Advances in Mathematics of Communications
Volume 5, No. 1, 2011, 41–57
doi:10.3934/amc.2011.5.41

FROM SKEW-CYCLIC CODES TO ASYMMETRIC QUANTUM CODES

Martianus Frederic Ezerman and San Ling

Division of Mathematical Sciences
School of Physical and Mathematical Sciences
Nanyang Technological University
21 Nanyang Link, Singapore 637371, Singapore

Patrick Solé

Centre National de la Recherche Scientifique (CNRS/LTCI)
Telecom-ParisTech, Dept Comelec
46 rue Barrault, 75634 Paris, France

Olfa Yemen

Institut Préparatoire aux Études d'Ingénieurs El Manar
Campus Universitaire El Manar, Tunis, Tunisia

(Communicated by Simon Litsyn)

Abstract. We introduce an additive but not $\mathbb{F}_4$-linear map S from $\mathbb{F}_4^n$ to $\mathbb{F}_4^{2n}$ and exhibit some of its interesting structural properties. If C is a linear $[n,k,d]_4$-code, then $S(C)$ is an additive $(2n, 2^{2k}, 2d)_4$-code. If C is an additive cyclic code then $S(C)$ is an additive quasi-cyclic code of index 2. Moreover, if C is a module θ-cyclic code, a recently introduced type of code which will be explained below, then $S(C)$ is equivalent to an additive cyclic code if n is odd and to an additive quasi-cyclic code of index 2 if n is even. Given any $(n, M, d)_4$-code C, the code $S(C)$ is self-orthogonal under the trace Hermitian inner product. Since the mapping S preserves nestedness, it can be used as a tool in constructing additive asymmetric quantum codes.

1. Introduction

The class of *skew-cyclic codes* was introduced in [2]. These linear codes have the property of being invariant under the operation of cyclic shift composed with overall conjugation. Demanding an ideal structure on the codes forces us, over $\mathbb{F}_4$, to work in even lengths only. By relaxing this structure to that of a module [3], it is now possible to deal with skew-cyclic codes of any lengths.

In the present work, a mapping S is introduced to map any skew-cyclic codes of length n over $\mathbb{F}_4$ into codes of length $2n$ which are invariant under a coordinate permutation denoted by σ. The permutation σ is a cyclic permutation for n odd and a product of two cycles of equal length for n even.

2000 *Mathematics Subject Classification:* Primary: 58F15, 58F17; Secondary: 53C35.
Key words and phrases: Additive codes, best-known linear codes, cyclic codes, quantum codes, Reed-Solomon codes, self-orthogonal codes, skew-cyclic codes.

Besides these structural properties, the mapping S has interesting duality properties and preserves nestedness. These allow us to construct *asymmetric quantum codes* following the method given in [6].

The material is organized as follows. In Section 2, we state some basic definitions and properties of linear and additive codes. More specifically, the two families, $\mathbf{4}^{\mathrm{H}}$ and $\mathbf{4}^{\mathrm{H}+}$, of codes over $\mathbb{F}_4$ are formally defined. Their respective dualities and weight enumerators are stated.

Section 3 introduces the mapping S and its basic properties. The definition of and some algebraic background on module θ-cyclic codes are discussed in Section 4. The study of the images of these codes under the mapping S is also given. A very brief introduction to asymmetric quantum codes follows in Section 5.

In Section 6, an analysis of the weight enumerators is performed. This is important in understanding the parameters of the asymmetric quantum codes that can be obtained under the mapping S. Two systematic constructions of asymmetric quantum codes are given in Section 7. The one based on best-known linear codes is presented in Subsection 7.1 while the other one, based on concatenated Reed-Solomon codes, is given in Subsection 7.2. The last section contains conclusions and open problems.

2. Preliminaries

Let p be a prime and $q = p^m$ for some positive integer m. An $[n, k, d]_q$-linear code C of length n, dimension k, and minimum distance d is a subspace of dimension k of the vector space $\mathbb{F}_q^n$ over the finite field $\mathbb{F}_q = GF(q)$ with q elements. For a general, not necessarily linear, code C, the notation $(n, M = |C|, d)_q$ is commonly used.

A linear $[n, k, d]_q$-code C is said to be *cyclic* if C is invariant under the cyclic shift. That is, whenever $\mathbf{v} = (v_0, v_1, \ldots, v_{n-2}, v_{n-1}) \in C$, we have

$$\mathbf{v}' = (v_{n-1}, v_0, v_1 \cdots, v_{n-2}) \in C.$$

Let n be a positive integer and let $1 \leq l < n$ be a divisor of n. A linear $[n, k, d]_q$-code C is *quasi-cyclic of index l* or *l-quasi-cyclic* if

$$\mathbf{v}'' = (v_{n-l}, v_{n-l+1}, \ldots, v_{n-1}, v_0, v_1, \ldots, v_{n-l-1}) \in C$$

whenever $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1}) \in C$. In particular, a 1-quasi-cyclic code is a cyclic code.

As is the case for linear codes, we define the notions of an *additive cyclic code* and an *additive quasi-cyclic code* similarly by requiring the code to be additive, instead of linear.

The *Hamming weight* of a vector or a codeword $\mathbf{v}$ in a code C, denoted by $\mathrm{wt}_H(\mathbf{v})$, is the number of its nonzero entries. Given two elements $\mathbf{u}, \mathbf{v} \in C$, the number of positions where their respective entries disagree, written as $\mathrm{dist}_H(\mathbf{u}, \mathbf{v})$, is called the *Hamming distance* of $\mathbf{u}$ and $\mathbf{v}$. For any code C, the *minimum distance* $d = d(C)$ is given by $d = d(C) = \min\{\mathrm{dist}_H(\mathbf{u}, \mathbf{v}) : \mathbf{u}, \mathbf{v} \in C, \mathbf{u} \neq \mathbf{v}\}$. If C is additive, then its additive closure property implies that $d(C)$ is given by the minimum Hamming weight of the nonzero vectors in C.

Definition 1. Let $\mathbb{F}_4 := \{0, 1, \omega, \omega^2 = \overline{\omega}\}$. For $x \in \mathbb{F}_4$, set $\overline{x} = x^2$, the conjugate of x. Let n be a positive integer and $\mathbf{u} = (u_0, u_1, \ldots, u_{n-1}), \mathbf{v} = (v_0, v_1, \ldots, v_{n-1}) \in \mathbb{F}_4^n$.

1. 4^{H} is the family of $\mathbb{F}_4$-linear codes of length n equipped with the *Hermitian inner product*

$$\langle \mathbf{u}, \mathbf{v} \rangle_{\mathrm{H}} := \sum_{i=0}^{n-1} u_i \cdot v_i^2. \tag{1}$$

2. $4^{\mathrm{H}+}$ is the family of $\mathbb{F}_2$-linear codes over $\mathbb{F}_4$ of length n equipped with the *trace Hermitian inner product*

$$\langle \mathbf{u}, \mathbf{v} \rangle_{\mathrm{tr}} := \sum_{i=0}^{n-1} (u_i \cdot v_i^2 + u_i^2 \cdot v_i). \tag{2}$$

Definition 2. A code C of length n over $\mathbb{F}_4$ is said to be an additive $\mathbb{F}_4$-code if C belongs to the family $4^{\mathrm{H}+}$.

Let C be a code. Under a chosen inner product $*$, the *dual code* $C^{\perp_*}$ of C is given by

$$C^{\perp_*} := \left\{ \mathbf{u} \in \mathbb{F}_q^n : \langle \mathbf{u}, \mathbf{v} \rangle_* = 0 \text{ for all } \mathbf{v} \in C \right\}.$$

A code is said to be *self-orthogonal* if it is contained in its dual and is said to be *self-dual* if its dual is itself. We say that a family of codes is *closed* if $(C^{\perp_*})^{\perp_*} = C$ for each C in that family. It has been established [14, Ch. 3] that both families of codes in Definition 1 are closed.

The weight distribution of a code and that of its dual are important in the studies of their properties.

Definition 3. The *weight enumerator* $W_C(X, Y)$ of an $(n, M = |C|, d)_q$-code C is the polynomial

$$W_C(X, Y) = \sum_{i=0}^{n} A_i X^{n-i} Y^i, \tag{3}$$

where A_i is the number of codewords of weight i in the code C.

