New Optimal Asymmetric Quantum Codes from Constacyclic Codes*

Guanghui Zhang[1], Bocong Chen[2], Liangchen Li[1]

[1]School of Mathematical Sciences, Luoyang Normal University, Luoyang, Henan, 471022, China
[2]School of Physical & Mathematical Sciences, Nanyang Technological University, Singapore 637616, Singapore

Abstract

In this paper, we construct two classes of asymmetric quantum codes by using constacyclic codes. The first class is the asymmetric quantum codes with parameters $[[q^2+1, q^2+1-2(t+k+1), (2k+2)/(2t+2)]]_{q^2}$ where q is an odd prime power, t, k are integers with $0 \leq t \leq k \leq \frac{q-1}{2}$, which is a generalization of [20, Theorem 2] in the sense that we do not assume that $q \equiv 1 \pmod 4$. The second one is the asymmetric quantum codes with parameters $[[\frac{q^2-1}{2}, \frac{q^2-1}{2}-t-k, (k+1)/(t+1)]]_{q^2}$, where $q \geq 5$ is an odd prime power, t, k are integers with $0 \leq t \leq k \leq q-1$. The constructed asymmetric quantum codes are optimal and their parameters are not covered by the codes available in the literature.

Keywords: Quantum code, Constacyclic code, Asymmetric quantum code

PACS number(s): 03.67.Pp, 89.70.-a

1 Introduction

Asymmetric quantum error-correcting codes (AQECC) were initiated by Steane in [1]. Quantum codes defined over quantum channels where qudit-flip errors and phase-shift errors may have different probabilities are called asymmetric quantum codes. The parameters $[[n, k, d_z/d_x]]_q$ customarily denote an asymmetric quantum code, where d_z is the minimum distance corresponding to phase-shift errors and d_x is the minimum distance corresponding to qudit-flip errors. In many quantum mechanical systems, the occurrence of bit flip and phase flip errors is quite different. The combined amplitude damping and dephasing channel is an example for a quantum channel that satisfies $d_z > d_x$, i.e., the probability of occurrence of phase-shift errors is greater than the probability of occurrence of qudit-flip errors.

In recent years, there have been intensive activities in the area of constructing AQECC. Aly *et al.* in [6] constructed several families of quantum BCH, RS and RM codes over asymmetric quantum channels. Wang *et al.* in [7] presented a mathematical characterization of asymmetric quantum codes. Leng and Ma in [14] constructed families of good asymmetric quantum BCH codes. Chee *et al.* in [8] constructed pure q-ary asymmetric quantum codes which can attain the quantum Sigleton bound. Qian *et al.* in [15, 17] studied asymmetric quantum codes by using cyclotomic cosets. More recently, Chen *et al.* in [20] constructed two families of asymmetric quantum codes by using negacyclic codes.

Motivated by [20], we construct two classes of asymmetric quantum codes by using constacyclic codes (e.g., see [12] or [13]), which constitute a remarkable generalization of cyclic codes and negacyclic code. The first class is the asymmetric quantum codes with parameters $[[q^2+1, q^2+1-2(t+k+1), (2k+2)/(2t+2)]]_{q^2}$ where q is an odd prime power, t, k are integers with $0 \leq t \leq k \leq \frac{q-1}{2}$, which is a generalization of [20, Theorem 2] in the sense that we do not assume that $q \equiv 1 \pmod 4$. The second one is the asymmetric quantum codes with parameters $[[\frac{q^2-1}{2}, \frac{q^2-1}{2}-t-k, (k+1)/(t+1)]]_{q^2}$, where $q \geq 5$ is an

*Email addresses: zghui2012@126.com (G. Zhang), bocong_chen@yahoo.com (B. Chen), lcli@yahoo.com (L. Li).

odd prime power, t, k are integers with $0 \leq t \leq k \leq q-1$. The constructed asymmetric quantum codes are optimal and their parameters are not covered by the codes available in the literature.

The organization of this paper is as follows. In Section 2, we present some definitions and basic results about constacyclic codes and asymmetric quantum codes. In Section 3, two classes of asymmetric quantum codes are constructed and some illustrative examples are given.

