Binary Generalized Quasi-Cyclic Self-orthogonal Codes and Binary Construction of Pure Quantum Codes

Weiliang Wang[1,2], Yangyu Fan[1], Luobin Guo[2]

[1] School of Electronics and Information Northwestern Polytechnical, Xi'an, P.R. China
[2] College of Science Air Force Engineering University, Xi'an, P.R. China
wlwangkg@gmail.com, fan_yangyu@sina.com, glbglb2011@163.com

Abstract - In this paper, a special subclass of binary generalized quasi-cyclic self-orthogonal codes and quantum codes constructed by Steane construction are discussed. Firstly, eight 16-dimensional even length generalized quasi-cyclic self-orthogonal codes with dual distance five are built based on circulant or partial circulant matrices. Secondly, pairs of nested self-orthogonal codes with dual distance five and three are designed by applying an algorithm for searching subcodes of a given code. Thirdly, revised pairs of codes with dual distance six and four are constructed by extending previous pairs of codes, and then eight quantum codes with distance six are obtained by Steane construction. These eight quantum codes are new binary construction by Steane construction and are best known ones.

Index Terms - Quantum code, Steane construction, self-orthogonal code, generalized quasi-cyclic code, pair of nested self-orthogonal codes.

1. Introduction

Quantum-error-correcting codes (quantum codes for short) play important roles in reducing both decoherence and inaccuracy while performing operations on quantum data. As an important subclass of quantum codes, the first examples of binary quantum stabilizer codes were discovered independently by Calderbank and Shor [1] and by Steane [2]. The systemic mathematical frameworks for designing binary quantum stabilizer codes were due to Shor, Steane, Gottesman and Calderbank *et al.*, see [2, 3, 4, 5, 6]. At the same time, some construction methods for binary quantum stabilizer codes have been proposed, in which the problem of constructing binary quantum stabilizer codes can be transformed into the problem of constructing classical self-orthogonal codes by CSS construction [1,2,3], Steane construction (see Theorem 1 below) [7] or quaternary construction [6].

Theorem 1 Let C and C' be binary $[n,k,d]$ and $[n,k_1,d_1]$ codes respectively. If $C^{\perp}\subset C\subset C'$ and $k_1\geq k+2$, then a quantum code $\left[\left[n,k_1+k-n,min\left\{d,\lceil 3d_1/2\rceil\right\}\right]\right]$ can be constructed.

In this paper, we focus on binary construction of quantum stabilizer codes by Steane construction. The key problem in this manner is to build pairs of nested self-orthogonal codes with possible larger dual distance and dimension difference. We start with the construction of binary even length self-orthogonal codes and their basic pairs of codes, followed by revised pairs of codes and quantum codes. Practically speaking, a special subclass of generalized quasi-cyclic codes constructed from circulant or partial circulant matrices is firstly discussed, and eight binary generalized quasi-cyclic self-orthogonal codes $[n,16]$ with dual distance five for length n = 50, 52, 66, 68, 70, 82, 84 and 86 are built. Secondly, a method for finding subcodes of linear codes is presented by specifying special dimensionality reduction matrices, followed by to design basic pairs of obtained self-orthogonal codes with dual distance five and three. Subsequently, the revised pairs of codes with dual distance six and four are obtained by extending previous pairs of codes. Lastly, eight quantum stabilizer codes with distance six are constructed from revised pairs of codes by Steane construction.

The material is organized as follows. Some basic notions and results on codes are recalled in section 2. Details on binary generalized quasi-cyclic self-orthogonal codes constructed from circulant or partial circulant matrices are discussed in section 3. Section 4 devotes to designing pairs of nested binary self-orthogonal codes and quantum codes. We subsequently compare our codes with the known ones in the last section.

2. Preliminaries

Let $F_2=\{0,1\}$ be binary field, a k-dimensional subspace C of F_2^n is called an $[n,k]$ linear code over F_2. The number $d(C)=\min\{wt(c)|c\in C,c\neq 0\}$ is the minimum distance of C, where $wt(x)=\#\{x_i|x_i\neq 0\}$ is the weight of $x=(x_1,\cdots,x_n)\in F_2^n$. An $[n,k]$ code with distance d is denoted by $[n,k,d]$.

