-1, d \geq c]_q$, where $c=q+j$ and $q+1<c<2q-2$. Applying Corollary III.3, we obtain an $[\![n, n-m(2c-4)-2, d \geq c+2]\!]_q$ quantum code, where $q+1<c<2q-2$.

Items (d) and (e) are analogous to the previous one. □

Example III.3. If $m=3$ and $q=7$ then $n=342$. From Theorems III.3 and III.4, quantum codes with parameters $[\![342, 337, d \geq 3]\!]_7$, $[\![342, 331, d \geq 4]\!]_7$, $[\![342, 325, d \geq 5]\!]_7$, $[\![342, 319, d \geq 6]\!]_7$, $[\![342, 313, d \geq 7]\!]_7$, $[\![342, 307, d \geq 8]\!]_7$, $[\![342, 302, d \geq 10]\!]_7$ are constructed.

IV. CODE COMPARISONS

In this section we compare the parameters of quantum BCH codes available in the literature with the parameters of the new quantum codes.

In Table I, the new codes are derived from Sec. III A and have parameters $[\![n, n-4(c-2)-2, d \geq c]\!]_q$, where $m=\mathrm{ord}_n(q^2)=2$, $3 \leq c \leq q^2$, and $n=q^4-1$; $[\![n', k', d']\!]_q = [\![n', n'-2m\lceil(\delta-1)(1-1/q^2)\rceil, d' \geq \delta]\!]_q$ denote the parameters of Hermitian quantum codes shown in Theorem 21 in [10], where $m=\mathrm{ord}_n(q^2)=2$ and $2 \leq \delta \leq \lfloor n(q^m-1)/(q^{2m}-1) \rfloor$.

In Table II, the new codes are derived from Sec. III B and have parameters $[\![n, k, d]\!]_q$ given by

(i) $[\![n, n-2mc-2, d \geq c+2]\!]_q$ for all $1 \leq c \leq q^2-2$,

(ii) $[\![n, n-2m(q^2-1)-2, d \geq q^2+2]\!]_q$,

(iii) $[\![n, n-2m(c-1)-2, d \geq c+2]\!]_q$ for all $q^2+1 \leq c \leq 2q^2-2$, and

(iv) $[\![n, n-4m(q^2-1)-2, d \geq 2q^2+2]\!]_q$,

where $n=q^{2m}-1$, $q \geq 4$ is a prime power, and $m=\mathrm{ord}_n(q^2) \geq 3$; $[\![n', k', d']\!]_q = [\![n', n'-2m\lceil(\delta-1)(1-1/q^2)\rceil, d' \geq \delta]\!]_q$ denote the parameters of Hermitian quantum codes shown in Theorem 21 in [10], where $m=\mathrm{ord}_n(q^2) \geq 3$ and $2 \leq \delta \leq \lfloor n(q^m-1)/(q^{2m}-1) \rfloor$.

In Table III, $[\![n, k, d]\!]_q$ denote the parameters of the new quantum codes derived from Sec. III C and assume the values

(i) $[\![n, n-m(2c-1)-2, d \geq c+2]\!]_q$ for all $1 \leq c \leq q-2$,

(ii) $[\![n, n-m(2q-3)-2, d \geq q+1]\!]_q$,

(iii) $[\![n, n-m(2q-1)-1, d \geq q+3]\!]_q$,

(iv) $[\![n, n-m(2c-4)-2, d \geq c+2]\!]_q$,

(v) $[\![n, n-m(4q-8)-2, d \geq 2q]\!]_q$, and

TABLE I. Code comparisons.