The weight enumerator of the Hermitian dual code $C^{\perp_{\mathrm{H}}}$ of an $[n, k, d]_4$-code C is connected to the weight enumerator of the code C via the *MacWilliams Equation*

$$W_{C^{\perp_{\mathrm{H}}}}(X, Y) = \frac{1}{|C|} W_C(X + 3Y, X - Y). \tag{4}$$

From [14, Sec. 2.3] we know that the family $4^{\mathrm{H}+}$ has the same MacWilliams Equation as does the family 4^{H}. Thus,

$$W_{C^{\perp_{\mathrm{tr}}}}(X, Y) = \frac{1}{|C|} W_C(X + 3Y, X - Y). \tag{5}$$

3. The mapping S on codes over $\mathbb{F}_4$

Codes belonging to the family $4^{\mathrm{H}+}$ have been studied primarily in connection to designs (e.g. [11]) and to stabilizer quantum codes (e.g. [10, Sec. 9.10]). It is well known that if C is an additive $(n, 2^k)_4$-code, then $C^{\perp_{\mathrm{tr}}}$ is an additive $(n, 2^{2n-k})_4$-code.

Note that if the code C is $\mathbb{F}_4$-linear with parameters $[n, k, d]_4$, then $C^{\perp_{\mathrm{H}}} = C^{\perp_{\mathrm{tr}}}$. This is because $C^{\perp_{\mathrm{H}}} \subseteq C^{\perp_{\mathrm{tr}}}$ and $C^{\perp_{\mathrm{H}}}$ is of size $4^{n-k} = 2^{2n-2k}$ which is also the size of $C^{\perp_{\mathrm{tr}}}$.

We are now ready to introduce the mapping S in aid of later constructions.

Definition 4. In $\mathbb{F}_4^n$, define the mapping

$$\begin{aligned} S: \quad & \mathbb{F}_4^n \to \mathbb{F}_4^{2n} \\ & (v_0, v_1, \ldots, v_{n-1}) \mapsto (v_0, \overline{v_0}, v_1, \overline{v_1}, \ldots, v_{n-1}, \overline{v_{n-1}}). \end{aligned} \tag{6}$$

It is immediately clear from the definition that S is an $\mathbb{F}_2$-linear map, injective but not surjective.

Example 1. The mapping S is not $\mathbb{F}_4$-linear. Consider $n = 2$ and $\mathbf{u} = (\omega, \overline{\omega})$. We have

$$\begin{aligned} S(\mathbf{u}) &= (\omega, \overline{\omega}, \overline{\omega}, \omega), \\ S(w \cdot \mathbf{u}) &= S((\overline{\omega}, 1)) = (\overline{\omega}, \omega, 1, 1) \\ &\neq \omega \cdot S(\mathbf{u}) = (\overline{\omega}, 1, 1, \overline{\omega}). \end{aligned}$$

Lemma 1. *Let C be an $(n, M, d)_4$-code. For all $\mathbf{u} \in C$ we have*

$$\begin{aligned} \mathrm{wt}_H(S(\mathbf{u})) &= 2\mathrm{wt}_H(\mathbf{u}) \quad \textit{and} \\ d(S(C)) &= 2d(C). \end{aligned}$$

Proof. For all $u \in \mathbb{F}_4$, $S(u) = (u, \overline{u})$. Now, $\overline{u} = 0$ if and only if $u = 0$. □

The mapping S is therefore a scaled isometry for the Hamming metric that preserves the code size. It sends an additive $(n, M, d)_4$-code C to an additive code $S(C)$ with parameters $(2n, M, 2d)_4$.

Lemma 2. *If C is an additive $(n, M, d)_4$-cyclic code then $S(C)$ is an additive $(2n, M, 2d)_4$-2-quasi-cyclic code.*

Proof. Since C is cyclic,

$$\mathbf{v} = (v_0, \ldots, v_{n-2}, v_{n-1}) \in C \textit{ if and only if } \mathbf{v}' = (v_{n-1}, v_0, \ldots, v_{n-2}) \in C.$$

Applying S yields

$$\begin{aligned} S(\mathbf{v}) &= (v_0, \overline{v_0}, \ldots, v_{n-2}, \overline{v_{n-2}}, v_{n-1}, \overline{v_{n-1}}) \in S(C), \\ S(\mathbf{v}') &= (v_{n-1}, \overline{v_{n-1}}, v_0, \overline{v_0}, \ldots, v_{n-2}, \overline{v_{n-2}}) \in S(C). \end{aligned}$$

By definition, $S(C)$ is an additive 2-quasi-cyclic code. □

Proposition 1. *Given an additive $(n, M, d)_4$-code C, $S(C) \subseteq S(C)^{\perp_{\mathrm{tr}}}$.*

Proof. Let $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1}), \mathbf{u} = (u_0, u_1, \ldots, u_{n-1}) \in C$. Then

$$\langle S(\mathbf{v}), S(\mathbf{u}) \rangle_{\mathrm{tr}} = \sum_{i=0}^{n-1} (v_i \overline{u_i} + \overline{v_i} u_i) + \sum_{i=0}^{n-1} (\overline{v_i} u_i + v_i \overline{u_i}) = 2 \sum_{i=0}^{n-1} (v_i \overline{u_i} + \overline{v_i} u_i) = 0.$$

□

4. Module θ-cyclic codes over $\mathbb{F}_4$

The motivation for our definition of *module θ-cyclic codes* comes from [2] and [3]. Given $\mathbb{F}_q$ and an automorphism θ of $\mathbb{F}_q$, we can define a ring structure on the set

$$\mathcal{R} = \mathbb{F}_q[X, \theta] = \{a_n X^n + \ldots + a_1 X + a_0 | a_i \in \mathbb{F}_q \text{ and } n \in \mathbb{N}\}.$$

In $\mathcal{R}$, the addition operation is the usual polynomial addition and the multiplication is defined by the extension to all elements of $\mathcal{R}$, by associativity and distributivity, the basic rule $Xa = \theta(a)X$ for all $a \in \mathbb{F}_q$.

The ring $\mathcal{R}$ is a left and right Euclidean ring whose left and right ideals are principal. Right division means that for nonzero $f(X), g(X) \in \mathcal{R}$, there exist unique polynomials $Q_r(X), R_r(X) \in \mathcal{R}$ such that

$$f(X) = Q_r(X) \cdot g(X) + R_r(X)$$

with $deg(R_r(X)) < deg(g(X))$ or $R_r(X) = 0$. If $R_r(X) = 0$, then $g(X)$ is a *right divisor* of $f(X)$ in $\mathcal{R}$.

Definition 5. [3, cf. Defs. 1 and 3] Let θ be an automorphism of $\mathbb{F}_q$. Let $f(X) \in \mathcal{R}$ be of degree n. If $I = (f(X))$ is a two-sided ideal of $\mathcal{R}$, then an *ideal θ-code* C is a left ideal $\mathcal{R}g(X)/\mathcal{R}f(X) \subset \mathcal{R}/\mathcal{R}f(X)$ where $g(X)$ is a right divisor of $f(X)$ in $\mathcal{R}$. If $f(X) = X^n - 1$, we call the ideal θ-code corresponding to the left ideal $\mathcal{R}g(X)/\mathcal{R}(X^n - 1) \subset \mathcal{R}/\mathcal{R}(X^n - 1)$ an *ideal θ-cyclic code*.

A *module θ-code* C is a left $\mathcal{R}$-submodule $\mathcal{R}g(X)/\mathcal{R}f(X) \subset \mathcal{R}/\mathcal{R}f(X)$ where $g(X)$ is a right divisor of $f(X)$ in $\mathcal{R}$. Furthermore,

1. if $f(X) = X^n - c$, with $c \in \mathbb{F}_q$, we call the module θ-code corresponding to the left $\mathcal{R}$-module $\mathcal{R}g(X)/\mathcal{R}f(X) \subset \mathcal{R}/\mathcal{R}f(X)$ a *module θ-constacyclic code*;
2. if $f(X) = X^n - 1$, we call the module θ-code corresponding to the left $\mathcal{R}$-module $\mathcal{R}g(X)/\mathcal{R}f(X) \subset \mathcal{R}/\mathcal{R}f(X)$ a *module θ-cyclic code*.