2 Preliminaries

In this section, we recall the following definitions and facts which are important to the constructions of asymmetric quantum codes.

2.1 Review of constacyclic codes

Let $\mathbb{F}_{q^2}$ be the finite field with q^2 elements. Let $\mathbb{F}_{q^2}^*$ denote the multiplicative group of nonzero elements of $\mathbb{F}_{q^2}$. For $\beta \in \mathbb{F}_{q^2}^*$, we denote by $r = \mathrm{ord}(\beta)$ the order of β in the group $\mathbb{F}_{q^2}^*$, i.e., r is the smallest positive integer s such that $\beta^s = 1$. Then $\mathrm{ord}(\beta)$ is a divisor of q^2-1, and β is called a *primitive rth root of unity*.

Starting from this section till the end of this paper, we assume that n is a positive integer relatively prime to q. Let $\mathbb{F}_{q^2}^n$ be the $\mathbb{F}_{q^2}$-vector space of n-tuples. A *linear code* C of length n over $\mathbb{F}_{q^2}$ is an $\mathbb{F}_{q^2}$-subspace of $\mathbb{F}_{q^2}^n$. For $\lambda \in \mathbb{F}_{q^2}^*$, a linear code C of length n over $\mathbb{F}_{q^2}$ is said to be *λ-constacyclic* if $(\lambda c_{n-1}, c_0, \cdots, c_{n-2}) \in C$ for every $(c_0, c_1, \cdots, c_{n-1}) \in C$. When $\lambda = 1$, λ-constacyclic codes are *cyclic codes*, and when $\lambda = -1$, λ-constacyclic codes are just *negacyclic codes*.

Each codeword $\mathbf{c} = (c_0, c_1, \cdots, c_{n-1}) \in C$ is customarily identified with its polynomial representation $c(X) = c_0 + c_1 X + \cdots + c_{n-1}X^{n-1}$. In this way, every λ-constacyclic code C is identified with exactly one ideal of the quotient algebra $\mathbb{F}_{q^2}[X]/\langle X^n - \lambda\rangle$ (e.g., see [12] or [13]).

Let $\lambda \in \mathbb{F}_{q^2}^*$ be a primitive rth of unity. Then there exists a primitive rnth root of unity (in some extension field of $\mathbb{F}_{q^2}$), say η, such that $\eta^n = \lambda$. The roots of $X^n - \lambda$ are precisely the elements η^{1+ri} for $0 \leq i \leq n-1$. Set $\theta_{r,n} = \{1 + ri \,|\, 0 \leq i \leq n-1\}$. The *defining set* of a constacyclic code $C = \langle g(X)\rangle$ of length n is the set $Z = \{j \in \theta_{r,n} \,|\, \eta^j \text{ is a root of } g(X)\}$. It is easy to see that the defining set Z is a union of some q^2-cyclotomic cosets modulo rn and $\dim_{\mathbb{F}_{q^2}}(C) = n - |Z|$ (see [19] or [21]).

The following theorem gives the BCH bound for constacyclic codes (see [19, Theorem 4.1]).

Theorem 2.1. *(**The BCH bound for constacyclic codes**) Let C be a λ-constacyclic code of length n over $\mathbb{F}_{q^2}$, where λ is a primitive rth root of unity. Let η be a primitive rnth root of unity in an extension field of $\mathbb{F}_{q^2}$ such that $\eta^n = \lambda$. Assume the generator polynomial of C has roots that include the set $\{\eta\zeta^i \,|\, i_1 \leq i \leq i_1 + d - 1\}$, where $\zeta = \eta^r$. Then the minimum distance of C is at least d.*

The *Hermitian inner product* on $\mathbb{F}_{q^2}^n$ is defined as

$$(\mathbf{x}, \mathbf{y})_h = x_0 y_0^q + x_1 y_1^q + \cdots + x_{n-1} y_{n-1}^q,$$

where $\mathbf{x} = (x_0, x_1, \cdots, x_{n-1}) \in \mathbb{F}_{q^2}^n$ and $\mathbf{y} = (y_0, y_1, \cdots, y_{n-1}) \in \mathbb{F}_{q^2}^n$. The *Hermitian dual code* of C is defined as

$$C^{\perp_h} = \Big\{\mathbf{x} \in \mathbb{F}_{q^2}^n \;\Big|\; \sum_{i=0}^{n-1} x_i y_i^q = 0, \quad \text{for any } \mathbf{y} \in C\Big\}.$$