New Hermitian codes	Hermitian codes in [9,10]
$[\![n, n-4(c-2)-2, d \geq c]\!]_q$	$[\![n', k', d']\!]_q$
$m=2$, $q=3$	
$[\![80, 74, d \geq 3]\!]_3$	$[\![80, 72, d' \geq 3]\!]_3$
$[\![80, 70, d \geq 4]\!]_3$	$[\![80, 68, d' \geq 4]\!]_3$
$[\![80, 66, d \geq 5]\!]_3$	$[\![80, 64, d' \geq 5]\!]_3$
$[\![80, 62, d \geq 6]\!]_3$	$[\![80, 60, d' \geq 6]\!]_3$
$[\![80, 58, d \geq 7]\!]_3$	$[\![80, 56, d' \geq 7]\!]_3$
$[\![80, 54, d \geq 8]\!]_3$	$[\![80, 52, d' \geq 8]\!]_3$
$[\![80, 50, d \geq 9]\!]_3$	
$m=2$, $q=4$	
$[\![255, 249, d \geq 3]\!]_4$	$[\![255, 247, d' \geq 3]\!]_4$
$[\![255, 245, d \geq 4]\!]_4$	$[\![255, 243, d' \geq 4]\!]_4$
$[\![255, 241, d \geq 5]\!]_4$	$[\![255, 239, d' \geq 5]\!]_4$
$[\![255, 237, d \geq 6]\!]_4$	$[\![255, 235, d' \geq 6]\!]_4$
$[\![255, 233, d \geq 7]\!]_4$	$[\![255, 231, d' \geq 7]\!]_4$
$[\![255, 229, d \geq 8]\!]_4$	$[\![255, 227, d' \geq 8]\!]_4$
$[\![255, 225, d \geq 9]\!]_4$	$[\![255, 223, d' \geq 9]\!]_4$
$[\![255, 221, d \geq 10]\!]_4$	$[\![255, 219, d' \geq 10]\!]_4$
$[\![255, 217, d \geq 11]\!]_4$	$[\![255, 215, d' \geq 11]\!]_4$
$[\![255, 213, d \geq 12]\!]_4$	$[\![255, 211, d' \geq 12]\!]_4$
$[\![255, 209, d \geq 13]\!]_4$	$[\![255, 207, d' \geq 13]\!]_4$
$[\![255, 205, d \geq 14]\!]_4$	$[\![255, 203, d' \geq 14]\!]_4$
$[\![255, 201, d \geq 15]\!]_4$	$[\![255, 199, d' \geq 15]\!]_4$
$[\![255, 197, d \geq 16]\!]_4$	
$m=2$, $q=5$	
$[\![624, 618, d \geq 3]\!]_5$	$[\![624, 616, d' \geq 3]\!]_5$
$[\![624, 614, d \geq 4]\!]_5$	$[\![624, 612, d' \geq 4]\!]_5$
$[\![624, 610, d \geq 5]\!]_5$	$[\![624, 608, d' \geq 5]\!]_5$
$[\![624, 606, d \geq 6]\!]_5$	$[\![624, 604, d' \geq 6]\!]_5$
$[\![624, 602, d \geq 7]\!]_5$	$[\![624, 600, d' \geq 7]\!]_5$
$[\![624, 598, d \geq 8]\!]_5$	$[\![624, 596, d' \geq 8]\!]_5$
$[\![624, 594, d \geq 9]\!]_5$	$[\![624, 592, d' \geq 9]\!]_5$
$[\![624, 590, d \geq 10]\!]_5$	$[\![624, 588, d' \geq 10]\!]_5$
$[\![624, 586, d \geq 11]\!]_5$	$[\![624, 584, d' \geq 11]\!]_5$
$[\![624, 582, d \geq 12]\!]_5$	$[\![624, 580, d' \geq 12]\!]_5$

TABLE II. Code comparisons.