The length of the module θ-code C is $n = deg(f(X))$ and its dimension is $k = deg(f(X)) - deg(g(X))$. If the minimum distance of C is d, the code C is said to be of type $[n, k, d]_q$.

If the codewords of C are identified with the list of the coefficients of the remainder of a right division by $f(X)$ in $\mathcal{R}$, then the elements of $\mathcal{R}g(X)/\mathcal{R}f(X)$ are all of the left multiples of $g(X) = g_r X^r + \ldots + g_1 X + g_0$.

Thus, a generator matrix G of the corresponding module θ-code of length $n = deg(f(X))$ is given by

$$G = \begin{pmatrix} g_0 & g_1 & \ldots & g_{r-1} & g_r & 0 & \ldots & 0 \\ 0 & \theta(g_0) & \theta(g_1) & \ldots & \theta(g_{r-1}) & \theta(g_r) & \ldots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 & \theta^{n-r-1}(g_0) & \ldots & \theta^{n-r-1}(g_{r-1}) & \theta^{n-r-1}(g_r) \end{pmatrix} \tag{7}$$

depending only on $g(X)$ and n.

Theorem 1. *A module θ-cyclic code C_θ has the following property*

$$(v_0, v_1, \ldots, v_{n-2}, v_{n-1}) \in C_\theta \Rightarrow (\theta(v_{n-1}), \theta(v_0), \theta(v_1), \ldots, \theta(v_{n-2})) \in C_\theta. \tag{8}$$

Proof. The proof of this property for an ideal θ-cyclic code C is established in [2, Theorem 1]. The same proof works when we replace ideal by module. □

Since a module θ-cyclic code C_θ has a representation in the skew polynomial ring $\mathcal{R} = \mathbb{F}_q[X, \theta]$ (see [3]), when θ is fixed, we call C_θ a *skew-cyclic code*.

We consider, for the rest of the paper, the Frobenius automorphism defined in $\mathbb{F}_4$ by $\theta(x) = x^2 = \overline{x}$ for $x \in \mathbb{F}_4$. Let $[2n]$ denote the set $\{1, 2, \ldots, 2n\}$. Let $\sigma = \tau \circ T^2$ be a permutation on $[2n]$ where T is the cyclic shift module $2n$ and $\tau = (12)(34)\ldots(2n-1, 2n)$. Since T^2 and τ commute, σ can be written as $T^2 \circ \tau$ as well. We denote the identity permutation by (1).

Let Σ be the permutation on elements of $\mathbb{F}_4^{2n}$ induced by σ. That is, for $\mathbf{v} = (v_1, v_2, \ldots, v_{2n}) \in \mathbb{F}_4^{2n}$,

$$\Sigma(\mathbf{v}) = \left(v_{\sigma(1)}, v_{\sigma(2)}, \ldots, v_{\sigma(2n)}\right). \tag{9}$$

Lemma 3. *Given an $(n, M, d)_4$-skew-cyclic code C_θ, the code $S(C_\theta)$ is invariant under Σ.*

Proof. Let $\mathbf{v} = (v_1, v_2, \ldots, v_{2n}) \in S(C_\theta)$. That is, there exists $\mathbf{u} = (u_1, u_2, \ldots, u_n) \in C_\theta$ such that

$$\mathbf{v} = (u_1, \overline{u_1}, u_2, \overline{u_2}, \ldots, u_n, \overline{u_n}) = S(\mathbf{u}).$$

Since C_θ is a skew-cyclic code, we have

$$\overline{\mathbf{u}} := (\overline{u_n}, \overline{u_1}, \ldots, \overline{u_{n-1}}) \in C_\theta.$$

Hence,

$$\begin{aligned}\Sigma(\mathbf{v}) &= (\overline{u_n}, u_n, \overline{u_1}, u_1, \ldots, \overline{u_{n-1}}, u_{n-1}) \\ &= S((\overline{u_n}, \overline{u_1}, \ldots, \overline{u_{n-1}})),\end{aligned}$$

implying $\Sigma(S(C_\theta)) \subset S(C_\theta)$. □

Lemma 4. *The order of σ is $2n$ if n is odd and n if n is even.*

Proof. For $1 \leq i \leq 2n$, σ follows the following rule

$$\sigma : i \mapsto \begin{cases} i+3 \pmod{2n} \text{ if } i \text{ is odd} \\ i+1 \pmod{2n} \text{ if } i \text{ is even} \end{cases}. \tag{10}$$

With computation done modulo $2n$, observe that if i is odd, then $\sigma(i) = i+3$ and $\sigma^2(i) = \sigma(i+3) = i+4$. If i is even, then $\sigma(i) = i+1$ and $\sigma^2(i) = \sigma(i+1) = i+4$. Hence, $\sigma^2 = T^4$.

Now, let $n = 2l$ for some positive integer l. We have

$$\sigma^n = \sigma^{2l} = T^{4l} = T^{2n} = (1),$$

the identity permutation. For $1 \leq k < n$, if $k = 2i$, then

$$\sigma^k = \sigma^{2i} = T^{4i} \neq (1)$$

since $4i = 2k < 2n$. If $k = 2i+1$,

$$\sigma^k = \sigma^{2i+1} = T^{4i} \circ \tau \neq (1)$$

since σ^k sends 1 to $4i+1 \neq 1$. Consequently, the order of σ is n.

In the case where $n = 2l+1$, we have

$$\sigma^{2n} = (T^{2n})^2 = (1).$$

To show minimality, we first note that $\sigma^n = \tau$ since

$$\sigma^n = \sigma^{2l+1} = T^{4l} \circ \sigma = T^{2n-2} \circ (\tau \circ T^2) = T^{2n-2} \circ (T^2 \circ \tau) = \tau.$$

Consider the following two subcases. For $1 \leq k < n$, the same argument as in the even case above shows that $\sigma^k \neq (1)$. For $n+1 \leq k < 2n$,

$$\sigma^k = \sigma^n \circ \sigma^{k-n} = \tau \circ \sigma^{k-n} \neq (1).$$

We conclude that the order of σ is $2n$. □

For conciseness, we adopt the following expressions following Lemma 4.

1. For n odd, σ is the following cycle of length $2n$

$$\sigma = (1, \sigma(1), \sigma^2(1), \ldots, \sigma^{2n-2}(1), \sigma^{2n-1}(1)). \tag{11}$$

2. Since $\sigma^k(1) \neq 2$ for all $0 \leq k \leq n-1$, for n even, σ can be written as the following product of two cycles, each of length n

$$\sigma = (1, \sigma(1), \sigma^2(1), \ldots, \sigma^{n-1}(1))(2, \sigma(2), \sigma^2(2), \ldots, \sigma^{n-1}(2)). \tag{12}$$

When it is clear from the context, we write C instead of C_θ.

Theorem 2. *Let C be an $[n, k, d]_4$-skew-cyclic code. If n is odd then $S(C)$ is equivalent to an additive $(2n, 2^{2k}, 2d)_4$-cyclic code C'. If n is even then $S(C)$ is equivalent to an additive $(2n, 2^{2k}, 2d)_4$-2-quasi-cyclic code C'.*

Proof. Recall that the permutation σ on $[2n]$ induces a permutation Σ on the vectors of $\mathbb{F}_4^{2n}$. Consider first the case n odd where Equation (11) holds. Define the permutation σ' by

$$\sigma' = \begin{pmatrix} 1 & 2 & \ldots & 2n-1 & 2n \\ \sigma^{2n-1}(1) & \sigma^{2n-2}(1) & \ldots & \sigma(1) & 1 \end{pmatrix}. \tag{13}$$

It is clear that for all $1 \leq j \leq 2n$,

$$\sigma'(j) = \sigma^{2n-j}(1). \tag{14}$$

The permutation σ' induces a permutation Σ' acting on the elements of $\mathbb{F}_4^{2n}$. For $\mathbf{v} = (v_1, v_2, \ldots, v_{2n}) \in \mathbb{F}_4^{2n}$,

$$\Sigma'(\mathbf{v}) = \left(v_{\sigma'(1)}, v_{\sigma'(2)}, \ldots, v_{\sigma'(2n)}\right). \tag{15}$$

