International Journal of Quantum Information
Vol. 4, No. 6 (2006) 1–7

World Scientific
www.worldscientific.com

# LINEAR QUANTUM CODES OF MINIMUM DISTANCE THREE

RUIHU LI[*,†,§], XUELIANG LI[‡,¶] and ZONGBEN XU[*,||]

[*]*College of Science, Xi'an Jiaotong University, Shaanxi 710049, People's Republic of China,*
[§]*liruihu@yahoo.com.cn*

[†]*Department of Applied Mathematics and Physics, College of Science, Air Force Engineering University Xi'an, Shaanxi 710051, People's Republic of China*
[¶]*x.li@eyou.com*

[‡]*Center for Combinatorics, Nankai University, Tianjin 300071, People's Republic of China,*
[||]*zbxu@mail.xjtu.edu.cn*

Received 12 November 2005
Revised 2 July 2006

We give elementary recursive constructions of quaternary self-orthogonal codes with dual distance three for all $n \geq 5$. Consequently, good linear quantum codes of minimum distance three for such length $n$ are obtained. Almost all of these linear quantum codes are optimal or near optimal.

*Keywords*: Quaternary code; self-orthogonal code; linear quantum error correcting code.

## 1. Introduction

It is an important problem to construct $[[n, k, d]]$ quantum code with $k$ maximal for given code length $n$ and minimum distance $d$. In Refs. 1–3, Gottesman, and Calderbank *et al.* proved that when $n$ is a power of 2 or sums of odd power of 2, or sums of even power of 2, there exists an $[[n, n-m-2, 3]]$ quantum code for certain $m$, see Theorem 1.2 below. In Ref. 4, we generalized their result to all even $n \geq 12$ and $n = 8$ via Steane's construction. In this paper, we will use quaternary self-orthogonal codes to construct $[[n, k, 3]]$ quantum codes for all $n \geq 5$, and improve the parameters of some near optimal codes obtained in Ref. 4.

Let $F_4 = \{0, 1, \omega, \varpi\}$ be the Galois field with four elements such that $\varpi = 1 + \omega = \omega^2, \omega^3 = 1$, and the conjugation is defined by $\bar{x} = x^2$. The Hermitian inner product of $\mathbf{u}$, $\mathbf{v} \in F_4^n$ is defined to be

$$(\mathbf{u}, \mathbf{v}) = \mathbf{u}\mathbf{v}^\dagger = u_1\bar{v_1} + u_2\bar{v_2} + \cdots + u_n\bar{v_n}.$$

From now on, orthogonality over $F_4^n$ will be with respect to the Hermitian inner product defined above. And we use $\mathbf{1_n}=(1, 1, \ldots, 1)_{1\times n}$ to denote the all-one vector of length $n$, and $H^\dagger = \bar{H}^{\mathrm{T}}$ to denote the conjugate transpose of $H$ for any matrix or vector $H$ over $F_4$. Theorem 1.1 from Ref. 1 can be used directly to obtain quantum codes from certain codes over $F_4$.

**Theorem 1.1 [1].** *Suppose $\mathcal{C}$ is an $[n, k]$ linear self-orthogonal code over $F_4$. Suppose also that the minimal weight of $\mathcal{C}^\perp \setminus \mathcal{C}$ is $d$. Then, an $[[n, n-2k, d]]$ quantum code can be obtained from $\mathcal{C}$.*

Note that such a quantum code is called a *linear quantum code* according to Ref. 1, and the self-orthogonal code $\mathcal{C}$ is called the *associated code* of this linear quantum code. If the minimum distance of $\mathcal{C}^\perp$ is $d$, then the $[[n, n-2k, d]]$ code is *pure* in the nomenclature of Ref. 1 and *nondegenerate* in the nomenclature of Ref. 2.

**Theorem 1.2.**

(1) ([1][2]) *For $m \geq 3$, there exists a $[[2^m, 2^m - m - 2, 3]]$ code.*
(2) ([1][3]) *For $m \geq 2$, there exists an $[[n, n-m-2, 3]]$ code, where $n$ is $n = \sum_{0\leq i\leq \frac{m}{2}} 2^{2i}$ for even $m$, and $n = \sum_{1\leq i\leq \frac{(m-1)}{2}} 2^{2i+1}$ for odd $m$.*

Our constructions are based on the following easily proved lemma, first we give a definition.

**Definition 1.1.** Let $\mathbf{v}$ be an $m$-dimensional column vector over $F_4$, if the first non-zero component of $\mathbf{v}$ is 1, then $\mathbf{v}$ is called a monic column vector.