New Hermitian codes	Hermitian codes in [9,10]
$[\![n,k,d]\!]_q$	$[\![n',k',d']\!]_q$
$m=3$, $q=4$	
$[\![4095,4087,d\geq 3]\!]_4$	$[\![4095,4083,d'\geq 3]\!]_4$
$[\![4095,4081,d\geq 4]\!]_4$	$[\![4095,4077,d'\geq 4]\!]_4$
$[\![4095,4075,d\geq 5]\!]_4$	$[\![4095,4071,d'\geq 5]\!]_4$
$[\![4095,4069,d\geq 6]\!]_4$	$[\![4095,4065,d'\geq 6]\!]_4$
$[\![4095,4063,d\geq 7]\!]_4$	$[\![4095,4059,d'\geq 7]\!]_4$
$[\![4095,4057,d\geq 8]\!]_4$	$[\![4095,4053,d'\geq 8]\!]_4$
$[\![4095,4051,d\geq 9]\!]_4$	$[\![4095,4047,d'\geq 9]\!]_4$
$[\![4095,4045,d\geq 10]\!]_4$	$[\![4095,4041,d'\geq 10]\!]_4$
$[\![4095,4039,d\geq 11]\!]_4$	$[\![4095,4035,d'\geq 11]\!]_4$
$[\![4095,4033,d\geq 12]\!]_4$	$[\![4095,4029,d'\geq 12]\!]_4$
$[\![4095,4027,d\geq 13]\!]_4$	$[\![4095,4023,d'\geq 13]\!]_4$
$[\![4095,4021,d\geq 14]\!]_4$	$[\![4095,4017,d'\geq 14]\!]_4$
$[\![4095,4015,d\geq 15]\!]_4$	$[\![4095,4011,d'\geq 15]\!]_4$
$[\![4095,4009,d\geq 16]\!]_4$	$[\![4095,4005,d'\geq 16]\!]_4$
	$[\![4095,4005,d'\geq 17]\!]_4$
$[\![4095,4003,d\geq 18]\!]_4$	$[\![4095,3999,d'\geq 18]\!]_4$
$[\![4095,3997,d\geq 19]\!]_4$	$[\![4095,3993,d'\geq 19]\!]_4$
$[\![4095,3991,d\geq 20]\!]_4$	$[\![4095,3987,d'\geq 20]\!]_4$
$[\![4095,3985,d\geq 21]\!]_4$	$[\![4095,3981,d'\geq 21]\!]_4$
$[\![4095,3979,d\geq 22]\!]_4$	$[\![4095,3975,d'\geq 22]\!]_4$
$[\![4095,3973,d\geq 23]\!]_4$	$[\![4095,3969,d'\geq 23]\!]_4$
$[\![4095,3967,d\geq 24]\!]_4$	$[\![4095,3963,d'\geq 24]\!]_4$
$[\![4095,3961,d\geq 25]\!]_4$	$[\![4095,3957,d'\geq 25]\!]_4$
$[\![4095,3955,d\geq 26]\!]_4$	$[\![4095,3951,d'\geq 26]\!]_4$
$[\![4095,3949,d\geq 27]\!]_4$	$[\![4095,3945,d'\geq 27]\!]_4$
$[\![4095,3943,d\geq 28]\!]_4$	$[\![4095,3939,d'\geq 28]\!]_4$
$[\![4095,3937,d\geq 29]\!]_4$	$[\![4095,3933,d'\geq 29]\!]_4$
$[\![4095,3931,d\geq 30]\!]_4$	$[\![4095,3927,d'\geq 30]\!]_4$
$[\![4095,3925,d\geq 31]\!]_4$	$[\![4095,3921,d'\geq 31]\!]_4$
$[\![4095,3919,d\geq 32]\!]_4$	$[\![4095,3915,d'\geq 32]\!]_4$
	$[\![4095,3915,d'\geq 33]\!]_4$
$[\![4095,3913,d\geq 34]\!]_4$	$[\![4095,3909,d'\geq 34]\!]_4$

(vi) $[\![n,n-m(4q-5)-2,d\geq 2q+2]\!]_q$, where $q+1<c<2q-2$.

The parameters $[\![n'',k'',d'']\!]_q$ denote the parameters of quantum BCH codes derived from q-ary Steane's construction (Corollary 4 in [25]) when applied to narrow-sense BCH codes. These codes are generated by the same method presented in Table I in [33] by considering the criterion for classical Euclidean self-orthogonal BCH codes of Theorems 3 and 5 in [10]:

Theorem IV.1. (Theorem 3 in [10]) Assume $m=\mathrm{ord}_n(q)$ is the multiplicative order of q mod n and let (statement)=1 if statement is true and (statement)=0 otherwise. If the designed distance δ is in the range $2\leq\delta\leq\delta_{\max}=\lfloor\gamma\rfloor$, where $\gamma=[n/(q^m-1)][q^{\lceil m/2\rceil}-1-(q-2)(m \text{ is odd})]$, then $\mathrm{BCH}(n,q;\delta)^{\perp}\subseteq\mathrm{BCH}(n,q;\delta)$.