If $C \subseteq C^{\perp_h}$, then C is called a (Hermitian) self-orthogonal code. Conversely, if $C^{\perp_h} \subseteq C$, we say that C is a (Hermitian) dual-containing code. Dual-containing codes are also known as weakly self-dual codes; it is the type of code we are most concerned with in this paper.

Let $\lambda \in \mathbb{F}_{q^2}^*$ be a primitive rth root of unity. For a λ-constacyclic code of length n over $\mathbb{F}_{q^2}$, it is shown that $C^{\perp_h}$ is a λ^{-q}-constacyclic code; further, $\lambda = \lambda^{-q}$ precisely when $r \mid (q+1)$ ([19, Lemma 2.1(ii)]).

The following propositions are important in constructing asymmetric quantum codes.

Proposition 2.2. *Let C_i be λ-constacyclic codes of length n over $\mathbb{F}_{q^2}$ with defining set Z_i for $i = 1, 2$. Then $C_1 \subseteq C_2$ if and only if $Z_2 \subseteq Z_1$.*

Proposition 2.3. *(**Singleton bound for linear codes**) If an $[n, k, d]$ linear code over $\mathbb{F}_{q^2}$ exists, then $k \leq n - d + 1$.*

The next result presents a criterion to determine whether or not a given λ-constacyclic code of length n over $\mathbb{F}_{q^2}$ is dual-containing (e.g., see [21, Lemma 2.2]).

Lemma 2.4. *Let $\lambda \in \mathbb{F}_{q^2}^*$ be of order r. Assume that C is a λ-constacyclic code of length n over $\mathbb{F}_{q^2}$ with defining set Z. Then C is a dual-containing code if and only if $Z \bigcap Z^{-q} = \emptyset$, where $Z^{-q} = \{-qz \pmod{rn} \,|\, z \in Z\}$.*

2.2 Error groups and asymmetric quantum codes

In this subsection, we begin with some basic concepts about quantum error operators and asymmetric quantum codes (see [11] and [16]). Assume that p is the characteristic of the finite field $\mathbb{F}_q$. Let H be the Hilbert space $H = \mathbb{C}^{q^n} = \mathbb{C}^q \otimes \cdots \otimes \mathbb{C}^q$. Let $|x\rangle$ be the vectors of an orthonormal basis of $\mathbb{C}^q$, where the labels x are elements of $\mathbb{F}_q$. For $a, b \in \mathbb{F}_q$, the unitary operators $X(a)$ and $Z(b)$ in $\mathbb{C}^q$ are defined by

$$X(a)|x\rangle = |x + a\rangle,\ Z(b)|x\rangle = \omega^{tr(bx)}|x\rangle,$$

where $\omega = exp(2\pi i/p)$ is a primitive pth root of unity and tr is the trace map from $\mathbb{F}_q$ to $\mathbb{F}_p$. Consider that $a = (a_1, a_2, \cdots, a_n) \in \mathbb{F}_q^n$ and $b = (b_1, b_2, \cdots, b_n) \in \mathbb{F}_q^n$. Denote by

$$X(a) = X(a_1) \otimes \cdots \otimes X(a_n),$$

$$Z(b) = Z(b_1) \otimes \cdots \otimes Z(b_n),$$

the tensor products of n error operators. The set $E_n = \{X(a)Z(b) \mid a, b \in \mathbb{F}_q^n\}$ is an error basis on the complex vector space $\mathbb{C}^{q^n}$ and the set $G_n = \{\omega^c X(a)Z(b) \mid a, b \in F_q^n, c \in \mathbb{F}_p\}$ is the error group associated with E_n. For a quantum error $e = \omega^c X(a)Z(b) \in G_n$, the quantum weight $\omega_Q(e)$, the X-weight $\omega_X(e)$ and the Z-weight $\omega_Z(e)$ of e, are defined respectively by