**Lemma 1.1.** *Let $H_n$ be a $k \times n$ matrix of rank $k$ such that*

$$H_n = \begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_{n-1} & \alpha_n \end{pmatrix}.$$

*If $H_n H_n^\dagger = \mathbf{0}$ and the $k$-dimensional column vectors $\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, \alpha_n$ are all different and monic, then $\mathcal{C}_n = \langle H_n \rangle$ is self-orthogonal and $\mathcal{C}_n^\perp = [n, n-k, 3]$.*

According to the sphere-packing bound given in Refs. 1 and 2, we give a reasonable definition and an obvious proposition in the following, so that in concluding remarks we can evaluate the optimality of the quantum codes we obtain.

**Definition 1.2.** (1) A pure quantum code $[[n, n-s, 2t+1]]$ is called *optimal* if there do not exist pure $[[n, n-s+1, 2t+1]]$ and $[[n, n-s, 2t+3]]$ codes.
(2) A pure quantum code $[[n, n-s, 2t+1]]$ is called *near optimal* if there do not exist pure $[[n, n-s+2, 2t+1]]$ and $[[n, n-s, 2t+3]]$ codes.

**Proposition 1.1.** (1) *If* $2^{s-1} < 1+3n \leq 2^s < 1+3n+\frac{9n(n-1)}{2}$, *then a pure quantum code* $[[n, n-s, 3]]$ *is optimal.*
(2) *If* $2^{s-2} < 1+3n \leq 2^s < 1+3n+\frac{9n(n-1)}{2}$, *then a pure quantum code* $[[n, n-s, 3]]$ *is near optimal.*

## 2. Codes Construction

Let $N_m = \frac{4^m-1}{3}$ for $m \geq 2$, and $U_m = 4^{m-3}$ for $m \geq 3$. It is obvious that the number of different $m$-dimensional monic column vectors over $F_4$ is $N_m$. We use all such vectors to form a matrix and denote it as $H_{m,N_m}$, then $H_{m,N_m}$ is the parity check matrix of $[N_m, N_m - m, 3]$ Hamming code over $F_4$.

Since $N_{m+1} = 4N_m + 1$, using a recursive step, we can construct $H_{m+1,N_{m+1}}$ from $H_{m,N_m}$ as

$$H_{m+1,N_{m+1}} = \begin{pmatrix} \mathbf{0_{m\times 1}} & H_{m,N_m} & H_{m,N_m} & H_{m,N_m} & H_{m,N_m} \\ 1 & \mathbf{0_{N_m}} & \mathbf{1_{N_m}} & \omega\mathbf{1_{N_m}} & \varpi\mathbf{1_{N_m}} \end{pmatrix}.$$

According to Ref. 1, we know that $H_{m,N_m}H^{\dagger}_{m,N_m} = \mathbf{0}$. Generally, we have the following lemma.

**Lemma 2.1.** *Let* $N_m = \frac{4^m-1}{3}$ *for* $m \geq 2$, *and* $U_m = 4^{m-3}$ *for* $m \geq 3$.

(1) *For* $m \geq 2$, *the rank of* $H_{m,N_m}$ *is* $m$ *and* $H_{m,N_m}H^{\dagger}_{m,N_m} = \mathbf{0}$.
(2) *For* $m \geq 3$, $H_{m,N_m}$ *has a sub-matrix* $G_{m,10i}$ *such that* $G_{m,10i}G^{\dagger}_{m,10i} = \mathbf{0}$ *and* $G_{m,10i}\mathbf{1_{10i}}^{\dagger} = \mathbf{0}$ *for* $1 \leq i \leq U_m$.
(3) *For* $m \geq 4$ *and* $1 \leq i \leq \frac{3}{4}U_m$, $H_{m,N_m}$ *has a sub-matrix* $G_{m,10i}$ *such that* $G_{m,10i}G^{\dagger}_{m,10i} = \mathbf{0}$ *and* $G_{m,10i}\mathbf{1_{10i}}^{\dagger} = \mathbf{0}$, *and each component of the last row of* $G_{m,10i}$ *is not zero.*

**Proof.** From Ref. 1 we know that (1) is correct. To prove (2) and (3), we use induction on $m$. Let

$$G_{3,10} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & \omega & \varpi & \omega & \varpi \\ 0 & 1 & 0 & 1 & \omega & \varpi & 1 & 1 & \varpi & \omega \end{pmatrix}.$$

It is easy to check that $G_{3,10}G^{\dagger}_{3,10} = \mathbf{0}$ and $G_{3,10}\mathbf{1_{10}}^{\dagger} = \mathbf{0}$.