To illustrate this procedure, we construct an $[\![80,60,d\geq 5]\!]_3$ quantum code. Consider the classical BCH codes with parameters $L=[80,68,5]_3$ and $L'=[80,72,4]_3$, according to Corollary III.3. From Theorem IV.1, $L=[80,68,5]_3$ is Euclidean self-orthogonal. In this case, $\lceil\frac{q+1}{q}d'\rceil=\lceil\frac{4}{3}4\rceil=6$, $K_0+K_0'-N_0=72+68-80=60$, and $d\geq 5$. Then an $[\![80,60,d\geq 5]\!]_3$ quantum code is generated. Note that if we consider $L=[80,68,5]_3$ and $L'=[80,76,2]_3$ the corresponding quantum code does not have minimum distance $d\geq 5$ since $\lceil\frac{4}{3}2\rceil=3$.

As can be seen in Tables I–III, the new codes have parameters better than the parameters of the quantum codes shown in [9,10]. Furthermore, the new codes have parameters better than the parameters of the quantum codes derived from q-ary Steane's construction (Corollary 4 in [25]) when applied to narrow-sense BCH codes. In other words, fixing n and d, these new families achieve greater values of the number of qudits than the codes shown in [9,10] and also to those derived from q-ary Steane's construction. Further, note that the $[\![63,58,d\geq 3]\!]_4$, $[\![124,119,d\geq 3]\!]_5$, and $[\![342,337,d\geq 3]\!]_7$ codes (see Table III) almost achieve the quantum Singleton bound given by $n\geq k+2d-2$.

V. FINAL REMARKS

We have presented three constructions generating new families of good nonbinary quantum codes derived from non-narrow-sense BCH codes. The quantum nonbinary BCH codes presented here have parameters better than the ones available in the literature.

ACKNOWLEDGMENTS

We would like to thank State University of Ponta Grossa for the financial support during this research. We also would like to thank Dr. Ricardo C. L. F. Oliveira, Dr. J. H. Kleinschmidt, and Dr. José Tadeu Teles Lunardi for critical reading.

APPENDIX: PROOF OF LEMMA III.10

Proof: From Lemma II.1, it suffices to show that $Z\cap Z^{-1}=\emptyset$. Seeking a contradiction, we assume that $Z\cap Z^{-1}\neq\emptyset$. The cases with respect to the coset $\mathbb{C}_{[s]}$ are straightforward.

(1) Assume first $\mathbb{C}_{[s+i]}=\mathbb{C}_{[-(s+j)]}$, where $1\leq i,j\leq q-1$. Then there exists $0\leq t\leq m-1$ such that $s+i\equiv-(s+j)q^t$. Since $\gcd(q,n)=1$, $q^m\equiv 1 \bmod n$, and $sq^t\equiv s$ for each $0\leq t\leq m-1$, it follows that

$$s+i\equiv -s-jq^t\Rightarrow 2s\equiv -(i+jq^t).$$

If $0\leq t\leq m-2$ then

$$2s+i+jq^t\leq\frac{2q^m-2}{q-1}+(q-1)(1+q^{m-2})<q^m-1\Rightarrow 2s+i+jq^t<q^m-1$$

because $q\geq 4$, and so $s+i=-s-jq^t$, which is a contradiction.

TABLE III. Code comparisons.