$$\omega_Q(e) = \sharp\{i : 1 \leq i \leq n, (a_i, b_i) \neq (0, 0)\},$$

$$\omega_X(e) = \sharp\{i : 1 \leq i \leq n, a_i \neq 0\},$$

$$\omega_Z(e) = \sharp\{i : 1 \leq i \leq n, b_i \neq 0\}.$$

A q-ary asymmetric quantum code C, denoted by $[[n, k, d_z/d_x]]_q$, is a q^k-dimensional subspace of the Hilbert space H and can control all qubit-flip errors up to $\lfloor (d_x - 1)/2 \rfloor$ and all phase-flip errors up to $\lfloor (d_z - 1)/2 \rfloor$. The code C also detects $d_x - 1$ qubit-flip errors as well as detects $d_z - 1$ phase-shift errors.

In order to construct asymmetric quantum codes, we reproduce the following important results from Refs. [3], [4] and [5].

Theorem 2.5. *(**CSS Construction**) Let C_i be a classical linear code with parameters $[n, k_i, d_i]$ for $i = 1, 2$, with $C_1^\perp \subseteq C_2$. Then there exists an asymmetric quantum code Q with parameters $[[n, k_1 + k_2 - n, d_z/d_x]]$, where $d_x = wt(C_1 \backslash C_2^\perp)$ and $d_z = wt(C_2 \backslash C_1^\perp)$.*

Proposition 2.6. *Let C be an asymmetric quantum code with parameters $[[n, k_1 + k_2 - n, d_z/d_x]]$, which is obtained by the CSS construction. Then*

$$k \leq n - d_x - d_z + 2.$$

Definition 2.7. *Let C be an asymmetric quantum code $[[n, k_1 + k_2 - n, d_z/d_x]]$. If C satisfies the equality $k = n - d_x - d_z + 2$, then it is called an optimal code.*

3 Code Constructions

In this section, we will use λ-constacyclic codes of lengths $n = q^2 + 1$ and $n = \frac{q^2-1}{2}$ to construct optimal asymmetric quantum codes, respectively. We always assume that q is an odd prime power.

3.1 Optimal asymmetric quantum codes of length $q^2 + 1$

Let $r = q+1$ and $n = q^2+1$. Let $\lambda \in \mathbb{F}_{q^2}^*$ be of order r and η (in some extension field of $\mathbb{F}_{q^2}$) be a primitive rnth root of unity such that $\eta^n = \lambda$. Observe that $(q^2)^2 \equiv 1 \pmod{rn}$ and $q^2 \not\equiv 1 \pmod{rn}$, which imply that each q^2-cyclotomic coset modulo rn contains one or two elements. Now, $\theta_{r,n} = \{1+(q+1)i \,|\, 0 \leq i \leq n-1\}$; expanding $q^2(1+(q+1)i) \equiv 1+(q+1)i \pmod{rn}$, we deduce that $q^2-1 \equiv 2(q+1)i \pmod{rn}$, or equivalently, $q - 1 \equiv 2i \pmod{q^2+1}$. This gives $i = \frac{q-1}{2} + k \cdot \frac{q^2+1}{2}$, which forces $k = 0$ or 1 since $0 \leq i \leq n-1$. We then know that $1 + (q+1) \cdot \frac{q-1}{2}$ and $1 + (q+1) \cdot (\frac{q-1}{2} + \cdot \frac{q^2+1}{2})$ are the only elements of $\theta_{r,n}$ with the property that $q^2 s \equiv s \pmod{rn}$ for $s \in \theta_{r,n}$.