For $m = 4$, let

$$G_{4,10} = \begin{pmatrix} G_{3,10} \\ \mathbf{1_{10}} \end{pmatrix}, \quad G_{4,20} = \begin{pmatrix} G_{3,10} & G_{3,10} \\ \mathbf{1_{10}} & \omega\mathbf{1_{10}} \end{pmatrix},$$

$$G_{4,30} = \begin{pmatrix} G_{3,10} & G_{3,10} & G_{3,10} \\ \mathbf{1_{10}} & \omega\mathbf{1_{10}} & \varpi\mathbf{1_{10}} \end{pmatrix}, \quad G_{4,40} = \begin{pmatrix} G_{3,10} & G_{3,10} & G_{3,10} & G_{3,10} \\ \mathbf{0_{1\times 10}} & \mathbf{1_{10}} & \omega\mathbf{1_{10}} & \varpi\mathbf{1_{10}} \end{pmatrix}.$$

Thus, the lemma holds for $m = 3, 4$.

Suppose the lemma holds for $m(\geq 4)$. Now we prove that the lemma also holds for $m+1$.

If $1 \leq i \leq U_m$, construct

$$G_{m+1,10i} = \begin{pmatrix} G_{m,10i} \\ \mathbf{1_{10i}} \end{pmatrix}.$$

If $U_m + 1 \leq i \leq 2U_m$, let $i_1 = i - U_m$ and construct

$$G_{m+1,10i} = \begin{pmatrix} G_{m,10U_m} & G_{m,10i_1} \\ \mathbf{1_{10U_m}} & \omega \mathbf{1_{10i_1}} \end{pmatrix}.$$

If $2U_m + 1 \leq i \leq 3U_m$, let $i_2 = i - 2U_m$ and construct

$$G_{m+1,10i} = \begin{pmatrix} G_{m,10U_m} & G_{m,10U_m} & G_{m,10i_2} \\ \mathbf{1_{10U_m}} & \omega \mathbf{1_{10U_m}} & \varpi \mathbf{1_{10i_2}} \end{pmatrix}.$$

If $3U_m + 1 \leq i \leq U_{m+1}$, let $i_3 = i - 3U_m$ and construct

$$G_{m+1,10i} = \begin{pmatrix} G_{m,10i_3} & G_{m,10U_m} & G_{m,10U_m} & G_{m,10U_m} \\ \mathbf{0_{1\times 10i_3}} & \mathbf{1_{10U_m}} & \omega \mathbf{1_{10U_m}} & \varpi \mathbf{1_{10U_m}} \end{pmatrix}.$$

According to the induction hypothesis, we can deduce that $G_{m+1,10j} G^{\dagger}_{m,10j} = \mathbf{0}$ and $G_{m+1,10j} \mathbf{1_{10j}}^{\dagger} = \mathbf{0}$ for $1 \leq j \leq U_{m+1}$, and each component of the last row of $G_{m,10i}$ is not zero when $1 \leq j \leq \frac{3}{4} U_{m+1}$. Thus, the lemma follows. □

In the rest of this section, we will say that the minimum distance of a linear quantum code is three even if its actual distance is more than three. We use $H_{m,n}$ to denote any sub-matrix of $H_{m,N_m}$ satisfying $H_{m,n} H^{\dagger}_{m,n} = \mathbf{0}$, and $H_{m,10i}$ also satisfying $H_{m,10i} \mathbf{1_{10i}}^{\dagger} = \mathbf{0}$ for $1 \leq i \leq U_m$ without explanation.

**Theorem 2.1.** *Let $N_m = \frac{4^m - 1}{3}$ for $m \geq 2$, and $U_m = 4^{m-3}$ for $m \geq 3$.*

(1) *If $m \geq 2$, there exists an $[[N_m, N_m - 2m, 3]]$ linear code.*
(2) *If $m \geq 3$ and $N_{m-1} < n \leq N_m - 5$, there exists an $[[n, n-2m, 3]]$ linear code.*
(3) *If $m \geq 3$ and $N_m - 5 < n < N_m$, there exists an $[[n, n-2m-2, 3]]$ linear code.*