	New codes—construction III	Codes shown in [25]
m, q	$[\![n,k,d]\!]_q$	$[\![n'',k'',d'']\!]_q : L,L'$
$m=3, q=4$	$[\![63,58,d\geq 3]\!]_4$	$[\![63,54,d''\geq 3]\!]_4$: $[63,57,3]_4$, $[63,60,2]_4$
	$[\![63,52,d\geq 4]\!]_4$	$[\![63,48,d''\geq 4]\!]_4$: $[63,54,5]_4$, $[63,57,3]_4$
	$[\![63,46,d\geq 5]\!]_4$	
		$[\![63,42,d''\geq 6]\!]_4$: $[63,51,6]_4$, $[63,54,5]_4$
	$[\![63,41,d\geq 7]\!]_4$	$[\![63,39,d''\geq 7]\!]_4$: $[63,48,7]_4$, $[63,54,5]_4$
	$[\![63,37,d\geq 8]\!]_4$	
		$[\![63,30,d''\geq 9]\!]_4$: $[63,45,9]_4$, $[63,48,7]_4$
	$[\![63,28,d\geq 10]\!]_4$	$[\![63,24,d''\geq 10]\!]_4$: $[63,42,10]_4$, $[63,45,9]_4$
$m=3, q=5$	$[\![124,119,d\geq 3]\!]_5$	$[\![124,115,d''\geq 3]\!]_5$: $[124,118,3]_5$, $[124,121,2]_5$
	$[\![124,113,d\geq 4]\!]_5$	$[\![124,109,d''\geq 4]\!]_5$: $[124,115,4]_5$, $[124,118,3]_5$
	$[\![124,107,d\geq 5]\!]_5$	$[\![124,103,d''\geq 5]\!]_5$: $[124,112,6]_5$, $[124,115,4]_5$
	$[\![124,101,d\geq 6]\!]_5$	
		$[\![124,97,d''\geq 7]\!]_5$: $[124,109,7]_5$, $[124,112,6]_5$
	$[\![124,96,d\geq 8]\!]_5$	$[\![124,94,d''\geq 8]\!]_5$: $[124,106,8]_5$, $[124,112,6]_5$
	$[\![124,92,d\geq 9]\!]_5$	$[\![124,88,d''\geq 9]\!]_5$: $[124,103,9]_5$, $[124,109,7]_5$
	$[\![124,86,d\geq 10]\!]_5$	$[\![124,82,d''\geq 10]\!]_5$: $[124,100,11]_5$, $[124,106,8]_5$
		$[\![124,79,d''\geq 11]\!]_5$: $[124,100,11]_5$, $[124,103,9]_5$
	$[\![124,77,d\geq 12]\!]_5$	$[\![124,73,d''\geq 12]\!]_5$: $[124,97,12]_5$, $[124,100,11]_5$
$m=3, q=7$	$[\![342,337,d\geq 3]\!]_7$	$[\![342,333,d''\geq 3]\!]_7$: $[342,336,3]_7$, $[342,339,2]_7$
	$[\![342,331,d\geq 4]\!]_7$	$[\![342,327,d''\geq 4]\!]_7$: $[342,333,4]_7$, $[342,336,3]_7$
	$[\![342,325,d\geq 5]\!]_7$	$[\![342,321,d''\geq 5]\!]_7$: $[342,330,5]_7$, $[342,333,4]_7$
	$[\![342,319,d\geq 6]\!]_7$	$[\![342,315,d''\geq 6]\!]_7$: $[342,327,6]_7$, $[342,330,5]_7$
	$[\![342,313,d\geq 7]\!]_7$	$[\![342,309,d''\geq 7]\!]_7$: $[342,324,8]_7$, $[342,327,6]_7$
	$[\![342,307,d\geq 8]\!]_7$	
		$[\![342,303,d''\geq 9]\!]_7$: $[342,321,9]_7$, $[342,324,8]_7$
	$[\![342,302,d\geq 10]\!]_7$	$[\![342,300,d''\geq 10]\!]_7$: $[342,318,10]_7$, $[342,324,8]_7$
	$[\![342,298,d\geq 11]\!]_7$	$[\![342,294,d''\geq 11]\!]_7$: $[342,315,11]_7$, $[342,321,9]_7$
	$[\![342,292,d\geq 12]\!]_7$	$[\![342,288,d''\geq 12]\!]_7$: $[342,312,12]_7$, $[342,318,10]_7$
	$[\![342,286,d\geq 13]\!]_7$	$[\![342,282,d''\geq 13]\!]_7$: $[342,309,13]_7$, $[342,315,11]_7$
	$[\![342,280,d\geq 14]\!]_7$	$[\![342,276,d''\geq 14]\!]_7$: $[342,306,15]_7$, $[342,312,12]_7$
		$[\![342,273,d''\geq 15]\!]_7$: $[342,306,15]_7$, $[342,309,13]_7$
	$[\![342,271,d\geq 16]\!]_7$	$[\![342,267,d''\geq 16]\!]_7$: $[342,303,16]_7$, $[342,306,15]_7$
$m=4, q=4$	$[\![255,249,d\geq 3]\!]_4$	$[\![255,243,d''\geq 3]\!]_4$: $[255,247,3]_4$, $[255,251,2]_4$
	$[\![255,241,d\geq 4]\!]_4$	$[\![255,235,d''\geq 4]\!]_4$: $[255,243,5]_4$, $[255,247,3]_4$
	$[\![255,233,d\geq 5]\!]_4$	
		$[\![255,227,d''\geq 6]\!]_4$: $[255,239,6]_4$, $[255,243,5]_4$
	$[\![255,226,d\geq 7]\!]_4$	$[\![255,223,d''\geq 7]\!]_4$: $[255,235,7]_4$, $[255,243,5]_4$
	$[\![255,221,d\geq 8]\!]_4$	
		$[\![255,211,d''\geq 9]\!]_4$: $[255,231,9]_4$, $[255,235,7]_4$
	$[\![255,209,d\geq 10]\!]_4$	$[\![255,203,d''\geq 10]\!]_4$: $[255,227,10]_4$, $[255,231,9]_4$
$m=4, q=5$	$[\![624,618,d\geq 3]\!]_5$	$[\![624,612,d''\geq 3]\!]_5$: $[624,616,3]_5$, $[624,620,2]_5$
	$[\![624,610,d\geq 4]\!]_5$	$[\![624,604,d''\geq 4]\!]_5$: $[624,612,4]_5$, $[624,616,3]_5$
	$[\![624,602,d\geq 5]\!]_5$	$[\![624,596,d''\geq 5]\!]_5$: $[624,608,6]_5$, $[624,612,4]_5$