To show that $\Sigma'(S(C))$ is cyclic we must prove that for all codewords $\mathbf{v} \in S(C)$, $T(\Sigma'(\mathbf{v})) \in \Sigma'(S(C))$ where T is the vector cyclic shift. Since $\Sigma(S(C)) = S(C)$ by Lemma 3, we only need to show that

$$T(\Sigma'(\mathbf{v})) = \Sigma'(\Sigma(\mathbf{v})). \tag{16}$$

Let us start from the right hand side. By definition,

$$\Sigma(\mathbf{v}) = \left(v_{\sigma(1)}, v_{\sigma(2)}, \ldots, v_{\sigma(2n)}\right) := (v'_1, v'_2, \ldots, v'_{2n}) = \mathbf{v}'. \tag{17}$$

From Equation (14), we know that

$$\Sigma'(\Sigma(\mathbf{v})) = \left(v'_{\sigma'(1)}, v'_{\sigma'(2)}, \ldots, v'_{\sigma'(2n)}\right) = \left(v'_{\sigma^{2n-1}(1)}, v'_{\sigma^{2n-2}(1)}, \ldots, v'_{\sigma^1(1)}, v'_{\sigma^0(1)}\right).$$

By Equation (17),

$$\Sigma'(\Sigma(\mathbf{v})) = \left(v_1, v_{\sigma^{2n-1}(1)}, \ldots, v_{\sigma^2(1)}, v_{\sigma(1)}\right). \tag{18}$$

Moving on to the left hand side. Equation (14) implies

$$\Sigma'(\mathbf{v}) = \left(v_{\sigma'(1)}, v_{\sigma'(2)}, \ldots, v_{\sigma'(2n)}\right) = \left(v_{\sigma^{2n-1}(1)}, v_{\sigma^{2n-2}(1)}, \ldots, v_{\sigma(1)}, v_1\right).$$

Applying the vector cyclic shift T on $\Sigma'(\mathbf{v})$ completes the proof of this case.

For n even, Equation (12) holds. Let the permutation σ'' be given by

$$\sigma'' = \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots & 2n-1 & 2n \\ \sigma^{n-1}(1) & \sigma^{n-1}(2) & \sigma^{n-2}(1) & \sigma^{n-2}(2) & \ldots & \sigma^0(1) & \sigma^0(2) \end{pmatrix}. \tag{19}$$

Let b be an integer such that $1 \leq b \leq n$. For all $1 \leq j \leq 2n$,

$$\sigma''(j) = \begin{cases} \sigma^{n-b}(1) \text{ if } j = 2b-1 \\ \sigma^{n-b}(2) \text{ if } j = 2b \end{cases}. \tag{20}$$

Let Σ'' be the permutation on vectors in $\mathbb{F}_4^{2n}$ induced by σ''. Applying Σ'' and by Equation (17), we have

$$\begin{aligned}\Sigma''(\Sigma(\mathbf{v})) &= \left(v'_{\sigma''(1)}, v'_{\sigma''(2)}, v'_{\sigma''(3)}, v'_{\sigma''(4)}, \ldots, v'_{\sigma''(2n-1)}, v'_{\sigma''(2n)}\right)\\ &= \left(v'_{\sigma^{n-1}(1)}, v'_{\sigma^{n-1}(2)}, v'_{\sigma^{n-2}(1)}, v'_{\sigma^{n-2}(2)}, \ldots, v'_{\sigma(1)}, v'_{\sigma(2)}, v'_1, v'_2\right)\end{aligned}$$

by Equation (20). Now, Equation(17) allows us to write

$$\Sigma''(\Sigma(\mathbf{v})) = \left(v_1, v_2, v_{\sigma^{n-1}(1)}, v_{\sigma^{n-1}(2)}, \ldots, v_{\sigma^2(1)}, v_{\sigma^2(2)}, v_{\sigma(1)}, v_{\sigma(2)}\right).$$

Since

$$\begin{aligned}\Sigma''(\mathbf{v}) &= \left(v_{\sigma''(1)}, v_{\sigma''(2)}, v_{\sigma''(3)}, v_{\sigma''(4)}, \ldots, v_{\sigma''(2n-3)}, v_{\sigma''(2n-2)}, v_{\sigma''(2n-1)}, v_{\sigma''(2n)}\right)\\ &= \left(v_{\sigma^{n-1}(1)}, v_{\sigma^{n-1}(2)}, v_{\sigma^{n-2}(1)}, v_{\sigma^{n-2}(2)}, \ldots, v_{\sigma(1)}, v_{\sigma(2)}, v_1, v_2\right)\end{aligned}$$

and $\Sigma(S(C)) = S(C)$, we get

$$T^2(\Sigma''(\mathbf{v})) = \Sigma''(\Sigma(\mathbf{v})) \in \Sigma''(S(C)).$$

Thus, $\Sigma''(S(C))$ is a 2-quasi-cyclic code. This completes the entire proof. □

Example 2. For $n = 4$, we have

$$\begin{aligned}\sigma &= (1,4,5,8)(2,3,6,7) \text{ and}\\ \sigma'' &= (1,8,2,7)(3,5,4,6).\end{aligned}$$

Following [2, Example 2], let C be a $[4,2,3]_4$-skew-cyclic code with generator matrix

$$G = \begin{pmatrix} 1 & 0 & \overline{\omega} & \omega \\ 0 & 1 & \omega & \overline{\omega} \end{pmatrix}. \tag{21}$$

Verifying that $S(C)$ is invariant under Σ is immediate.

Choose $\mathbf{u} = (1,0,\overline{\omega},\omega) \in C$. Let $\mathbf{v} = S(\mathbf{u}) = (1,1,0,0,\overline{\omega},\omega,\omega,\overline{\omega})$. Then

$$\begin{aligned}\Sigma''(\Sigma(\mathbf{v})) &= \left(v_{\sigma^4(1)}, v_{\sigma^4(2)}, v_{\sigma^3(1)}, v_{\sigma^3(2)}, v_{\sigma^2(1)}, v_{\sigma^2(2)}, v_{\sigma(1)}, v_{\sigma(2)}\right)\\ &= (v_1, v_2, v_8, v_7, v_5, v_6, v_4, v_3) = (1,1,\overline{\omega},\omega,\overline{\omega},\omega,0,0), \text{ while}\\ \Sigma''(\mathbf{v}) &= \left(v_{\sigma^3(1)}, v_{\sigma^3(2)}, v_{\sigma^2(1)}, v_{\sigma^2(2)}, v_{\sigma(1)}, v_{\sigma(2)}, v_1, v_2\right)\\ &= (v_8, v_7, v_5, v_6, v_4, v_3, v_1, v_2) = (\overline{\omega},\omega,\overline{\omega},\omega,0,0,1,1).\end{aligned}$$

Explicit computation up to length $n = 21$ shows that the only examples of module θ-cyclic codes of odd lengths are the usual cyclic codes.

Example 3. For $n = 7$, we have

$$\begin{aligned}\sigma &= (1,4,5,8,9,12,13,2,3,6,7,10,11,14) \text{ and}\\ \sigma' &= (1,14)(2,11,8,13,4,7)(3,10,9,12,5,6).\end{aligned}$$

Let C be a $[7,4,3]_4$-skew-cyclic code with generator matrix

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}. \tag{22}$$

Let $\mathbf{v} = (1,1,1,1,0,0,1,1,0,0,0,0,0,0)$. Then

$$\begin{aligned}\Sigma'(\Sigma(\mathbf{v})) &= (v_1, v_{14}, v_{11}, v_{10}, v_7, v_6, v_3, v_2, v_{13}, v_{12}, v_9, v_8, v_5, v_4)\\ &= (1,0,0,0,1,0,1,1,0,0,0,1,0,1), \text{ while}\\ \Sigma'(\mathbf{v}) &= \left(v_{\sigma^{13}(1)}, v_{\sigma^{12}(1)}, v_{\sigma^{11}(1)}, v_{\sigma^{10}(1)}, \ldots, v_{\sigma(1)}, v_1\right)\\ &= (v_{14}, v_{11}, v_{10}, v_7, v_6, v_3, v_2, v_{13}, v_{12}, v_9, v_8, v_5, v_4, v_1)\\ &= (0,0,0,1,0,1,1,0,0,0,1,0,1,1).\end{aligned}$$

Theorem 2, our main result in this section, reveals the structural connection between skew-cyclic codes under the mapping S and additive cyclic or additive 2-quasi-cyclic codes, depending on the parity of the length. Combined with the orthogonality property that the mapping S induces, we can further make a connection to asymmetric quantum codes.

