Binary construction of quantum codes of minimum distances five and six *

Ruihu Li[(a)] and Xueliang Li[(b)]

[(a)]Department of Applied Mathematics and Physics, College of Science

Air Force Engineering University, Xi'an, Shaanxi 710051, P.R. China

E-mail: liruihu@yahoo.com.cn

[(b)]Center for Combinatorics and LPMC

Nankai University, Tianjin 300071, P.R. China

E-mail: lxl@nankai.edu.cn

Abstract

In this paper, we construct a large number of good quantum codes of minimum distances five and six by Steane's Construction. Our methods involve the study of the check matrices of binary extended BCH-codes, together with puncturing and combining such matrices.

Keywords: binary code, self-orthogonal code, quantum (error-correcting) code

1 Introduction

Quantum error-correcting codes (quantum codes, for short) have attracted much attention since their initial discovery [14], and various code constructions have been given in [1-12], [16-19] and [21-23]. A thorough discussion on the principles of quantum coding theory was given in [2] and [9], and in [2] many example codes were given, together with a tabulation of codes and bounds on the minimum distance for codeword length n up to 30 quantum bits. For larger n there has been less progress, and only a few general code constructions were known, see [1-12], [16-19] and [21-23]. In [19] Steane presented the *Steane's Construction* of additive quantum codes that use pairs of nested self-orthogonal binary codes (see Theorem 1.1 below), and he constructed some very good quantum codes from binary BCH-codes and extended BCH-codes. Quantum codes constructed by Steane's Construction are additive and pure. In the nomenclature of [7], an

*Supported by NSFC, the "973" project and a science research foundation of the Collage of Science of AFE University.

additive code is a *stabilizer code*, and a pure additive code is *nondegenerate*.

In this paper, we will generalize Steane's Construction in the special case of minimum distances five and six. In this section, we review Steane's Construction, introduce some definition and do some preparation for further discussion. In Section 2, we construct many matrix pairs, which are basic ingredients for constructing quantum codes. In Section 3, using the matrix pairs constructed in Section 2, we construct many quantum codes of minimum distances five and six by Steane's Construction. In the last section, we list our quantum codes of length $M < 1000$, and compare our codes with previous known ones.

Theorem 1.1 (Steane's Construction [19]) Let $\mathcal{C}$ and $\mathcal{C}'$ be binary $[N, k, d]$ and $[N, k_1, d_1]$ codes, respectively. If $\mathcal{C}^{\perp} \subset \mathcal{C} \subset \mathcal{C}'$ and $k_1 \geq k + 2$, then a quantum code $[[N, k + k_1 - N, min\{d, \lceil \frac{3}{2}d_1 \rceil\}]]$ can be constructed.

Definition 1.1 Let m be even, X be an $r \times m$ binary matrix and Y an $s \times m$ binary matrix. Let $\mathbf{1_m}$ be the all-ones vector of length m, and

$$H_1 = \begin{pmatrix} \mathbf{1_m} \\ X \\ Y \end{pmatrix}, H_2 = \begin{pmatrix} \mathbf{1_m} \\ X \end{pmatrix}, H_3 = \begin{pmatrix} X \\ Y \end{pmatrix}.$$

If the codes generated by H_1 and H_2 are all self-orthogonal, and their dual codes are $[m, m - r - s - 1, \geq 6]$ and $[m, m - r - 1, 4]$, respectively, then the binary matrix pair (X, Y) is called an $(m; r, s; 6, 4)$ *pair*. If, in addition, the dual codes of the codes generated by H_3 and X are $[m, m - r - s, \geq 5]$ and $[m, m - r, \geq 3]$, respectively, then the binary matrix pair (X, Y) is called a *strict* $(m; r, s; 6, 4)$ *pair*.

If there is an $(m; r, s; 6, 4)$ pair (X, Y), one can obtain a pair of nested self-orthogonal codes $\mathcal{C}^{\perp}\subset\mathcal{C}\subset\mathcal{C}'$, with $\mathcal{C}= [m, m - r - s - 1, \geq 6]$ and $\mathcal{C}'= [m, m - r - 1, 4]$; in addition, if (X, Y) is strict, there are also nested self-orthogonal codes $\mathcal{C}_1{}^{\perp}\subset\mathcal{C}_1\subset\mathcal{C}_1'$, such that $\mathcal{C}_1= [m, m - r - s - 1, \geq 5]$ and $\mathcal{C}_1'= [m, m - r - 1, \geq 3]$. To unify the statement of our results, we will use the terminology of $(m; r, s; 6, 4)$ *pair* rather than nested self-orthogonal codes in the following.

From Theorem 1.1, we have

Proposition 1.1 Let $s > 1$, if (X, Y) is an $(m; r, s; 6, 4)$ pair, then there is a quantum code $[[m, m - 2r - s - 2, 6]]$. If, in addition, (X, Y) is a strict $(m; r, s; 6, 4)$ pair, then there is also a quantum code $[[m, m - 2r - s, 5]]$.

Theorem 1.2 Let (X, Y) be an $(m; r, s; 6, 4)$ pair and (X_1, Y_1) an $(n; r_1, s_1; 6, 4)$ pair. If $r \leq r_1$ and $s \leq s_1$, then there is a quantum code $[[m + n, m + n - 2r_1 - s_1 - r - 4, 6]]$. In addition, if (X_1, Y_1) is strict, there is also a quantum code $[[m + n, m + n - 2r_1 - s_1 - r - 2, 5]]$. Especially, if $(X, Y) = (X_1, Y_1)$ is a strict $(m; r, s; 6, 4)$ pair, there are quantum codes $[[2m, 2m - 3r - s - 2, 5]]$ and $[[2m, 2m - 3r - s - 4, 6]]$.