TABLE III. (*Continued.*)

	New codes—construction III	Codes shown in [25]
m, q	$[\![n,k,d]\!]_q$	$[\![n'',k'',d'']\!]_q : L,L'$
	$[\![624,594,d\geq 6]\!]_5$	
		$[\![624,588,d''\geq 7]\!]_5$: $[624,604,7]_5$, $[624,608,6]_5$
	$[\![624,587,d\geq 8]\!]_5$	$[\![624,584,d''\geq 8]\!]_5$: $[624,600,8]_5$, $[624,608,6]_5$
	$[\![624,582,d\geq 9]\!]_5$	$[\![624,576,d''\geq 9]\!]_5$: $[624,596,9]_5$, $[624,604,7]_5$
	$[\![624,574,d\geq 10]\!]_5$	$[\![624,568,d''\geq 10]\!]_5$: $[624,592,11]_5$, $[624,600,8]_5$
		$[\![624,564,d''\geq 11]\!]_5$: $[624,592,11]_5$, $[624,596,9]_5$
	$[\![624,562,d\geq 12]\!]_5$	$[\![624,556,d''\geq 12]\!]_5$: $[624,588,12]_5$, $[624,592,11]_5$

Next we consider the case $t=m-1$. It is easy to see that for each $1\leq i,j\leq q-3$, one obtains

$$2s+i+jq^{m-1}<q^m-1,$$

and since $s+i=-s-jq^{m-1}$ does not hold, this implies in a contradiction. Similarly, if $j=q-3$ and $1\leq i\leq q-1$, one concludes that

$$2s+i+jq^{m-1}<q^m-1,$$

and since $s+i\neq -s-jq^{m-1}$ one has a contradiction.

If $j\geq q-2$, it follows that $2s+i+jq^t>q^m-1$. Let us compute the equivalence $2s\equiv -(i+jq^{m-1})$ for $j=q-2$ and $1\leq i\leq q-1$,

$$2s\equiv -[i+(q-2)q^{m-1}]\Rightarrow 2s\equiv -i-1+2q^{m-1}.$$

Since $0<2s+i+1-2q^{m-1}<q^m-1$ and also $2s\neq -i-1+2q^{m-1}$ hold, one has a contradiction.