5. Asymmetric quantum codes

For brevity, it is assumed that the reader is familiar with the standard error model in quantum error-correction, both symmetric and asymmetric. For references on the motivation and previous constructions of asymmetric quantum codes, [16] and [17] can be consulted.

Definition 6. Let d_x and d_z be positive integers. A quantum code Q in $V_n = \mathbb{C}^{q^n}$ with dimension $K \geq 2$ is called an *asymmetric quantum code* with parameters $((n, K, d_z/d_x))_q$ or $[[n, k, d_z/d_x]]_q$, where $k = \log_q K$, if Q detects $d_x - 1$ quantum digits of X-errors and, at the same time, $d_z - 1$ quantum digits of Z-errors.

The following result has been shown recently in [6].

Theorem 3. [6, Th. 4.5] *Let $q = r^2$ be an even power of a prime p. For $i = 1, 2$, let C_i be a classical additive code with parameters $(n, K_i, d_i)_q$. If $C_1^{\perp_{\mathrm{tr}}} \subseteq C_2$, then there exists an asymmetric quantum code Q with parameters $((n, \frac{|C_2|}{|C_1^{\perp_{\mathrm{tr}}}|}, d_z/d_x))_q$ where $\{d_z, d_x\} = \{d_1, d_2\}$.*

As explained in [2] and in [3], there are two major gains of using module θ-codes. First, there is more flexibility and generality in constructing (linear) codes without increasing the complexity of the encoding and decoding process. The notion of *q-cyclic codes*, introduced in [8], for instance, covers ideal θ-cyclic codes with θ limited to the Frobenius automorphism only.

More important to the agenda of constructing asymmetric quantum codes is the second gain, which is the minimum distance improvement. Exhaustive search on module θ-codes up to certain length has yielded linear codes with better parameters. More systematically, the BCH approach of constructing codes with a prescribed lower bound on the minimum distance can be extended to module θ-codes as well. Section 3 of [3] contains the construction details. The resulting improvements have been added to the database of *best-known linear codes* (BKLC) of MAGMA [1].

For the remaining of the paper, we will concentrate on constructing asymmetric quantum codes with $d_z \geq d_x = 2$ based on Theorem 3. We will see how the mapping S can be used as an aid in construction. All computations are done in MAGMA V2.16-5.

6. Analysis on the weight enumerators

In this section, the weight enumerators of $S(C)$ and of $S(C)^{\perp_{\mathrm{tr}}}$ are analyzed. This analysis will be useful in determining d_x.

Let A_i be the number of codewords of weight i in an additive $(n, M, d)_4$-code C. Then the weight enumerators of $S(C)$ and $S(C)^{\perp_{\mathrm{tr}}}$ can be written in terms of the weight enumerator of C with the help of Equation (5)

$$W_{S(C)}(X,Y) = \sum_{i=0}^{n} A_i X^{2(n-i)} Y^{2i}, \tag{23}$$

$$W_{S(C)^{\perp_{\mathrm{tr}}}}(X,Y) = \frac{1}{|S(C)|} W_{S(C)}(X+3Y, X-Y). \tag{24}$$

More explicitly,

$$W_{S(C)^{\perp_{\mathrm{tr}}}}(X,Y) = \frac{1}{M} \sum_{i=0}^{n} A_i L_i, \tag{25}$$

where L_i is given by

$$\left(\sum_{j=0}^{n-i} \binom{n-i}{j} X^{n-i-j} (3Y)^j \right)^2 \left(\sum_{l=0}^{i} \binom{i}{l} X^{i-l} (-Y)^l \right)^2. \tag{26}$$

Denote the number of codewords of weight i in the code $C^{\perp_{\mathrm{tr}}}$ by $A_i^{\perp_{\mathrm{tr}}}$. By using the *Pless power moments* with $q = 4$ (see [10, p. 259] for the linear version), we have

$$\sum_{i=0}^{n} A_i = |C| = M, \tag{27}$$

$$\sum_{i=0}^{n} i A_i = \frac{M}{4}(3n - A_1^{\perp_{\mathrm{tr}}}), \tag{28}$$

$$\sum_{i=0}^{n} i^2 A_i = \frac{M}{4^2} \left\{ (9n^2 + 3n) - (6n-2) A_1^{\perp_{\mathrm{tr}}} + 2 A_2^{\perp_{\mathrm{tr}}} \right\}. \tag{29}$$

If we further assume that $A_1^{\perp_{\mathrm{tr}}} = A_2^{\perp_{\mathrm{tr}}} = 0$, then the following statements hold for Equation (24).

1. The coefficient of $Y^0 X^{2n}$ is $\frac{1}{M} \sum_{i=0}^{n} A_i = 1$.
2. The coefficient of $Y X^{2n-1}$ is

$$\begin{aligned} &\frac{1}{M} \sum_{i=0}^{n} A_i \left(2 \cdot (n-i) \cdot 3 - 2i\right) \\ &= \frac{1}{M} \sum_{i=0}^{n} A_i (6n - 8i) = 6n - 4^{-1} \cdot 8(3n) = 0 \end{aligned}$$

by Equation (28).

3. The coefficient of Y^2X^{2n-2} is

$$\begin{aligned}&\frac{1}{M}\sum_{i=0}^{n} A_i\left(18n^2-48ni+32i^2-9n+8i\right)\\&=\frac{18n^2-9n}{M}\sum_{i=0}^{n}A_i+\frac{8-48n}{M}\sum_{i=0}^{n}iA_i+\frac{32}{M}\sum_{i=0}^{n}i^2A_i\\&=3n\end{aligned}$$

by Equations (28) and (29).

If we rewrite

$$W_{S(C)^{\perp_{\mathrm{tr}}}}(X,Y)=\sum_{i=0}^{2n}B_iX^{2n-i}Y^i, \tag{30}$$

then $B_0=1, B_1=0$, and $B_2=3n$. This is true for any additive $(n,M,d)_4$-code C with $d(C^{\perp_{\mathrm{tr}}})\geq 3$. If $d(C^{\perp_{\mathrm{tr}}})=1$, then $B_1=2A_1^{\perp_{\mathrm{tr}}}>0$. If $d(C^{\perp_{\mathrm{tr}}})=2$, then $B_1=0$ and $B_2=3n+4A_2^{\perp_{\mathrm{tr}}}>0$.

As a direct consequence of Proposition 1 and the above analysis on the weight enumerators, we derive the following result.

Proposition 2. *Given any additive $(n,M,d)_4$-code C such that $d(C^{\perp_{\mathrm{tr}}})\geq 2$, there exists an asymmetric quantum code Q with parameters $[[2n,\log_4\left(\frac{|S(C)^{\perp_{\mathrm{tr}}}|}{|S(C)|}\right),2/2]]_4$.*

Proof. By Proposition 1, $S(C)\subseteq S(C)^{\perp_{\mathrm{tr}}}$. Apply Theorem 3 by taking $C_1=C_2=S(C)^{\perp_{\mathrm{tr}}}$. The values $d_z=d_x=2$ follow from the analysis on the weight enumerators. □

The parameters of the resulting code Q based on the construction in Proposition 2 are not so good. Fortunately, the mapping S preserves nestedness. This fact can be used to derive asymmetric quantum codes with better parameters.