Proof. To prove the theorem, it is sufficient to show that there is an $(m + n; r_1 + 1, s_1 + r; 6, 4)$ pair, and this pair is also strict when (X_1, Y_1) is strict.

Let

$$X_0 = \begin{pmatrix} X \\ \mathbf{0_{(r_1-r)\times m}} \end{pmatrix}, Y_0 = \begin{pmatrix} Y \\ \mathbf{0_{(s_1-s)\times m}} \end{pmatrix}.$$

Construct

$$K_1 = \begin{pmatrix} X_0 & X_1 \\ \mathbf{1_m} & \mathbf{0_{1\times n}} \end{pmatrix}, K_2 = \begin{pmatrix} Y_0 & Y_1 \\ X & \mathbf{0_{r\times n}} \end{pmatrix},$$

$$G_1 = \begin{pmatrix} \mathbf{1_{m+n}} \\ K_1 \\ K_2 \end{pmatrix} = \begin{pmatrix} \mathbf{1_m} & \mathbf{1_n} \\ X_0 & X_1 \\ \mathbf{1_m} & \mathbf{0_{1\times n}} \\ Y_0 & Y_1 \\ X & \mathbf{0_{r\times n}} \end{pmatrix}, G_2 = \begin{pmatrix} \mathbf{1_{m+n}} \\ K_1 \end{pmatrix} = \begin{pmatrix} \mathbf{1_m} & \mathbf{1_n} \\ X_0 & X_1 \\ \mathbf{1_m} & \mathbf{0_{1\times n}} \end{pmatrix}.$$

It is easy to check that $G_1 G_1^T = 0$ and $G_2 G_2^T = 0$. In the following, we will prove that (K_1, K_2) is an $(m+n; r_1+1, s_1+r; 6, 4)$ pair.

Let $\mathcal{C}_i$ be the self-orthogonal code generated by G_i for $1 \leq i \leq 2$. Notice that the columns of G_2 are obviously different, which implies that the minimum distance of $\mathcal{C}_2^{\perp}$ is at least three. From the first row of G_2, it follows that the minimum distance of $\mathcal{C}_2^{\perp}$ is even, and hence it is at least four. Similarly, if one can show that any four columns of G_1 are linearly independent, then it follows that the minimum distance of $\mathcal{C}_1^{\perp}$ is at least six.

To ease the proof, we reorder the rows of G_1 as G_3, where G_3 is

$$G_3 = \begin{pmatrix} \mathbf{1_m} & \mathbf{1_n} \\ X_0 & X_1 \\ Y_0 & Y_1 \\ \mathbf{1_m} & \mathbf{0_{1\times n}} \\ X & \mathbf{0_{r\times n}} \end{pmatrix}.$$

Let u_1, u_2, u_3, u_4 be four different columns of G_3. If they are all chosen from the first m columns or all from the last n columns of G_3, it is obvious that they are linearly independent. Otherwise, let $u_1, \cdots, u_i, 1 \leq i \leq 3$ be chosen from the first m columns and $u_{i+1}, \cdots, u_4$ from the last n columns of G_3. Since any three columns of

$$\begin{pmatrix} \mathbf{1_m} \\ X \end{pmatrix}$$

are linearly independent, and the last $r+1$ components of $u_{i+1}, \cdots, u_4$ are all 0, we get that u_1, u_2, u_3, u_4 are also linearly independent.

If, in addition, (X_1, Y_1) is strict, it is easy to check that (K_1, K_2) is also strict. Summarizing the above, the theorem follows. ∎

2 Construction of matrix pairs

In this section, we will study the check matrices of binary extended BCH-codes and use combining technique to construct new $(m; r, s; 6, 4)$ pair. Binary BCH-codes have been well discussed in existing literature, see [13]. Grassel et al. [11] derived the useful criterion that a BCH-code contains its dual. To unify the statement of our results, we give the following notation and lemma.

Let $(n, 2) = 1$, and s be an integer such that $0 \leq s < n$. The *2-cyclotomic coset* of s mod n is the set $C_s^{(2)} = \{s, 2s, 4s, ..., 2^{k-1}s\} \pmod{n}$, where k is the smallest positive integer such that $2^k s \equiv s \pmod{n}$. We call a 2-cyclotomic coset $C_s^{(2)}$ *symmetric* if $n - s \in C_s^{(2)}$, and *asymmetric* if otherwise. The asymmetric cosets appear in pairs $C_s^{(2)}$ and $C_{-s}^{(2)} = C_{n-s}^{(2)}$, and an *asymmetric coset pair* is denoted as $(C_s^{(2)}, C_{-s}^{(2)})$.

According to [11], we have the following lemma.

Lemma 2.1 Let $(n, 2) = 1$. If $(C_1^{(2)}, C_{-1}^{(2)})$ and $(C_3^{(2)}, C_{-3}^{(2)})$ are different asymmetric coset pairs of mod n, then the binary BCH-codes with length n and designed distances three and five contain their dual, and hence there is an $(n+1; \mid C_1^{(2)} \mid, \mid C_3^{(2)} \mid; 6, 4)$ pair that can be deduced from the related extended BCH-codes.