**Proof.** Equation (1) follows obviously from Lemma 2.1. To prove (2) and (3), we use induction on $m$. For $m = 3$, let

$$H_{3,5} = \begin{pmatrix} H_{2,5} \\ \mathbf{0} \end{pmatrix}, \quad H_{3,6} = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & \omega & \varpi \end{pmatrix},$$

$$H_{3,7} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix},$$

$$H_{3,8} = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & \omega & \varpi & \omega & \varpi \\ 0 & 1 & 0 & 1 & 1 & 1 & \omega & \varpi \end{pmatrix},$$

$$H_{3,9} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & \omega & \varpi & \omega & \varpi \\ 1 & 0 & 1 & \omega & \varpi & 0 & 0 & \varpi & \omega \end{pmatrix},$$

$$H_{3,10} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & \omega & \varpi & \omega & \varpi \\ 0 & 1 & 0 & 1 & \omega & \varpi & 1 & 1 & \varpi & \omega \end{pmatrix}.$$

It is easy to check that $H_{3,n}H^{\dagger}_{3,n} = \mathbf{0}$ for $5 \le n \le 10$. Deleting the columns that belong to $H_{3,n}$ from $H_{3,N_3}$ for $5 \le n \le 10$, we can obtain $H_{3,21-n}$ satisfying $H_{3,21-n}H^{\dagger}_{3,21-n} = \mathbf{0}$. Thus, for $6 \le n \le 16$, we have a self-orthogonal code $\mathcal{C}_n = \langle H_{3,n}\rangle$ and $\mathcal{C}_n^{\perp}=[n, n-3, 3]$. Consequently, for such $n$, there exists an $[[n, n-6, 3]]$ linear code.

While $17 \le n \le 20$, let

$$H_{4,n} = \begin{pmatrix} H_{3,n-10} & G_{3,10} \\ \mathbf{0_{1\times(n-10)}} & \mathbf{1_{10}} \end{pmatrix}.$$

It is easy to check that $H_{3,n}H^{\dagger}_{3,n} = \mathbf{0}$ for $17 \le n \le 20$. Thus, we have proved the existence of an $[[n, n-8, 3]]$ linear code for $17 \le n \le 20$. Thus, the lemma holds for $m = 3$.

Suppose that the lemma holds for $m$. Now we prove that it also holds for $m+1$.

(i) If $5 \le j \le N_m - 5$ or $j = N_m$, construct

$$H_{m+1,j} = \begin{pmatrix} H_{m,j} \\ \mathbf{0_{1\times j}} \end{pmatrix}.$$

If $N_m - 5 < j < N_m$, let

$$H_{m+1,j} = \begin{pmatrix} H_{m,j-10} & H_{m,10} \\ \mathbf{0_{1\times(j-10)}} & \mathbf{1_{10}} \end{pmatrix}.$$

It is obvious that $H_{m+1,j}H^{\dagger}_{m+1,j} = \mathbf{0}$ for $5 \le j \le N_m$. Delete the columns that belong to $H_{m+1,j}$ from $H_{m+1,N_{m+1}}$, we can obtain $H_{m+1,n}$ for $n = N_{m+1} - j$ such that $\mathcal{C}_n = \langle H_{m+1,n}\rangle$ is self-orthogonal and $\mathcal{C}_n^{\perp}=[n, n-m-1, 3]$. Thus, for $3N_m \le n \le N_{m+1} - 5$, there exists an $[[n, n-2m-2, 3]]$ linear quantum code.

(ii) If $N_m + 1 \le n \le 2N_m$, since $10 \times \frac{3}{4}U_{m+1} > \frac{5}{4} \times 4^{m-1}$, there exists an $i, 1 \le i \le U_m$ such that $5 \le n - 10i \le N_m - 5$. Construct

$$H_{m+1,n} = \left( H_{m+1,n-10i} \; H_{m+1,10i} \right),$$

where

$$H_{m+1,n-10i} = \begin{pmatrix} H_{m,n-10i} \\ \mathbf{0_{1\times(n-10i)}} \end{pmatrix},$$

and $H_{m+1,10i}$ satisfies (3) of Lemma 2.1. Then, the code $\mathcal{C}_n = \langle H_{m+1,n} \rangle$ is self-orthogonal and $\mathcal{C}_n^{\perp}=[n, n-m-1, 3]$. Thus, for $N_m + 1 \le n \le 2N_m$, there exists an $[[n, n-2m-2, 3]]$ linear quantum code. Deleting the columns that belong to $H_{m+1,j}$ from $H_{m+1,N_{m+1}}$ for $N_m + 1 \le j \le 2N_m$, we can obtain $H_{m+1,n}$ for $2N_m + 1 \le n \le 3N_m$ satisfying $H_{m+1,n}H^{\dagger}_{m+1,n} = \mathbf{0}$. Thus, we have proved the existence of an $[[n, n-2m-2, 3]]$ linear quantum code for $2N_m + 1 \le n \le 3N_m$.