Theorem 4. *Let C be an additive $(n,M_1,d_1)_4$-code such that $d(C^{\perp_{\mathrm{tr}}})\geq 2$. Let D be an additive $(n,M_2,d_2)_4$-code satisfying $C\subseteq D$. Then there exists an asymmetric quantum code Q with parameters $[[2n,\log_4\left(\frac{M_2}{M_1}\right),2d_2/2]]_4$.*

Proof. Apply Theorem 3 by taking $C_1=S(C)^{\perp_{\mathrm{tr}}}$ and $C_2=S(D)$. The code $S(C)$ is an additive $(2n,M_1,2d_1)_4$-code. Similarly, $S(D)$ is an additive code of parameters $(2n,M_2,2d_2)_4$. The values for d_z and d_x follow from the discussion on the weight enumerators above. □

Example 4. Let $C=D$ be the $[n,1,n]_4$-repetition code generated by the all one vector $\mathbf{1}=(1,\ldots,1)$. It can be directly verified that $d(C^{\perp_{\mathrm{tr}}})=2$. Hence, we get an asymmetric quantum code Q with parameters $[[\mathbf{2n},\mathbf{0},\mathbf{2n/2}]]_{\mathbf{4}}$ by Theorem 4. This code Q satisfies the equality of the quantum version of the Singleton bound $k\leq n-d_x-d_z+2$.

Henceforth, any asymmetric quantum code Q satisfying $k=n-d_x-d_z+2$ is printed in boldface. We call such a code an *asymmetric quantum MDS code*.

Example 5. Consider the $[4,2,3]_4$-module θ-cyclic code D with generator matrix G in Equation(21) above. The code D contains the $[4,1,4]_4$-repetition code C generated by $\mathbf{1}$. Applying Theorem 3 with $C=C_1^{\perp_{\mathrm{tr}}}$ and $D=C_2$ results in a

$[[\mathbf{4},\mathbf{1},\mathbf{3/2}]]_\mathbf{4}$-asymmetric quantum code. Under the mapping S, by Theorem 4, we arrive at an $[[8,1,6/2]]_4$-asymmetric quantum code.

The investigation on self-dual module θ-code yields new Hermitian self-dual linear $\mathbb{F}_4$-codes with parameters $[50,25,14]_4$ and $[58,29,16]_4$. These codes are listed down in [3, Table 3]. They can be used to derive asymmetric quantum codes Q with parameters $[[50,0,14/14]]_4$ and $[[58,0,16/16]]_4$ following [6, Th. 7.1]. The latter code improves on the $[[58,0,14/14]]_4$-code in [6, Table III].

The next section presents two systematic constructions of asymmetric quantum codes with $d_z \geq d_x = 2$ by using the database of BKLC and by applying the mapping S on concatenated Reed-Solomon codes, respectively.

7. Two constructions

Under the mapping S, Theorem 4 says that while we cannot improve on $d_x = 2$, we can relax the condition on the inner code C to possibly improve on the size of Q as well as on d_z. Our aim, then, is to choose the smallest possible subcode C of D such that $d(C^{\perp_{\mathrm{tr}}}) \geq 2$ while keeping the size and the minimum distance of D relatively large.

Note that there is no additive $(n,2,d)_4$-code with $d(C^{\perp_{\mathrm{tr}}}) \geq 2$. The smallest additive code with $d(C^{\perp_{\mathrm{tr}}}) = 2$ is an $(n,4,n)_4 = [n,1,n]_4$-code C consisting of the scalar multiples of a codeword $\mathbf{v}$ of weight n. Since this code C is MDS, its dual $C^{\perp_{\mathrm{tr}}} = C^{\perp_{\mathrm{H}}}$ is of parameters $[n,n-1,2]_4$.

7.1. Construction from best-known linear codes (BKLC). Let n,k be fixed with $2 \leq k \leq n-1$. The strategy here is to consider the best-known linear code D of length n and dimension k stored in the MAGMA database and check if the code contains codewords of weight n and put them in a set R. If R is non-empty, we choose an arbitrary codeword $\mathbf{v} \in R$ and construct a subcode $C \subset D$ of parameters $[n,1,n]_4$ whose elements are the four scalar multiples of $\mathbf{v}$.

Based on the codes C and D, two asymmetric quantum codes can be derived, one from Theorem 3 directly without the mapping S by letting $C_1^{\perp_{\mathrm{tr}}} = C$ and $C_2 = D$ and another from Theorem 4 under the mapping S. We label the first quantum code Q while the second one Q_S.

Theorem 5. *Given any positive integer $n \geq 3$, there exists an $[[\mathbf{n},\mathbf{n-2},\mathbf{2/2}]]_\mathbf{4}$-asymmetric quantum MDS code.*

Proof. A general proof for the existence of an $[[\mathbf{n},\mathbf{n-2},\mathbf{2/2}]]_\mathbf{q}$-asymmetric quantum MDS code is already given in [17, Cor. 3.4]. Here we present a simple constructive proof for $q = 4$. A cyclic code D with parameters $[n,n-1,2]_4$ can be constructed by using $X+1$ as its generator polynomial. Its minimum distance is two since the check polynomial is $1 + X + \ldots + X^{n-1}$. By [5, Th. 1], D has codewords of length n. One such codeword can be chosen to form an $[n,1,n]_4$-code C. Applying Theorem 3 with $C_1^{\perp_{\mathrm{tr}}} = C$ and $C_2 = D$ brings us to the conclusion. □

For a fixed n, it is not guaranteed that for all $k \in \{2,\ldots,n-2\}$, the best-known linear code with parameters $[n,k,d]_4$ has codewords of weight n. For example, there is no codeword of weight 6 in the best-known $[6,4,2]_4$-code stored in the database of MAGMA that we use here.

Table 1 lists down the resulting quantum codes for $n = 4$ to $n = 20$ based on the list of best-known linear codes with parameters $[n,k]_4$ invoked under the command

BKLC in MAGMA. We exclude the case of $k = n-1$ in light of Theorem 5 and the case of $k = 1$ due to [6, Ex. 8.2]. The process can of course be done for larger values of n if so desired. Interested readers may contact the first author for the complete list of codes Q and Q_S with $d_z \geq d_x = 2$ which are derived from the best-known linear codes for up to $n = 46$.

Remark 1. Aside from its nice structural property, the advantage of using the mapping S can be seen, for instance, from the fact that we have the $[[18, 2, 12/2]]_4$-code Q_S which cannot be derived directly from the best-known linear codes for $n = 18$. Similarly for the following Q_S codes: $[[30, 2, 22/2]]_4$, $[[30, 3, 20/2]]_4$, $[[32, 3, 22/2]]_4$, $[[38, 4, 22/2]]_4$, $[[40, 4, 24/2]]_4$, $[[42, 4, 26/2]]_4$, $[[44, 4, 28/2]]_4$, and $[[46, 4, 28/2]]_4$.

7.2. CONSTRUCTION FROM CONCATENATED REED-SOLOMON CODES. Let m be a positive integer. Concatenation is used to obtain codes over $\mathbb{F}_q$ from codes over an extension $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$. A general method of performing concatenation is presented in [12, Sec. 6.3] and in [13, Ch. 10].

Our strategy here is to construct nested codes $C \subset D$ over $\mathbb{F}_4$ from nested codes $A \subset B$ over $\mathbb{F}_{4^m}$. We then use the codes C and D and the mapping S to get a quantum code Q.

The field $\mathbb{F}_{4^m}$ can be viewed as an $\mathbb{F}_4$-vector space with basis $\{\beta_1 \ldots, \beta_m\}$. Then, an element $x \in \mathbb{F}_{4^m}$ can be written uniquely as

$$x = \sum_{j=1}^{m} a_j \beta_j \text{ with } a_j \in \mathbb{F}_4.$$

We define a mapping $\phi : \mathbb{F}_{4^m} \to \mathbb{F}_4^m$ given by $x \mapsto (a_1, \ldots, a_m)$. This mapping is a bijective $\mathbb{F}_4$-linear transformation and extends naturally to the mapping ϕ^*

$$\begin{aligned} \phi^* : \quad & \mathbb{F}_{4^m}^N \to \mathbb{F}_4^{mN} \\ & (x_1, \ldots, x_n) \mapsto (\phi(x_1), \ldots, \phi(x_n)). \end{aligned} \tag{31}$$

If A is an $[N, K, D]_{4^m}$-code and letting $C = \phi^*(A)$, then it is easy to verify that C is an $[mN, mK, \geq D]_4$-code. Moreover, the mapping ϕ^* preserves nestedness by its $\mathbb{F}_4$-linearity. That is, if an $[N, K_1, D_1]_{4^m}$-code A is a subcode of an $[N, K_2, D_2]_{4^m}$-code B, then $C = \phi^*(A)$ is a subcode of $D = \phi^*(B)$ as codes over $\mathbb{F}_4$.