Let F_{2^r} be a finite field with 2^r elements and α be a primitive element of F_{2^r}. We use the notation $\alpha^{-\infty} = 0$ and $\alpha^0 = 1$. Then, $(\alpha^i)^k = \alpha^i$ for $i \in \{-\infty, 0\}$. Since $B = \{\alpha^0, \alpha, \cdots, \alpha^{r-1}\}$ is a base of F_{2^r} over F_2, any α^j can be represented as $\alpha^j = (\alpha^0, \alpha, ..., \alpha^{r-1})(a_{j1}, a_{j2}, \cdots, a_{jr})^T$ with $a_{ji} \in F_2$ for $1 \leq i \leq r$. The binary column vector $(a_{j1}, a_{j2}, \cdots, a_{jr})^T$ is called the *representation vector* of α^j with respect to the base B.

If $H = (\alpha^{k_1}, \alpha^{k_2}, \cdots, \alpha^{k_n})$ is an n-dimensional vector over F_{2^r}, then H can be represented as $H = (\alpha^0, \alpha, \cdots, \alpha^{r-1})A$, where A is a binary $r \times n$ matrix and

$$A = \begin{pmatrix} a_{k_1 1} & a_{k_2 1} & \cdots & a_{k_n 1} \\ a_{k_1 2} & a_{k_2 2} & \cdots & a_{k_n 2} \\ \cdots & \cdots & \cdots & \cdots \\ a_{k_1 r} & a_{k_2 r} & \cdots & a_{k_n r} \end{pmatrix}.$$

We call A the *representation matrix* of H with respect to the base B. Let $H(1, r)$ and $H(3, r)$ be the representation matrices of $(\alpha^{-\infty}, \alpha^0, \alpha, \cdots, \alpha^{2^r-2})$ and $(\alpha^{-\infty}, \alpha^0, \alpha^3, \cdots, \alpha^{3(2^r-2)})$ with respect to the base B, respectively. Let $n \mid (2^r - 1)$, $2^r - 1 = ns$. Since α is a primitive element of F_{2^r}, $\xi = \alpha^s$ is a primitive n-th root of unity. Let $H(1, r; n)$ and $H(3, r; n)$ be the representation matrices of $(\xi^{-\infty}, \xi^0, \xi, \cdots, \xi^{2^r-2}) = (\alpha^{-\infty}, \alpha^0, \alpha^s, \cdots, \alpha^{(2^r-2)s})$ and $(\xi^{-\infty}, \xi^0, \xi^3, \cdots, \xi^{3(2^r-2)}) = (\alpha^{-\infty}, \alpha^0, \alpha^{3s}, \cdots, \alpha^{3(2^r-2)s})$ with respect to the base B, respectively. Let

$$H_1 = \begin{pmatrix} \mathbf{1_{2^r}} \\ H(1,r) \end{pmatrix}, H_2 = \begin{pmatrix} \mathbf{1_{2^r}} \\ H(1,r) \\ H(3,r) \end{pmatrix}.$$

$$H_1^{'} = \begin{pmatrix} \mathbf{1_{n+1}} \\ H(1,r;n) \end{pmatrix}, H_2^{'} = \begin{pmatrix} \mathbf{1_{n+1}} \\ H(1,r;n) \\ H(3,r;n) \end{pmatrix}.$$

Then $H_1^{'}$ is a submatrix of H_1 and $H_2^{'}$ is a submatrix of H_2. From [13], we know that the codes with check matrices H_1 and H_2 are binary extended primitive BCH-codes with parameters $[2^r, 2^r - r - 1, 4]$ and $[2^r, 2^r - 2r - 1, 6]$, respectively. The codes with check matrices $H_1^{'}$ and $H_2^{'}$ are binary extended BCH-codes with parameters $[n+1, n - |C_1^{(2)}|, 4]$ and $[n+1, n- \mid C_1^{(2)} \mid - \mid C_3^{(2)} \mid, 6]$, respectively.

From [19] we know that if $5 \leq r \leq u$, then the primitive binary BCH-codes with designed distances three and five contain their dual, and hence $(H(1,r), H(3,r))$ is a $(2^r; r, r; 6, 4)$ pair and $(H(1,u), H(3,u))$ is a $(2^u; u, u; 6, 4)$ pair. Thus, using the results on BCH codes in [19] and combining Theorem 1.2, we have

Corollary 2.1 If $5 \leq r \leq u$, then there is a quantum code $[[2^r + 2^u, 2^r + 2^u - 3u - r - 4, 6]]$.

Using the above notations, we give the following two methods for constructing matrix pairs.

A. Construction of Matrix Pairs by Puncturing

Theorem 2.1 Let $n \mid (2^r - 1)$ and $r \geq 6$. If $(C_1^{(2)}, C_{-1}^{(2)})$ and $(C_3^{(2)}, C_{-3}^{(2)})$ are different asymmetric coset pairs of mod n, then there is a strict $(2^r - n - 1; r, r; 6, 4)$ pair, and hence there are quantum codes $[[2^r - n - 1, 2^r - n - 1 - 3r, 5]]$ and $[[2^r - n - 1, 2^r - n - 3 - 3r, 6]]$.

Proof. LetH_1 and H_2, $H_1^{'}$ and $H_2^{'}$ be as above. Since $r \geq 6$, the extended primitive BCH-codes with check matrices H_1 and H_2 all contain their dual. According to Lemma 2.1, since $(C_1^{(2)}, C_{-1}^{(2)})$ and $(C_3^{(2)}, C_{-3}^{(2)})$ are different asymmetric coset pairs of mod n, the extended binary BCH-codes with check matrices $H_1^{'}$ and $H_2^{'}$ also contain their dual. Thus, we have $H_i H_i^T = 0$ and $H_i^{'}(H_i^{'})^T = 0$ for $1 \leq i \leq 2$.