Let δ be an integer with $0 \leq \delta \leq \frac{q-1}{2}$. Consider λ-constacyclic code C of length q^2+1 over $\mathbb{F}_{q^2}$ with defining set

$$Z = \Big\{1 + \Big(q+1\Big)i \,\Big|\, \frac{q-1}{2} - \delta \leq i \leq \frac{q-1}{2} + \delta\Big\}. \tag{3.1}$$

It follows that $|Z| = 2\delta + 1$. We need to prove that Z is a disjoint union of some q^2-cyclotomic cosets modulo rn. To this end, it suffices to show that $q^2(1+(q+1)i) \pmod{rn} \in Z$ for any $\frac{q-1}{2} - \delta \leq i \leq \frac{q-1}{2} + \delta$. After routine computations,

$$q^2(1 + (q+1)i) \equiv 1 + (q+1)(q-1-i) \pmod{rn}. \tag{3.2}$$

It is easy to see that $\frac{q-1}{2} - \delta \leq q - 1 - i \leq \frac{q-1}{2} + \delta$, which gives that Z is a disjoint union of some q^2-cyclotomic cosets modulo rn.

We have shown that C is a λ-constacyclic code of length q^2+1 over $\mathbb{F}_{q^2}$. In the next result, we prove that C satisfies $C^{\perp_h} \subseteq C$.

Lemma 3.1. *Let q be an odd prime power and $\lambda \in \mathbb{F}_{q^2}$ be a primitive $(q+1)$th root of unity. If C is a λ-constacyclic code of length $n = q^2 + 1$ over $\mathbb{F}_{q^2}$ with defining set Z as in (3.1), then C satisfies $C^{\perp_h} \subseteq C$.*

Proof. Let $r = q + 1$. By Lemma 2.4, it suffices to prove that $Z \bigcap Z^{-q} = \emptyset$, where $Z^{-q} = \{-qz \pmod{rn} \,|\, z \in Z\}$. Simple calculations show that

$$-q(1 + (q+1)i) \equiv 1 + (q+1)(q^2 - qi) \pmod{rn}. \tag{3.3}$$

For $\frac{q-1}{2} - \delta \leq i \leq \frac{q-1}{2} + \delta$ and $0 \leq \delta \leq \frac{q-1}{2}$, one gets $0 \leq i \leq q-1$. It follows that $0 < q^2 - qi < q^2 + 1 = n$. We claim that $q^2 - qi > \frac{q-1}{2} + \delta$. Indeed, it follows from $i \leq \frac{q-1}{2} + \delta$ and $0 \leq \delta \leq \frac{q-1}{2}$ that

$$q^2 - qi - (\frac{q-1}{2} + \delta) \geq q^2 - q(q-1) - (q-1) = 1 > 0.$$

Suppose otherwise that $Z \bigcap Z^{-q} \neq \emptyset$. Then two integers i, j with $\frac{q-1}{2} - \delta \leq i, j \leq \frac{q-1}{2} + \delta$ can be found such that $-q(1+(q+1)i) \equiv 1+(q+1)j \pmod{rn}$. Combining equation (3.3), we have $1+(q+1)(q^2-qi) \equiv 1+(q+1)j \pmod{rn}$. Since $0 < q^2 - qi < n$ and $0 \leq j < n$, it follows that $1+(q+1)(q^2-qi) = 1+(q+1)j$, i.e., $q^2 - qi = j$. However, $q^2 - qi > \frac{q-1}{2} + \delta \geq j$, which is a contradiction. □

Combining the BCH bound for constacyclic codes (Theorem 2.1) and the Singleton boud for linear codes (Proposition 2.3), we conclude that C is a λ-constacyclic MDS code over $\mathbb{F}_{q^2}$ with parameters $[q^2+1, q^2+1-(2\delta+1), 2(\delta+1)]$. It follows that $C^{\perp_h}$ is also a λ-constacyclic MDS code over $\mathbb{F}_{q^2}$ with parameters $[q^2+1, 2\delta+1, q^2-2\delta+1]$.