Considering $j=q-1$ and $1\leq i\leq q-1$ and computing the equivalence $2s\equiv -(i+jq^{m-1})$, it implies that

$$2s\equiv -[i+(q-1)q^{m-1}]\Rightarrow 2s\equiv -i-1+q^{m-1}.$$

Since $0<2s+i+1-q^{m-1}<q^m-1$ and also $2s\neq -i-1+q^{m-1}$ are true, the equivalence $2s\equiv -[i+(q-1)q^{m-1}]$ does not hold, which is a contradiction.

(2) Suppose that $\mathbb{C}_{[s-i]}=\mathbb{C}_{[-(s-j)]}$, where $1\leq i,j\leq q-1$. Then there exists $0\leq t\leq m-1$ such that $s-i\equiv -(s-j)q^t$. Since $\gcd(q,n)=1$, $q^m\equiv 1 \bmod n$, and $sq^t\equiv s$ for each $0\leq t\leq m-1$, it follows that

$$s-i\equiv -s+jq^t\Rightarrow 2s\equiv i+jq^t.$$

If $0\leq t\leq m-2$ then the inequalities $2s<q^m-1$ and $2s>i+jq^t$ are true, which is a contradiction.

If $t=m-1$, let us compute the equivalence $2s\equiv i+jq^{m-1}$,

$$2s\equiv i+jq^{m-1}\Rightarrow 2(q^m-1)\equiv (q-1)(i+jq^{m-1})\Rightarrow (q-1)i+(q-1)jq^{m-1}\equiv 0\Rightarrow (q-1)i+j-jq^{m-1}\equiv 0\Rightarrow jq^{m-1}-(q-1)i-j\equiv 0.$$

Since $0<jq^{m-1}-(q-1)i-j<q^m-1$, the equivalence $2s\equiv i+jq^t$ does not hold, which is a contradiction.

(3) Assume that $\mathbb{C}_{[s+i]}=\mathbb{C}_{[-(s-j)]}$, where $1\leq i,j\leq q-1$. Then there exists $0\leq t\leq m-1$ such that $s+i\equiv -(s-j)q^t$ and so

$$2s\equiv jq^t-i.$$

If $t=0$ and $i=j$, it implies that $2s\equiv 0$, which is a contradiction since $0<2s<q^m-1$. If $0\leq t\leq m-2$ and $i\neq j$ then we know that

$$2s\equiv jq^t-i\Rightarrow (q-1)(jq^t-i)\equiv 0,$$

and so $-(q^m-1)<(q-1)(jq^t-i)<q^m-1$ and $(q-1)(jq^t-i)\neq 0$, which is a contradiction.

If $t=m-1$, one obtains

$$(q-1)(jq^{m-1}-i)\equiv 0\Rightarrow jq^{m-1}+i(q-1)-j\equiv 0.$$

Since $0<jq^{m-1}+i(q-1)-j<q^m-1$, the equivalence $s+i\equiv -(s-j)q^t$ does not hold, which is a contradiction.

(4) Finally, if $\mathbb{C}_{[s-i]}=\mathbb{C}_{[-(s+j)]}$ then $s-i\equiv -(s+j)q^t$ for some $0\leq t\leq m-1$. Thus

$$2s\equiv i-jq^t.$$

As above, if $t=0$ and $i=j$, it implies that $2s\equiv 0$, which is a contradiction since $0<2s<q^m-1$. If $0\leq t\leq m-2$ and $i\neq j$ then we know that

$$2s\equiv i-jq^t\Rightarrow (q-1)(i-jq^t)\equiv 0,$$

which is a contradiction. Moreover, it is easy to see that the equivalence $(q-1)(i-jq^{m-1})\equiv 0$ does not hold, which is a contradiction.