Let $q = 4^m$ and $\alpha_1, \ldots, \alpha_{q-1}$ be the nonzero elements of $\mathbb{F}_q$. It is well-known (see, e.g., [13, Ch. 10 and Ch.11]) that the $[q, k, q-k+1]_q$-extended Reed-Solomon (henceforth, RS) code B has a parity check matrix

$$H = \begin{pmatrix} 1 & 1 & \ldots & 1 & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_{q-1} & 0 \\ \alpha_1^2 & \alpha_2^2 & \ldots & \alpha_{q-1}^2 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha_1^{q-k-1} & \alpha_2^{q-k-1} & \ldots & \alpha_{q-1}^{q-k-1} & 0 \end{pmatrix}. \tag{32}$$

Let A be the $[q, 1, q]_q$-repetition code generated by $\mathbf{1} = (1, \ldots, 1)$. For $1 \leq j \leq q-2$, the sum $s = \sum_{l=1}^{q-1} \alpha_l^j = 0$. To see this, we choose α a primitive element of $\mathbb{F}_q$. Then $\alpha^j s = \sum_{l=1}^{q-1} (\alpha \cdot \alpha_l)^j = s$. Since $\alpha^j \neq 1$, we conclude that $s = 0$. This implies that $A \subset B$.

Note that we can choose an $\mathbb{F}_4$-basis $\{\beta_1 \ldots, \beta_m\}$ of $\mathbb{F}_q$ such that a generator matrix of $C' = \phi^*(A)$ is given by the $m \times mq$ matrix $G = (I_m | I_m | \ldots | I_m)$ where I_m is the $m \times m$ identity matrix. Hence, C' is of parameters $[mq, m, q]_4$. Define C to

TABLE 1. Asymmetric QECC from BKLC

n	**Code** Q	**Code** Q_S	n	**Code** Q	**Code** Q_S
4	$[[\mathbf{4,1,3/2}]]_\mathbf{4}$	$[[8,1,6/2]]_4$	15	$[[15,7,6/2]]_4$	$[[30,7,12/2]]_4$
5	$[[\mathbf{5,2,3/2}]]_\mathbf{4}$	$[[10,2,6/2]]_4$		$[[15,8,5/2]]_4$	$[[30,8,10/2]]_4$
6	$[[\mathbf{6,2,4/2}]]_\mathbf{4}$	$[[12,2,8/2]]_4$		$[[15,10,4/2]]_4$	$[[30,10,8/2]]_4$
7	$[[7,2,4/2]]_4$	$[[14,2,8/2]]_4$		$[[15,11,3/2]]_4$	$[[30,11,6/2]]_4$
	$[[7,3,3/2]]_4$	$[[14,3,6/2]]_4$	16	$[[16,2,12/2]]_4$	$[[32,2,24/2]]_4$
8	$[[8,1,6/2]]_4$	$[[16,1,12/2]]_4$		$[[16,3,11/2]]_4$	$[[32,3,22/2]]_4$
	$[[8,2,5/2]]_4$	$[[16,2,10/2]]_4$		$[[16,6,8/2]]_4$	$[[32,6,16/2]]_4$
	$[[8,3,4/2]]_4$	$[[16,3,8/2]]_4$		$[[16,7,7/2]]_4$	$[[32,7,14/2]]_4$
	$[[8,4,3/2]]_4$	$[[16,4,6/2]]_4$		$[[16,8,6/2]]_4$	$[[32,8,12/2]]_4$
9	$[[9,2,6/2]]_4$	$[[18,2,12/2]]_4$		$[[16,9,5/2]]_4$	$[[32,9,10/2]]_4$
	$[[9,3,5/2]]_4$	$[[18,3,10/2]]_4$		$[[16,11,4/2]]_4$	$[[32,11,8/2]]_4$
	$[[9,4,4/2]]_4$	$[[18,4,8/2]]_4$		$[[16,12,3/2]]_4$	$[[32,12,6/2]]_4$
	$[[9,5,3/2]]_4$	$[[18,5,6/2]]_4$	17	$[[17,5,9/2]]_4$	$[[34,5,18/2]]_4$
10	$[[10,3,6/2]]_4$	$[[20,3,12/2]]_4$		$[[17,8,7/2]]_4$	$[[34,8,14/2]]_4$
	$[[10,4,5/2]]_4$	$[[20,4,10/2]]_4$		$[[17,9,6/2]]_4$	$[[34,9,12/2]]_4$
	$[[10,5,4/2]]_4$	$[[20,5,8/2]]_4$		$[[17,10,5/2]]_4$	$[[34,10,10/2]]_4$
	$[[10,6,3/2]]_4$	$[[20,6,6/2]]_4$		$[[17,12,4/2]]_4$	$[[34,12,8/2]]_4$
11	$[[11,2,7/2]]_4$	$[[22,2,14/2]]_4$		$[[17,13,3/2]]_4$	$[[34,13,6/2]]_4$
	$[[11,4,6/2]]_4$	$[[22,4,12/2]]_4$	18	$[[18,5,10/2]]_4$	$[[36,5,20/2]]_4$
	$[[11,5,5/2]]_4$	$[[22,5,10/2]]_4$		$[[18,6,9/2]]_4$	$[[36,6,18/2]]_4$
	$[[11,6,4/2]]_4$	$[[22,6,8/2]]_4$		$[[18,8,8/2]]_4$	$[[36,8,16/2]]_4$
	$[[11,7,3/2]]_4$	$[[22,7,6/2]]_4$		$[[18,10,6/2]]_4$	$[[36,10,12/2]]_4$
12	$[[12,2,8/2]]_4$	$[[24,2,16/2]]_4$		$[[18,11,5/2]]_4$	$[[36,11,10/2]]_4$
	$[[12,3,7/2]]_4$	$[[24,3,14/2]]_4$		$[[18,12,4/2]]_4$	$[[36,12,8/2]]_4$
	$[[12,5,6/2]]_4$	$[[24,5,12/2]]_4$		$[[18,14,3/2]]_4$	$[[36,14,6/2]]_4$
	$[[12,7,4/2]]_4$	$[[24,7,8/2]]_4$	19	$[[19,4,11/2]]_4$	$[[38,4,22/2]]_4$
	$[[12,8,3/2]]_4$	$[[24,8,6/2]]_4$		$[[19,5,10/2]]_4$	$[[38,5,20/2]]_4$
13	$[[13,2,9/2]]_4$	$[[26,2,18/2]]_4$		$[[19,6,9/2]]_4$	$[[38,6,18/2]]_4$
	$[[13,4,7/2]]_4$	$[[26,4,14/2]]_4$		$[[19,8,8/2]]_4$	$[[38,8,16/2]]_4$
	$[[13,5,6/2]]_4$	$[[26,5,12/2]]_4$		$[[19,9,7/2]]_4$	$[[38,9,14/2]]_4$
	$[[13,6,5/2]]_4$	$[[26,6,10/2]]_4$		$[[19,11,6/2]]_4$	$[[38,11,12/2]]_4$
	$[[13,8,4/2]]_4$	$[[26,8,8/2]]_4$		$[[19,12,5/2]]_4$	$[[38,12,10/2]]_4$
	$[[13,9,3/2]]_4$	$[[26,9,6/2]]_4$		$[[19,13,4/2]]_4$	$[[38,13,8/2]]_4$
14	$[[14,2,10/2]]_4$	$[[28,2,20/2]]_4$		$[[19,15,3/2]]_4$	$[[38,15,6/2]]_4$
	$[[14,3,9/2]]_4$	$[[28,3,18/2]]_4$	20	$[[20,4,12/2]]_4$	$[[40,4,24/2]]_4$
	$[[14,4,8/2]]_4$	$[[28,4,16/2]]_4$		$[[20,5,11/2]]_4$	$[[40,5,22/2]]_4$
	$[[14,5,7/2]]_4$	$[[28,5,14/2]]_4$		$[[20,6,10/2]]_4$	$[[40,6,20/2]]_4$
	$[[14,6,6/2]]_4$	$[[28,6,12/2]]_4$		$[[20,7,9/2]]_4$	$[[40,7,18/2]]_4$
	$[[14,7,5/2]]_4$	$[[28,7,10/2]]_4$		$[[20,9,8/2]]_4$	$[[40,9,16/2]]_4$
	$[[14,9,4/2]]_4$	$[[28,9,8/2]]_4$		$[[20,10,7/2]]_4$	$[[40,10,14/2]]_4$
	$[[14,10,3/2]]_4$	$[[28,10,6/2]]_4$		$[[20,12,6/2]]_4$	$[[40,12,12/2]]_4$
15	$[[15,2,11/2]]_4$	$[[30,2,22/2]]_4$		$[[20,13,5/2]]_4$	$[[40,13,10/2]]_4$
	$[[15,3,10/2]]_4$	$[[30,3,20/2]]_4$		$[[20,14,4/2]]_4$	$[[40,14,8/2]]_4$
	$[[15,6,7/2]]_4$	$[[30,6,14/2]]_4$		$[[20,16,3/2]]_4$	$[[40,16,6/2]]_4$