Theorem 3.2. *Let q be an odd prime power. Let t, k be integers with $0 \leq t \leq k \leq \frac{q-1}{2}$. Then there exist optimal asymmetric quantum codes with parameters $[[q^2+1, q^2+1-2(t+k+1), (2k+2)/(2t+2)]]_{q^2}$.*

Proof. Assume that $\lambda \in \mathbb{F}_{q^2}$ is a primitive $(q+1)$th root of unity. Let C_i, $i = 1, 2$, be λ-constacyclic codes of length q^2+1 over $\mathbb{F}_{q^2}$ with defining sets $Z_1 = \{1+(q+1)i \,|\, \frac{q-1}{2} - t \leq i \leq \frac{q-1}{2} + t\}$ and $Z_2 = \{1+(q+1)i \,|\, \frac{q-1}{2} - k \leq i \leq \frac{q-1}{2} + k\}$, respectively. From the above discussion, we see that C_1 is a $[q^2+1, q^2+1-(2t+1), 2(t+1)]$ MDS code satisfying $C_1^{\perp_h} \subseteq C_1$, and C_2 is a $[q^2+1, q^2+1-(2k+1), 2(k+1)]$ MDS code satisfying $C_2^{\perp_h} \subseteq C_2$. Obviously $Z_1 \subseteq Z_2$, and so $C_2 \subseteq C_1$ by Proposition 2.2, which implies that $C_1^{\perp_h} \subseteq C_2^{\perp_h}$. We then have $C_1^{\perp_h} \subseteq C_2$ and $C_2^{\perp_h} \subseteq C_1$. To complete the proof, we claim that $d_x = wt(C_1 \setminus C_2^{\perp_h}) = wt(C_1) = 2(t+1)$ and $d_z = wt(C_2 \setminus C_1^{\perp_h}) = wt(C_2) = 2(k+1)$. Note that $C_2^{\perp_h}$ is a $[q^2+1, 2k+1, q^2-2k+1]$ MDS code, which implies that the Hamming weights of all nonzero codewords of $C_2^{\perp_h}$ are greater than or equal to q^2-2k+1. On the other hand, $wt(C_1) = 2(t+1)$ and $q^2-2k+1 > 2(t+1)$. This gives that the codewords with Hamming weight $2(t+1)$ are not contained in $C_2^{\perp_h}$. Therefore, $d_x = wt(C_1 \setminus C_2^{\perp_h}) = wt(C_1) = 2(t+1)$. Similar reasoning shows that $d_z = wt(C_2 \setminus C_1^{\perp_h}) = wt(C_2) = 2(k+1)$. Using the CSS construction, we know that there exist asymmetric quantum codes with parameters $[[q^2+1, q^2+1-2(t+k+1), (2k+2)/(2t+2)]]_{q^2}$. Further, $q^2+1-d_x-d_z+2 = q^2-2t-2k-1$, which shows the desired result. □

Example 3.3. *Take $q = 11$, so $r = 12$ and $n = 122$. The following table gives the optimal asymmetric quantum codes derived from Theorem 3.2.*

Table 1: Optimal asymmetric quantum codes derived from Theorem 3.2

t	k	*asymmetric quantum optimal codes*
1	5	$[[122, 108, 12/4]]_{121}$
2	5	$[[122, 106, 12/6]]_{121}$
3	5	$[[122, 104, 12/8]]_{121}$
4	5	$[[122, 102, 12/10]]_{121}$
2	3	$[[122, 110, 8/6]]_{121}$
2	4	$[[122, 108, 10/6]]_{121}$
3	4	$[[122, 106, 10/8]]_{121}$

Example 3.4. *Take $q = 13$, so $r = 14$ and $n = 170$. The following table gives the optimal asymmetric quantum codes derived from Theorem 3.2.*

Table 2: Optimal asymmetric quantum codes derived from Theorem 3.2

t	k	*asymmetric quantum optimal codes*
1	6	$[[170, 154, 14/2]]_{169}$
2	6	$[[170, 152, 14/6]]_{169}$
3	6	$[[170, 150, 14/8]]_{169}$
4	6	$[[170, 148, 14/10]]_{169}$
5	6	$[[170, 146, 14/12]]_{169}$
1	5	$[[170, 156, 12/4]]_{169}$
2	5	$[[170, 154, 12/6]]_{169}$
3	5	$[[170, 152, 12/8]]_{169}$
4	5	$[[170, 150, 12/10]]_{169}$
1	4	$[[170, 158, 10/4]]_{169}$
2	4	$[[170, 156, 10/6]]_{169}$
3	4	$[[170, 154, 10/8]]_{169}$
1	3	$[[170, 160, 8/4]]_{169}$
2	3	$[[170, 158, 8/6]]_{169}$

3.2 Optimal asymmetric quantum codes of length $\frac{q^2-1}{2}$

Let $q \geq 5$ be an odd prime power and let $n = \frac{q^2-1}{2}$. Observe that $q^2 \equiv 1 \pmod{2n}$, which implies that each q^2-cyclotomic coset modulo $2n$ contains exactly one element. Taking $r = 2$ in [21, Lemma 3.1], we have the following result.