Delete the columns of $H(1,r;n)$ from $H(1,r)$ and denote the resulting matrix by $H(1,r;2^r - n - 1)$; delete the columns of $H(3,r;n)$ from $H(3,r)$ and denote the resulting matrix by $H(3,r;2^r - n - 1)$. It is easy to show that $(H(1,r;2^r - n - 1), H(3,r;2^r - n - 1))$ is a strict $(2^r - n - 1; r, r; 6, 4)$ pair. From Proposition 1.1, the theorem follows. ∎

From Corollary 1.1, Theorems 1.2 and 2.1, one can easily derive the following three corollaries.

(1) Let $r = 2k, k \geq 3$, $n_1(r) = \frac{2^r - 1}{3}$ and $N_1(r) = 2n_1(r) = 2^r - n_1(r) - 1$. It is easy to check that $(C_1^{(2)}, C_{-1}^{(2)})$ and $(C_3^{(2)}, C_{-3}^{(2)})$ are different asymmetric coset pairs of mod $n_1(r)$, and hence there is a strict $(N_1(r); r, r; 6, 4)$ pair. Thus we have

Corollary 2.2 If $r \geq 6$ is even, then there are quantum codes $[[N_1(r), N_1(r) - 3r, 5]]$, $[[N_1(r), N_1(r) - 3r - 2, 6]]$; $[[2^r + N_1(r), 2^r + N_1(r) - 4r - 2, 5]]$, $[[2^r + N_1(r), 2^r + N_1(r) - 4r - 4, 6]]$; $[[2N_1(r), 2N_1(r) - 4r - 2, 5]]$, $[[2N_1(r), 2N_1(r) - 4r - 4, 6]]$.

(2) Let $r = 3k, k \geq 3$, $n_2(r) = \frac{2^r-1}{7}$ and $N_2(r) = 6n_2(r)$. It is easy to check that $(C_1^{(2)}, C_{-1}^{(2)})$ and $(C_3^{(2)}, C_{-3}^{(2)})$ are different asymmetric coset pairs of mod $n_2(r)$, and hence there is a strict $(N_2(r); r, r; 6, 4)$ pair. Thus we have

Corollary 2.3 If $r = 3k, k \geq 3$, then there are quantum codes $[[N_2(r), N_2(r) - 3r, 5]]$, $[[N_2(r), N_2(r) - 3r - 2, 6]]$; $[[2^r + N_2(r), 2^r + N_2(r) - 4r - 2, 5]]$, $[[2^r + N_2(r), 2^r + N_2(r) - 4r - 4, 6]]$; $[[2N_2(r), 2N_2(r) - 4r - 2, 5]]$, $[[2N_2(r), 2N_2(r) - 4r - 4, 6]]$.

(3) Let $r = 4k, k \geq 3$, $n_3(r) = \frac{2^r-1}{5}$ and $N_3(r) = 4n_3(r)$. It is easy to check that $(C_1^{(2)}, C_{-1}^{(2)})$ and $(C_3^{(2)}, C_{-3}^{(2)})$ are different asymmetric coset pairs of mod $n_3(r)$, and hence there is a strict $(N_3(r); r, r; 6, 4)$ pair. Thus we have

Corollary 2.4 If $r = 4k, k \geq 3$, then there are quantum codes $[[N_3(r), N_3(r) - 3r, 5]]$, $[[N_3(r), N_3(r) - 3r - 2, 6]]$; $[[2^r + N_3(r), 2^r + N_3(r) - 4r - 2, 5]]$, $[[2^r + N_3(r), 2^r + N_3(r) - 4r - 4, 6]]$; $[[2N_3(r), 2N_3(r) - 4r - 2, 5]]$, $[[2N_3(r), 2N_3(r) - 4r - 4, 6]]$.

B. The $(a + x \mid b + x \mid a + b + x)$ Construction of Matrix Pairs

In [11] Sloane et al. used the $(a + x \mid b + x \mid a + b + x)$ construction to construct a family of binary codes with parameters $[3 \cdot 2^r, 3r + 3, 2^r]$. Now we use this method to construct $(3 \cdot 2^r; r + 2, 2r; 6, 4)$ matrix pair $(X_{3 \cdot 2^r}, Y_{3 \cdot 2^r})$ for $r \geq 3$ odd, and the code generated by

$$\begin{pmatrix} \mathbf{1}_{3\cdot 2^r} \\ X_{3\cdot 2^r} \\ Y_{3\cdot 2^r} \end{pmatrix}$$

has parameters $[3 \cdot 2^r, 3r + 3, 2^r]$.