be the $[mq, 1, mq]_4$-repetition code subset of C'. This is valid since we know that $\mathbf{1} = (1, \ldots, 1) \in C'$. The code $D = \phi^*(B)$ is an $[mq, mk, d' \geq (q - k + 1)]_4$-code that contains C. Repeating the proof of Theorem 4 yields the following result.

Theorem 6. *Let m be a positive integer, $q = 4^m$, and $1 \leq k \leq q$. Then there exists a $[[2mq, mk - 1, (\geq 2(q - k + 1))/2]]_4$-asymmetric quantum code Q.*

Remark 2. For a specific value of m and a given basis $\{\beta_1, \ldots, \beta_m\}$, $d' = d(D)$ can be explicitly computed. As noted in [13, Ch. 10], a change of basis may change the weight distribution and even the minimum weight of the code D.

Example 6. For $m = 2$ and $1 \leq k \leq 16$ we get the $[[64, k', d_z/2]]_4$-quantum codes listed in Table 2.

Table 2. $[[64, k', d_z/2]]_4$-code Q from $[16, k, 16-k+1]_{16}$-extended RS codes

k	1	2	3	4	5	6	7	8
k'	1	3	5	7	9	11	13	15
$d_z \geq$	32	30	28	26	24	22	20	18
k	9	10	11	12	13	14	15	16
k'	17	19	21	23	25	27	29	31
$d_z \geq$	16	14	12	10	8	6	4	2

Example 7. For $m = 3$ and $1 \leq k \leq 64$ the $[[384, k', d_z/2]]_4$-quantum codes listed in Table 3 are derived.

8. Conclusions and open problems

In this paper we have given a special construction of asymmetric quantum codes. An analysis on the weight enumerators of the resulting quantum codes is also presented. It seems that the construction is especially useful when the constraint on d_x is minimal and the demand on d_z is critical.

This allows us to give a more general criterion to use in choosing a pair of $\mathbb{F}_4$-linear codes $C \subset D$ that, in some cases, yields asymmetric quantum codes with improved parameters compared to those listed in [6]. Many new asymmetric quantum codes are also found.

There are direct generalizations of the mapping S. One direction might be to use non-quadratic extensions. Another one is to generalize it to fields of odd characteristics. The latter might be more promising than the former.

Acknowledgment

The work of M. F. Ezerman was carried out under the Nanyang Technological University PhD Research Scholarship. The work of S. Ling and P. Solé was partially supported by Singapore National Research Foundation Competitive Research Program grant NRF-CRP2-2007-03 and by the Merlion Programme 01.01.06. P. Solé acknowledges the hospitality of the Department of Mathematics at El Manar Tunis where part of the research was done. Likewise, O. Yemen is grateful for the hospitality she experienced at the I3S-CNRS Laboratory at Sophia Antipolis. Her work was supported by the Algebra and Number Theory Laboratory 99/UR/15-18, the Faculty of Sciences of Tunis.

TABLE 3. $[[384, k', d_z/2]]_4$-code Q from $[64, k, 64-k+1]_{64}$-extended RS codes

k	1	2	3	4	5	6	7	8
k'	2	5	8	11	14	17	20	23
$d_z \geq$	128	126	124	122	120	118	116	114
k	9	10	11	12	13	14	15	16
k'	26	29	32	35	38	41	44	47
$d_z \geq$	112	110	108	106	104	102	100	98
k	17	18	19	20	21	22	23	24
k'	50	53	56	59	62	65	68	71
$d_z \geq$	96	94	92	90	88	86	84	82
k	25	26	27	28	29	30	31	32
k'	74	77	80	83	86	89	92	95
$d_z \geq$	80	78	76	74	72	70	68	66
k	33	34	35	36	37	38	39	40
k'	98	101	104	107	110	113	116	119
$d_z \geq$	64	62	60	58	56	54	52	50
k	41	42	43	44	45	46	47	48
k'	122	125	128	131	134	137	140	143
$d_z \geq$	48	46	44	42	40	38	36	34
k	49	50	51	52	53	54	55	56
k'	146	149	152	155	158	161	164	167
$d_z \geq$	32	30	28	26	24	22	20	18
k	57	58	59	60	61	62	63	64
k'	170	173	176	179	182	185	188	191
$d_z \geq$	16	14	12	10	8	6	4	2

REFERENCES

[1] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language*, J. Symb. Comput., **24** (1997), 235–265.

[2] D. Boucher, W. Geiselmann and F. Ulmer, *Skew-cyclic codes*, Applied Algebra Engin. Commun. Comput., **18** (2007), 379–389.

[3] D. Boucher and F. Ulmer, *Codes as modules over skew polynomial rings*, in "Proceedings of the 12th IMA Conference on Cryptography and Coding," Cirencester, (2009), 38–55.

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

[5] M. F. Ezerman, M. Grassl and P. Solé, *The weights in MDS codes*, IEEE Trans. Inform. Theory, **57** (2011), 392–396.

[6] M. F. Ezerman, S. Ling and P. Solé, *Additive asymmetric quantum codes*, preprint, arXiv:1002.4088.

[7] K. Feng, S. Ling and C. Xing, *Asymptotic bounds on quantum codes from algebraic geometry codes*, IEEE Trans. Inform. Theory, **52** (2006), 986–991.

[8] E. M. Gabidulin, *Theory of codes with maximum rank distance*, Probl. Peredach. Inform. (in Russian), **21** (1985), 3–16; English translation, 1–12.

[9] M. Grassl, *Bounds on the minimum distance of linear codes and quantum codes*, available online at http://www.codetables.de.

[10] W. C. Huffman and V. Pless, "Fundamentals of Error-Correcting Codes," Cambridge University Press, Cambridge, 2003.

[11] J. L. Kim and V. Pless, *Designs in additive codes over $GF(4)$*, Des. Codes Crypt., **30** (2003), 187–199.
[12] S. Ling and C. P. Xing, "Coding Theory. A First Course," Cambridge University Press, Cambridge, 2004.
[13] F. J. MacWilliams and N. J. A. Sloane, "The Theory of Error-Correcting Codes," North-Holland, Amsterdam, 1977.
[14] G. Nebe, E. M. Rains and N. J. A. Sloane, "Self-Dual Codes and Invariant Theory," Springer-Verlag, Berlin, Heidelberg, 2006.
[15] E. M. Rains and N. J. A. Sloane, *Self-dual codes*, in "Handbook of Coding Theory I" (eds. V.S. Pless and W.C. Huffman), Elsevier, (1998), 177–294.
[16] P. K. Sarvepalli, A. Klappenecker and M. Rötteler, *Asymmetric quantum codes: constructions, bounds and performance*, Proc. Royal Soc. A, **465** (2009), 1645–1672.
[17] L. Wang, K. Feng, S. Ling and C. Xing, *Asymmetric quantum codes: characterization and constructions*, IEEE Trans. Inform. Theory, **56** (2010), 2938–2945.

Received for publication May 2010.

E-mail address: mart0005@e.ntu.edu.sg
E-mail address: lingsan@ntu.edu.sg
E-mail address: sole@enst.fr
E-mail address: olfa_yemen@yahoo.fr