Lemma 3.5. *Let $q \geq 5$ be an odd prime power. If C is a negacyclic code of length $\frac{q^2-1}{2}$ over $\mathbb{F}_{q^2}$ with defining set $Z = \{1 + 2(j-1) \,|\, 1 \leq j \leq \delta\}$, where $1 \leq \delta \leq q-1$. Then C is a $[\frac{q^2-1}{2}, \frac{q^2-1}{2} - \delta, \delta + 1]$ MDS code satisfying $C^{\perp_h} \subseteq C$.*

Theorem 3.6. *Let $q \geq 5$ be an odd prime power. Let t, k be integers with $0 \leq t \leq k \leq q-1$. Then there exist optimal asymmetric quantum codes with parameters $[[\frac{q^2-1}{2}, \frac{q^2-1}{2} - t - k, (k+1)/(t+1)]]_{q^2}$.*

Proof. Let C_i, $i = 1, 2$, be negacyclic codes of length $\frac{q^2-1}{2}$ over $\mathbb{F}_{q^2}$ with defining sets $Z_1 = \{1 + 2(j-1) \,|\, 1 \leq j \leq t\}$ and $Z_2 = \{1 + 2(j-1) \,|\, 1 \leq j \leq k\}$, respectively. We then know from Lemma 3.5 that C_1 is a $[\frac{q^2-1}{2}, \frac{q^2-1}{2} - t, t+1]$ MDS code satisfying $C_1^{\perp_h} \subseteq C_1$, and C_2 is a $[\frac{q^2-1}{2}, \frac{q^2-1}{2} - k, k+1]$ MDS code satisfying $C_2^{\perp_h} \subseteq C_2$. Obviously $Z_1 \subseteq Z_2$, and so $C_2 \subseteq C_1$ by Proposition 2.2, which implies that $C_1^{\perp_h} \subseteq C_2^{\perp_h}$. We then have $C_1^{\perp_h} \subseteq C_2$ and $C_2^{\perp_h} \subseteq C_1$. To complete the proof, we only need to prove that $d_x = wt(C_1 \setminus C_2^{\perp_h}) = wt(C_1) = t + 1$ and $d_z = wt(C_2 \setminus C_1^{\perp_h}) = wt(C_2) = k + 1$.

Note that $C_2^{\perp_h}$ is a $[\frac{q^2-1}{2}, k, \frac{q^2-1}{2} - k + 1]$ MDS code, which implies that the Hamming weights of all nonzero codewords of $C_2^{\perp_h}$ are greater than or equal to $\frac{q^2-1}{2} - k + 1$. On the other hand, $wt(C_1) = t + 1$ and $\frac{q^2-1}{2} - k + 1 > t + 1$ since $q \geq 5$. This gives that the codewords with Hamming weight $t + 1$ are not contained in $C_2^{\perp_h}$. Therefore, $d_x = wt(C_1 \setminus C_2^{\perp_h}) = wt(C_1) = t + 1$. Taking similar arguments, we have $d_z = wt(C_2 \setminus C_1^{\perp_h}) = wt(C_2) = k + 1$. Using the CSS construction, we know that there exist asymmetric quantum codes with parameters $[[\frac{q^2-1}{2}, \frac{q^2-1}{2} - t - k, (k+1)/(t+1)]]_{q^2}$. Further, $\frac{q^2-1}{2} - d_x - d_z + 2 = \frac{q^2-1}{2} - t - k$, which shows the desired result. □

Example 3.7. *Take $q = 11$, so $n = 60$. The following table lists some optimal asymmetric quantum codes derived from Theorem 3.6.*