Let $r \geq 3$ be odd. From [19] we know that if $r = 3$, the codes generated by

$$\begin{pmatrix} \mathbf{1}_8 \\ H(1,3) \end{pmatrix}, \begin{pmatrix} \mathbf{1}_8 \\ H(3,3) \end{pmatrix}$$

are all $[8, 4, 4]$ self-dual codes, and the dual code of the code generated by

$$\begin{pmatrix} \mathbf{1}_8 \\ H(1,3) \\ H(3,3) \end{pmatrix}$$

is the $[8,1,8]$ repetition code. While, if $r \geq 5$, then $(H(1,r), H(3,r))$ is a $(2^r; r, r; 6, 4)$ pair. Now we construct

$$X_{3\cdot 2^r} = \begin{pmatrix} H(1,r) & H(1,r) & H(1,r) \\ \mathbf{0_{1\times 2^r}} & \mathbf{1_{2^r}} & \mathbf{1_{2^r}} \\ \mathbf{1_{2^r}} & \mathbf{0_{1\times 2^r}} & \mathbf{1_{2^r}} \end{pmatrix}, Y_{3\cdot 2^r} = \begin{pmatrix} \mathbf{0_{1\times 2^r}} & H(3,r) & H(3,r) \\ H(3,r) & \mathbf{0_{1\times 2^r}} & H(3,r) \end{pmatrix}.$$

Similar to the discussion of Theorem 1.2, we can prove that $(X_{3\cdot 2^r}, Y_{3\cdot 2^r})$ is a $(3\cdot 2^r; r+2, 2r; 6, 4)$ pair. Thus we have

Corollary 2.5 If $r \geq 3$ is odd, then there is a quantum code $[[3\cdot 2^r, 3\cdot 2^r - 4r - 6, 6]]$.

Let D_0, D_1, D_2, C_1 and C_2 be the codes generated by $\mathbf{1_{2^r}}$, K_1, K_2, L_1 and L_2, respectively, where

$$K_1 = \begin{pmatrix} \mathbf{1_{2^r}} \\ H(1,r) \end{pmatrix}, K_2 = \begin{pmatrix} \mathbf{1_{2^r}} \\ H(3,r) \end{pmatrix}, L_1 = \begin{pmatrix} \mathbf{1_{3\cdot 2^r}} \\ X_{3\cdot 2^r} \end{pmatrix}, L_2 = \begin{pmatrix} \mathbf{1_{2^r}} \\ X_{3\cdot 2^r} \\ Y_{3\cdot 2^r} \end{pmatrix}.$$

It is easy to check that any $c_1 \in C_1$ can be represented as $c_1 = (a_1 + x_1 \mid b_1 + x_1 \mid a_1 + b_1 + x_1)$, where $a_1, b_1 \in D_0$ and $x_1 \in D_1$; and any $c_2 \in C_2$ can be represented as $c_2 = (a_2 + x_2 \mid b_2 + x_2 \mid a_2 + b_2 + x_2)$ where $a_2, b_2 \in D_2$ and $x_2 \in D_1$.

3 Construction of quantum codes

In Section 2 we gave the following five kinds of matrix pairs: $(2^r; r, r; 6, 4)$ pair, $(N_i(r); r, r; 6, 4)$ pairs for $1 \leq i \leq 3$, and $(3\cdot 2^r; r+2, 2r; 6, 4)$ pair. In this section we use these matrix pairs to construct quantum codes. According to Theorem 1.2, we will combine an $(m; r, s; 6, 4)$ pair and an $(n; u, v; 6, 4)$ pair, such that $r \leq u$ and $s \leq v$, to obtain an $(m+n; a, b; 6, 4)$ pair for suitable a and b. The proofs of the following theorems are trivial and thus omitted.

Theorem 3.1 Let $5 \leq t \leq r$.
(1) if r is even, there are quantum codes $[[2^t + N_1(r), 2^t + N_1(r) - 3r - t - 2, 5]]$, $[[2^t + N_1(r), 2^t + N_1(r) - 3r - t - 4, 6]]$.
(2) if $r = 3k$, $k \geq 3$, there are quantum codes $[[2^t + N_2(r), 2^t + N_2(r) - 3r - t - 2, 5]]$, $[[2^t + N_2(r), 2^t + N_2(r) - 3r - t - 4, 6]]$.
(3) if $r = 4h$, $h \geq 3$, there are quantum codes $[[2^t + N_3(r), 2^t + N_3(r) - 3r - t - 2, 5]]$, $[[2^t + N_3(r), 2^t + N_3(r) - 3r - t - 4, 6]]$.

Theorem 3.2 Let $6 \leq r \leq u$ and r be even. Then there is a quantum code $[[N_1(r) + 2^u, N_1(r) + 2^u - 3u - r - 4, 6]]$. In addition,
(1) if u is even, there are quantum codes $[[N_1(r) + N_1(u), N_1(r) + N_1(u) - 3u - r - 2, 5]]$, $[[N_1(r) + N_1(u), N_1(r) + N_1(u) - 3u - r - 4, 6]]$;
(2) if $u = 3k$, $k \geq 3$, there are quantum codes $[[N_1(r) + N_2(u), N_1(r) + N_2(u) - 3u - r - 2, 5]]$, $[[N_1(r) + N_2(u), N_1(r) + N_2(u) - 3u - r - 4, 6]]$;
(3) if $u = 4h$, $h \geq 3$, there are quantum codes $[[N_1(r) + N_3(u), N_1(r) + N_3(u) - 3u - r - 2, 5]]$, $[[N_1(r) + N_3(u), N_1(r) + N_3(u) - 3u - r - 4, 6]]$.