Therefore, C is Euclidean self-orthogonal, as desired. □

[1] A. Ashikhmin and E. Knill, IEEE Trans. Inf. Theory **47**, 3065(2001).
[2] J. Bierbrauer and Y. Edel, J. Comb. Designs **8**, 174 (2000).
[3] A. R. Calderbank *et al.*, IEEE Trans. Inf. Theory **44**, 1369 (1998).
[4] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, Phys. Rev. Lett. **78**, 405 (1997).
[5] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).
[6] A. Ketkar *et al.*, IEEE Trans. Inf. Theory **52**, 4892 (2006).
[7] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[8] C. D. Albuquerque *et al.*, J. Math. Phys. **50**, 023513 (2009).
[9] S. A. Aly *et al.*, Proceedings of the International Symposium on Information Theory (ISIT), 2006, pp. 1114-1118.
[10] S. A. Aly *et al.*, IEEE Trans. Inf. Theory **53**, 1183 (2007).
[11] S. Bravyi and A. Kitaev, e-print arXiv:quant-ph/9811052.
[12] H. F. Chau, Phys. Rev. A **56**, R1 (1997).
[13] H. Chen, IEEE Trans. Inf. Theory **47**, 2059 (2001).
[14] H. Chen *et al.*, IEEE Trans. Inf. Theory **51**, 2915 (2005).
[15] G. D. Cohen *et al.*, IEEE Trans. Inf. Theory **45**, 2495 (1999).
[16] G. D. Forney *et al.*, IEEE Trans. Inf. Theory **53**, 865 (2007).
[17] M. Freedman and D. Meyer, e-print arXiv:quant-ph/9810055.
[18] D. Gottesman, Phys. Rev. A **54**, 1862 (1996).
[19] M. Grassl, T. Beth, and T. Pellizzari, Phys. Rev. A **56**, 33 (1997).
[20] M. Grassl and T. Beth, Proceedings of the Tenth International Symposium on Theoretical and Electrical Engineering, 1999, p. 207–212.
[21] M. Grassl *et al.*, Int. J. Quantum Inf. **2**, 757 (2004).
[22] M. Grassl *et al.*, AAECC-13, 1999, Vol. 1709, 231–244.
[23] M. Grassl, P. Shor, G. Smith, J. Smolin, and B. Zeng, Phys. Rev. A **79**, 050306(R) (2009).
[24] K. Guenda, Int. J. Quantum Inf. **7**, 373 (2009).
[25] M. Hamada, IEEE Trans. Inf. Theory **54**, 5689 (2008).
[26] A. Kitaev, Ann. Phys. **303**, 2 (2003).
[27] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, Phys. Rev. Lett. **77**, 198 (1996).
[28] R. Li and X. Li, IEEE Trans. Inf. Theory **50**, 1331 (2004).
[29] R. Li and X. Li, Discrete Math. **308**, 1603 (2008).
[30] Z. Ma *et al.*, Lect. Notes Comput. Sci. **3959**, 675 (2006).
[31] M. Postol, e-print arXiv:quant-ph/0108131.
[32] P. K. Sarvepalli and A. Klappenecker, Proceedings of the International Symposium on Information Theory (ISIT), 2005, p. 1023–1027.
[33] A. Steane, IEEE Trans. Inf. Theory **45**, 2492 (1999).
[34] A. M. Steane, IEEE Trans. Inf. Theory **45**, 1701 (1999).
[35] B. Sundeep and A. Thangaraj, IEEE Trans. Inf. Theory **53**, 2480 (2007).
[36] A. Thangaraj and S. McLaughlin, IEEE Trans. Inf. Theory **47**, 1176 (2001).
[37] L. Xiaoyan, IEEE Trans. Inf. Theory **50**, 547 (2004).
[38] L. Zhang and I. Fuss, e-print arXiv:quant-ph/9703045.
[39] Y. Xu, Z. Ma, and C. Zhang, Chin. J. Electron. **26**, 64(2009).
[40] W. W. Peterson and W. J. Weldon, Jr., *Error-Correcting Codes* (MIT Press, Cambridge, MA, 1972).
[41] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes* (North-Holland, Amsterdam, 1977).
[42] R. C. Bose and D. K. Ray-Chaudhuri, Inf. Control. **3**, 68 (1960).
[43] R. C. Bose and D. K. Ray-Chaudhuri, Inf. Control. **3**, 279 (1960).
[44] A. Hocquenghem, Chiffres **2**, 147 (1959).
[45] D.-W. Yue and G.-Z. Feng, IEEE Trans. Inf. Theory **46**, 2625 (2000).
[46] D.-W. Yue and Z.-M. Hu, Chin. J. Electron. **18**, 263 (1996).