Table 3: Optimal asymmetric quantum codes derived from Theorem 3.6

t	k	*asymmetric quantum optimal codes*
1	10	$[[60, 49, 11/2]]_{121}$
3	10	$[[60, 47, 11/4]]_{121}$
5	10	$[[60, 45, 11/6]]_{121}$
7	10	$[[60, 43, 11/8]]_{121}$
2	9	$[[60, 49, 10/3]]_{121}$
4	9	$[[60, 47, 10/5]]_{121}$
6	9	$[[60, 45, 10/7]]_{121}$
2	8	$[[60, 50, 9/3]]_{121}$
4	8	$[[60, 48, 9/5]]_{121}$
6	8	$[[60, 46, 9/7]]_{121}$
2	7	$[[60, 51, 8/3]]_{121}$
4	7	$[[60, 49, 8/5]]_{121}$
2	6	$[[60, 52, 7/3]]_{121}$

Acknowledgements The authors would like to sincerely thank the referees for a very meticulous reading of this manuscript, and for many valuable suggestions which help to create an improved version. The authors also deeply thank Dr. Martianus Frederic Ezerman for many helpful discussions. The first author is supported by NSFC (Grant No. 11171370), the Youth Backbone Teacher Foundation of

Henan's University (Grant No. 2013GGJS-152) and, Science and Technology Development Program of Henan Province in 2014 (144300510051). The research of the second author is partially supported by NSFC (Grant No. 11271005) and Nanyang Technological University's research grant number M4080456. The research of the third author is supported by NSFC (Grant No. 11301254) and the Natural Science Foundation of Henan Province (Grant No. 132300410313).

References

[1] A. M. Steane, Phys. Rev. A, **54** (1996) 4741.

[2] L. Ioffe, M. Mezard, Phys. Rev. A, **75** (2007) 032345(1).

[3] S.A. Aly, In: Proc. Computer Engineering and Systems, (2008) 157.

[4] P. K. Sarvepalli, M. Rotteler, A. Klappenecker, in Proc. ISIT, (2008) 305.

[5] P. K. Sarvepalli, M. Rotteler, A. Klappenecker, Proc. R. Soc. A, **465** (2009) 1645.

[6] S.A. Aly, A. Ashikhmin, In: IEEE Information Theory Workshop, (2010) 1.

[7] L. Wang, K. Feng, S. Ling, C. Xing, IEEE Trans. Inf. Theory., **56** (2010) 2938.

[8] Y. Chee, S. Jitman, M. F. Ezerman, 3rd Int. Castle Meeting on Coding Theory and Applications, (2011) 97.

[9] M. F. Ezerman, S. Ling, P. Sóle, IEEE Trans. Inf. Theory., **57** (2011) 5536.

[10] M. F. Ezerman, S. Ling, Adv. Math. Commun., **5** (2011) 41.

[11] G. G. La Guardia, Quantum Inf. Comput., **11** (2011) 0239.

[12] H. Q. Dinh, Finite Fields Appl., **18** (2012) 133.

[13] B. Chen, Y. Fan, L. Lin, H. Liu, Finite Fields Appl., **18** (2012) 1217.

[14] R. Leng and Z. Ma, Sci. China-Phys. Mech. Astron., **55** (2012) 465.

[15] J. Qian, L. Zhang, Mod. Phys. Lett. B, **26** (2012) 1250173.

[16] G. G. La Guardia, Quantum Inf. Process., **11** (2012) 591.

[17] J. Qian, L. Zhang, Mod. Phys. Lett. B, **27** (2013) 1350010.

[18] X. KaiM S. Zhu, IEEE Trans. Info. Theory, **59** (2013) 1193.

[19] Y. Yang, W. Cai, Designs, Codes and Crypt., (2013) DOI: 10.1007/s10623-013-9865-9.

[20] J. Chen, J. Li, J. Lin, Int. J. Theor. Phys., **53** (2014) 72.

[21] X. Kai, S. Zhu, and P. Li, IEEE Trans. Inf. Theory, (2014) DOI: 10.1109/TIT.2014.2308180.