Theorem 3.3 Let $9 \le r \le u$ and $r = 3l$. Then there is a quantum code $[[N_2(r) + 2^u, N_2(r) + 2^u - 3u - r - 4, 6]]$. In addition,
(1) if u is even, there are quantum codes $[[N_2(r) + N_1(u), N_2(r) + N_1(u) - 3u - r - 2, 5]]$, $[[N_2(r) + N_1(u), N_2(r) + N_1(u) - 3u - r - 4, 6]]$;
(2) if $u = 3k$, $k \ge 3$, there are quantum codes $[[N_2(r) + N_2(u), N_2(r) + N_2(u) - 3u - r - 2, 5]]$, $[[N_2(r) + N_2(u), N_2(r) + N_2(u) - 3u - r - 4, 6]]$;
(3) if $u = 4h$, $h \ge 3$, there are quantum codes $[[N_2(r) + N_3(u), N_2(r) + N_3(u) - 3u - r - 2, 5]]$, $[[N_2(r) + N_3(u), N_2(r) + N_3(u) - 3u - r - 4, 6]]$.

Theorem 3.4 Let $12 \le r \le u$ and $r = 4l$. Then there is a quantum code $[[N_3(r) + 2^u, N_3(r) + 2^u - 3u - r - 4, 6]]$. In addition,
(1) if u is even, there are quantum codes $[[N_3(r) + N_1(u), N_3(r) + N_1(u) - 3u - r - 2, 5]]$, $[[N_3(r) + N_1(u), N_3(r) + N_1(u) - 3u - r - 4, 6]]$;
(2) if $u = 3k$, $k \ge 3$, there are quantum codes $[[N_3(r) + N_2(u), N_3(r) + N_2(u) - 3u - r - 2, 5]]$, $[[N_3(r) + N_2(u), N_3(r) + N_2(u) - 3u - r - 4, 6]]$;
(3) if $u = 4h$, $h \ge 3$, there are quantum codes $[[N_3(r) + N_3(u), N_3(r) + N_3(u) - 3u - r - 2, 5]]$, $[[N_3(r) + N_3(u), N_3(r) + N_3(u) - 3u - r - 4, 6]]$.

Using the $(24; 5, 6; 6, 4)$ pair (X_{24}, Y_{24}) constructed in Section 2.B for $r = 3$, we have

Theorem 3.5 Let $r \ge 6$. Then there is a quantum code $[[24 + 2^r, 24 + 2^r - 3r - 9, 6]]$. In addition,
(1) if r is even, there are quantum codes $[[24 + N_1(r), 24 + N_1(r) - 3r - 7, 5]]$ $[[24 + N_1(r), 24 + N_1(r) - 3r - 9, 6]]$;
(2) if $r = 3l, l \ge 3$, there are quantum codes $[[24 + N_2(r), 24 + N_2(r) - 3r - 7, 5]]$, $[[24 + N_2(r), 24 + N_2(r) - 3r - 9, 6]]$;
(3) if $r = 4k, k \ge 3$, there are quantum codes $[[24 + N_3(r), 24 + N_3(r) - 3r - 7, 5]]$, $[[24 + N_3(r), 24 + N_3(r) - 3r - 9, 6]]$.

Remark. For $r = 5$, using the $(32; 5, 5; 6, 4)$ matrix pairs $(H(1, 5), H(3, 5))$ and (X_{24}, Y_{24}), we can obtain quantum code [[56,31,6]].

4 Concluding remarks

Definition 1.1 for $(m; r, s; 6, 4)$ pair can be generalized to any $(m; r, s; 2a, 2b)$ pair with $a > b$, and the method of combining two pairs to obtain the third pair in Theorem 1.2 can also be generalized, which will be discussed in another paper.

As one of the referees pointed out, our puncturing technique in Theorem 2.1 is a particular case of the puncturing technique by Rains in [22]. Actually, the CSS code used in Theorem 2.1 can be obtained via Rains puncturing technique from a code of length 2^r. The only requirement is that after deleting some positions, the resulting code is contained in its dual. Deleting the coordinates corresponding to some n-th root of unity is just one choice. The result of Theorem 2.1 then follows using Steane's enlargement technique. Nevertheless, our puncturing technique is easily understandable, and it is easy to check that the codes constructed by our technique contain their dual, and the minimum distances of the codes can be easily determined.

From [19] we know that the quantum codes constructed in Sections 2 and 3 are additive and pure. Thus, according to Theorem 6 (b) of [2], we know that for each $[[M, K, 6]]$ code constructed in these two sections, there is an additive quantum code $[[M-1, K+1, 5]]$. We call the quantum code $[[M-1, K+1, 5]]$ *induced quantum code* of $[[M, K, 6]]$.

For convenience, we collect our quantum codes $[[M, K, D]]$ for even $M < 1000$ in Table 1, but omit the corresponding induced codes. If by using different corollaries or theorems, we can construct $[[M, K, D]]$ and $[[M, K_1, D]]$ with $K < K_1$, then in Table 1 we only list a better one. The length M is a function of r or r, u, etc. So we call r or r, u, etc. the variables of M.

Almost all of the quantum codes in Table 1 are new, and some of our quantum codes in Table 1 and the corresponding induced codes are better than or comparable with previously known codes quoted in [2], [15-16] and [20]. For example, the [[23,7,5]] and [[24,6,6]] codes fill the existence lower bounds in [2], the codes [[74,47,6]] and [[106,78,6]] are better than the codes [[74,45,6]] and [[106,68,6]] quoted in [19-20].