(iii) Similar to the discussion for $17 \le n \le 20$, we can prove the existence of an $[[n, n-2m-4, 3]]$ linear quantum code for $N_{m+1} - 5 < n < N_{m+1}$.

Summarizing the above discussion, the theorem follows. □

**Remark.** (1) Our construction is different from the shorting technique of Calderbank *et al.* [1, Theorem 7] and the puncturing technique of Gottesman [5, Theorem 3]. Using our construction to construct quantum codes, neither need one to determine the supports of the codewords in the dual of a self-orthogonal code $\mathcal{C}$ as in Ref. 1, nor need one to determine the puncturing code of a symplectic code $\mathcal{C}$ as in Ref. 5.
(2) The linear quantum codes constructed from $\mathcal{C}_6 = \langle H_{3,6} \rangle$ is actually $[[6, 0, 4]]$, see Ref. 1.

## 3. Concluding Remarks

From Lemma 1.1, the quantum codes obtained in Theorem 2.1 are pure. In the sense of Definition 1.2, almost all of our quantum codes are optimal or near optimal. One can easily check the following result by using Proposition 1.1.

**Theorem 3.1.**
(1) *For $m \ge 2$, the pure $[[N_m, N_m - 2m, 3]]$ linear quantum code is optimal.*
(2) *For $m \ge 3$. If $\frac{2^{2m-1}-1}{3} < n \le N_m - 5$, then the pure $[[n, n-2m, 3]]$ linear code is optimal. If $N_{m-1} < n \le \frac{2^{2m-1}-1}{3}$, then the pure $[[n, n-2m, 3]]$ linear quantum code is near optimal.*

The number $n = \sum_{0\le i\le \frac{m}{2}} 2^{2i}$ for even $m \ge 2$ is just our $N_{\frac{m}{2}+1}$, and the number $n = \sum_{1\le i\le \frac{(m-1)}{2}} 2^{2i+1}$ for odd $m$ satisfies $N_{\frac{m+1}{2}+1} < n < N_{\frac{m+1}{2}+2}$. It follows that, for even $m$, our $[[N_{\frac{m}{2}+1},\ N_{\frac{m}{2}+1} - m - 2, 3]]$ linear quantum code have the same parameter as the additive code of the same length obtained by Theorem 11 of Ref. 1. However, for odd $m$, our $[[40, 32, 3]], [[168, 158, 3]], \ldots$ linear quantum codes are not as good as the additive codes $[[40, 33, 3]], [[168, 159, 3]], \ldots$ obtained by Theorem 11 of Ref. 1.

Since $N_m < 2^{2m-1} < 2^{2m} < N_{m+1}$, our $[[2^{2m}, 2^{2m} - 2m - 2, 3]]$ linear quantum code has the same parameters as the $[[2^{2m}, 2^{2m} - 2m - 2, 3]]$ additive quantum code obtained by Theorem 10 of Ref. 1. However, our $[[2^{2m-1}, 2^{2m-1} - 2m - 2, 3]]$ linear quantum code is not as good as the $[[2^{2m-1}, 2^{2m-1} - 2m - 1, 3]]$ additive quantum code obtained by Theorem 10 of Ref. 1.

Since $\frac{2^{2m+1}-1}{3} < 2^{2m} < N_{m+1} - 5$ for $m \geq 3$. It follows that when $n$ is even and $2^{2m} < n \leq N_{m+1} - 5$ for $m \geq 3$, the near optimal $[[n, n - 2m - 3, 3]]$ additive code obtained in Ref. 4 can be improved into an optimal $[[n, n - 2m - 2, 3]]$ linear quantum code.

**Acknowledgments**

The authors are very grateful to one of the anonymous referee for his valuable comments and suggestions, which helped to improve the manuscript significantly.

This work is supported by Nature Science Foundation of China under Grant No. 60573040, and Science Foundation of Collage of Science in AFEU.

**References**

1. 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.
2. D. Gottesman, Class of quantum error-correcting codes saturating the quantum Hamming bound, *Phys. Rev. A* **54** (1996) 1862–1868.
3. D. Gottesman, Pasting quantum codes, LANL e-print quant-ph/9607027.
4. R. Li and X. Li, Binary construction of quantum codes of minimum distance three and four, *IEEE Trans. Inform. Theory* **50** (2004) 1331–1336.
5. E. M. Rains, Nonbinary quantum codes, *IEEE Trans. Inform. Theory* **45** (1999) 1827–1832.