Table 1 Quantum codes $[[M, K, D]]$ for even $M < 1000$.

type of M	quantum codes	corollary or theorem	variables of M
$3 \cdot 2^r$	$[[24, 6, 6]]$	Cor. 2.5	$r = 3$
$N_1(r)$	$[[42, 24, 5]]$	Cor. 2.2	$r = 6$
$N_1(r)$	$[[42, 22, 6]]$	Cor.2.2	$r = 6$
$2^t + N_1(r)$	$[[74, 49, 5]]$	Th. 3.1	$t = 5, r = 6$
$2^t + N_1(r)$	$[[74, 47, 6]]$	Th. 3.1	$t = 5, r = 6$
$24 + 2^r$	$[[88, 61, 6]]$	Th. 3.5	$r = 6$
$3 \cdot 2^r$	$[[96, 70, 6]]$	Cor. 2.5	$r = 5$
$2^r + N_1(r)$	$[[106, 80, 5]]$	Cor. 2.2	$r = 6$
$2^r + N_1(r)$	$[[106, 78, 6]]$	Cor. 2.2	$r = 6$
$24 + 2^r$	$[[152, 122, 6]]$	Th. 3.5	$r = 7$
$2^r + 2^u$	$[[160, 130, 6]]$	Cor. 2.1	$r = 5, u = 7$
$N_1(r)$	$[[170, 146, 5]]$	Cor. 2.2	$r = 8$
$N_1(r)$	$[[170, 144, 6]]$	Cor. 2.2	$r = 8$
$2^r + 2^u$	$[[192, 161, 6]]$	Cor. 2.1	$r = 6, u = 7$
$2^t + N_1(r)$	$[[202, 171, 5]]$	Th. 3.1	$t = 5, r = 8$
$2^t + N_1(r)$	$[[202, 169, 6]]$	Th. 3.1	$t = 5, r = 8$
$N_1(r) + N_1(u)$	$[[212, 180, 5]]$	Th. 3.2	$r = 6, u = 8$
$N_1(r) + N_1(u)$	$[[212, 178, 6]]$	Th. 3.2	$r = 6, s = 8$
$2^t + N_1(r)$	$[[234, 202, 5]]$	Th. 3.1	$t = 6, r = 8$
$2^t + N_1(r)$	$[[234, 200, 6]]$	Th. 3.1	$r = 6, s = 8$

Table 1(Continued) Quantum codes $[[M, K, D]]$ for even $M < 1000$.

type of M	quantum codes	corollary or theorem	variables of M
$24 + 2^r$	$[[280, 247, 6]]$	Th. 3.5	$r = 8$
$2^r + 2^u$	$[[288, 255, 6]]$	Cor. 2.1	$r = 5, u = 8$
$N_1(r) + 2^u$	$[[298, 264, 6]]$	Th 3.2	$r = 6, u = 8$
$2^r + 2^u$	$[[320, 286, 6]]$	Cor. 2.1	$r = 6, u = 8$
$3 \cdot 2^r$	$[[384, 350, 6]]$	Cor. 2.5	$r = 7$
$2^r + N_1(r)$	$[[426, 392, 5]]$	Cor. 2.2	$r = 8$
$2^r + N_1(r)$	$[[426, 390, 6]]$	Cor. 2.2	$r = 8$
$N_2(r)$	$[[438, 411, 5]]$	Cor. 2.3	$r = 9$
$N_2(r)$	$[[438, 409, 6]]$	Cor. 2.3	$r = 9$
$24 + N_2(r)$	$[[462, 428, 5]]$	Th. 3.5	$r = 9$
$24 + N_2(r)$	$[[462, 426, 6]]$	Th. 3.5	$r = 9$
$2^t + N_2(r)$	$[[470, 436, 5]]$	Th. 3.1	$t = 5, r = 9$
$2^t + N_2(r)$	$[[470, 434, 6]]$	Th. 3.1	$t = 5, r = 9$
$N_1(r) + N_2(u)$	$[[480, 445, 5]]$	Th. 3.2	$r = 6, u = 9$
$N_1(r) + N_2(u)$	$[[480, 443, 6]]$	Th. 3.2	$r = 6, u = 9$
$2^t + N_2(r)$	$[[502, 467, 5]]$	Th. 3.1	$t = 6, r = 9$
$2^t + N_2(r)$	$[[502, 465, 6]]$	Th. 3.1	$t = 6, r = 9$
$24 + 2^r$	$[[536, 500, 6]]$	Th. 3.5	$r = 9$
$2^r + 2^u$	$[[544, 508, 6]]$	Cor. 2.1	$r = 5, u = 9$
$N_1(r) + 2^u$	$[[554, 517, 6]]$	Th 3.2	$r = 6, u = 9$
$2^t + N_2(r)$	$[[566, 530, 5]]$	Th. 3.1	$t = 7, r = 9$
$2^t + N_2(r)$	$[[566, 528, 6]]$	Th. 3.1	$t = 7, r = 9$
$2^r + 2^u$	$[[576, 539, 6]]$	Cor. 2.1	$r = 6, u = 9$
$N_1(r) + N_2(u)$	$[[608, 571, 5]]$	Th. 3.2	$r = 8, u = 9$
$N_1(r) + N_2(u)$	$[[608, 569, 6]]$	Th. 3.2	$r = 8, u = 9$
$2^r + 2^u$	$[[640, 602, 6]]$	Cor. 2.1	$r = 7, u = 9$
$N_1(r)$	$[[682, 652, 5]]$	Cor. 2.2	$r = 10$
$N_1(r)$	$[[682, 650, 6]]$	Cor. 2.2	$r = 10$
$2^t + N_2(r)$	$[[694, 657, 5]]$	Th. 3.1	$t = 8, r = 9$
$2^t + N_2(r)$	$[[694, 655, 6]]$	Th. 3.1	$t = 8, r = 9$
$24 + N_1(r)$	$[[706, 669, 5]]$	Th. 3.5	$r = 10$
$24 + N_1(r)$	$[[706, 667, 6]]$	Th. 3.5	$r = 10$
$2^t + N_1(r)$	$[[714, 677, 5]]$	Th. 3.1	$t = 5, r = 10$
$2^t + N_1(r)$	$[[714, 675, 6]]$	Th. 3.1	$t = 5, r = 10$
$N_1(r) + N_1(u)$	$[[724, 686, 5]]$	Th. 3.2	$r = 6, u = 10$
$N_1(r) + N_1(u)$	$[[724, 684, 6]]$	Th. 3.2	$r = 6, u = 10$
$2^t + N_1(r)$	$[[746, 708, 5]]$	Th. 3.1	$t = 6, r = 10$
$2^t + N_1(r)$	$[[746, 706, 6]]$	Th. 3.1	$t = 6, r = 10$
$2^r + 2^u$	$[[768, 729, 6]]$	Cor. 2.1	$r = 8, u = 9$
$2^t + N_1(r)$	$[[810, 771, 5]]$	Th. 3.1	$t = 7, r = 10$
$2^t + N_1(r)$	$[[810, 769, 6]]$	Th. 3.1	$r = 7, s = 10$
$N_1(r) + N_1(u)$	$[[852, 812, 5]]$	Th. 3.2	$r = 8, u = 10$
$N_1(r) + N_1(u)$	$[[852, 810, 6]]$	Th. 3.2	$r = 8, u = 10$

Table 1(Continued) Quantum codes $[[M, K, D]]$ for even $M < 1000$.

type of M	quantum codes	corollary or theorem	variables of M
$2N_2(r)$	$[[876, 838, 5]]$	Cor. 2.3	$r = 9$
$2N_2(r)$	$[[876, 836, 6]]$	Cor. 2.3	$r = 9$
$2^t + N_1(r)$	$[[938, 898, 5]]$	Th. 3.1	$t = 8, r = 10$
$2^t + N_1(r)$	$[[938, 896, 6]]$	Th. 3.1	$t = 8, r = 10$
$2^r + N_2(r)$	$[[950, 912, 5]]$	Cor. 2.3	$r = 9$
$2^r + N_2(r)$	$[[950, 910, 6]]$	Cor. 2.3	$r = 9$

Acknowledgement. The authors are very grateful to the anonymous referees for their valuable comments and suggestions, which help to improve the manuscript significantly.

References

[1] J. Bierbrauer and Y. Edel, Quantum twisted codes, J. Combin. Designs 8(2000), 174-188.

[2] 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.

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

[4] G. Cohen, S. Encheva and S. Litsyn, On binary construction of quantum codes, IEEE. Trans. Inform. Theory 45(1999), 2495-2498.

[5] H. Chen, Some good quantum error-correcting codes from algebraic geometric codes, IEEE. Trans. Inform. Theory 47(2001), 2059-2061.

[6] H. Chen, S. Ling and C.P. Xing, Quantum codes from concatenated algebraic geometric codes, Preprint 2001.

[7] D. Gottesman, Class of quantum error-correcting codes saturating the quantum Hamming bound, Phys. Rev. A 54(1996), 1862-1868.

[8] D. Gottesman, Pasting quantum codes, arXiv: quant-ph/9607027, 1996.

[9] D. Gottesman, Stabilizer codes and quantum error correction, arXiv: quant-ph/9705052, 1997.

[10] D. Gottesman, An introduction to quantum error correction, arXiv: quant-ph/0004072, 2000.

[11] M. Grassl, T. Beth and T. Pellizzari, Codes for the quantum erasure channel, Phys. Rev. A 56(1997), 33-38.

[12] M. Grassl and T. Beth, Quantum BCH codes, arXiv: quant-ph/9910060, 1999

[13] F.J. MacWillams and N.J.A. Sloane, The Theory of Error-Correcting Codes, Amsterdam, The Netherlands: North-Holland, 1977.

[14] P.W. Shor, Scheme for reducing decoherence in quantum computer memory, Phys. Rev. A 52(1995), 2493-2496.

[15] N.J.A. Sloane, S.M. Reddy and C.L. Chen, New binary codes, IEEE. Trans. Inform. Theory 18(1972), 503-510.

[16] A.M. Steane, Multiple particle interference and quantum error correction, Proc. Roy. Soc. London A 452(1996), 2551-2577.

[17] A.M. Steane, Error correcting codes in quantum theory, Phys. Rev. Lett 77(1996), 793-797.

[18] A.M. Steane, Quantum Reed-Muller codes, IEEE. Trans. Inform. Theory 45(1999), 1701-1703.

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

[20] http://www.mathi.uni-heidelberg/∼ yves/matritzen/QTBCH/QTBCHTab2.html

[21] M. Grassl and T. Beth and M. Roetteler, On optimal quantum codes, International Journal of Quantum Information 2(1)(2004), 55-64. arXiv: quant-ph/0312164, 2003

[22] E.M. Rains, Nonbinary quantum codes, IEEE Transactions on Information Theory 45(6)(1999), 1827-1832. arXiv: quant-ph/9703048, 1997

[23] A. Ashikhmin, S. Litsyn, and M.A. Tsfasman, Asymptotically good quantum codes, Physical Review A 63(2001). arXiv: quant-ph/0006061.