The matrix G whose rows form a basis for a code $C=[n,k]$ is a generator matrix for C. In this case, the code C is represented as $C=\langle G\rangle$. Any $[n,k]$ code C has a unique generator matrix in standard form $G=\left(I_k\left|A_{k\times(n-k)}\right.\right)$, where I_k is the binary $k\times k$ identity matrix. An $(n-k)\times n$ matrix H defined by $C=\left\{x\in F_2^n\left|Hx^T=0\right.\right\}$ is a parity check matrix for C. For the binary code $C=\langle G\rangle$, if $G=\left(I_k\left|A_{k\times(n-k)}\right.\right)$, then $H=\left(A^T\left|I_{n-k}\right.\right)$ is a parity check matrix for C.

Two $[n,k]$ linear codes C_1 and C_2 are permutation equivalent if there exists a binary permutation matrix P such

that $G_1 = G_2 P$, where G_1 and G_2 are generator matrices for C_1 and C_2 respectively. The permutation equivalent codes are essentially the same.

The Euclidean inner product on F_2^n is $x \cdot y = \sum_{i=1}^{n} x_i y_i$, where $x = (x_1, \cdots, x_n)$, $y = (y_1, \cdots, y_n) \in F_2^n$. The $[n, n-k]$ code $C^{\perp} = \{x \in F_2^n \mid x \cdot c = 0, c \in C\}$ is known as the dual of an $C = [n, k]$ code, and $C^{\perp} = \langle H \rangle$ if H is a parity check matrix for C. If $d^{\perp} = d(C^{\perp})$, then C is called a code with dual distance $d^{\perp}$. A code C is self-orthogonal if $C \subset C^{\perp}$ and self-dual if $C = C^{\perp}$. Any codeword of a binary self-orthogonal code has even weight, and any subcode of a binary self-orthogonal code is self-orthogonal.

Lemma Let $C = [n, k]$ be a binary self-orthogonal code with dual distance $d^{\perp}$, G be a generator matrix for C, and $1_n = (1, \cdots, 1) \in F_2^n$ be the all-ones vector.

If n is even and $1_n \notin C$, then $G' = \begin{pmatrix} G \\ 1_n \end{pmatrix}$ generates a self-orthogonal code $C' = [n+1, k+1]$. The dual distance of C' equals $d^{\perp}$ if $d^{\perp}$ is even and is greater than or equal to $d^{\perp} + 1$ if $d^{\perp}$ is odd.

3. Binary Generalized Quasi-cyclic Self-orthogonal Codes

As a natural generalization of cyclic codes, quasi-cyclic codes are known to be good codes. Many optimal or best known linear codes are quasi-cyclic codes [8, 9, 10, 11]. The algebra structure of quasi-cyclic codes has been researched for a long time [12, 13, 14, 15] and some feasible construction methods for one-generator quasi-cyclic codes have been proposed [9, 10, 16]. Although degenerate quasi-cyclic codes might reduce dependency between length and dimensionality of codes [9], there is little flexibility for these two parameters. In this section, we design binary self-orthogonal codes from circulant or partial circulant matrices, which can be viewed as a special subclass of generalized quasi-cyclic codes. For general notions on generalized quasi-cyclic codes, see [17, 18, 19] please.

For any $f(x) = \sum_{j=0}^{l-1} f_j x^j \in F_2[x]/(x^l - 1)$, let

$$M_f = \begin{pmatrix} f(x) \\ xf(x) \\ \vdots \\ x^{l-1} f(x) \end{pmatrix} = \begin{pmatrix} f_0 & f_1 & \cdots & f_{l-1} \\ f_{l-1} & f_0 & \cdots & f_{l-2} \\ \vdots & \vdots & \ddots & \vdots \\ f_1 & f_2 & \cdots & f_0 \end{pmatrix}. \quad (1)$$

Suppose $T = \{i_1, \cdots, i_k\} \subset \{1, \cdots, l\}$ and $M_{f,T}$ is a matrix whose rows come from M_f indexed by T. Matrices M_f and $M_{f,T}$ are known as circulant and partial circulant matrix over F_2 respectively. Let $l_i \geq k$, $T_i = T = \{1, 2, \cdots, k\}$ and

$$G = \begin{pmatrix} I_k & M_{f_1,T} & \cdots & M_{f_p,T} \end{pmatrix}. \quad (2)$$

where $f_i(x) = \sum_{j=0}^{l_i - 1} f_{ij} x^j \in F_2[x]/(x^{l_i} - 1)$ and $M_{f_i,T}$ is a $k \times l_i$ binary circulant or partial circulant matrix for $1 \leq i \leq p$. Then (2) can generate an $C = [k + \sum_{i=1}^{p} l_i, k]$ generalized quasi-cyclic code determined by $(f_1, \cdots, f_p)$. The dual of C defined by (2) is $C^{\perp} = \langle H \rangle$, where

$$H = \left(\begin{array}{c|c} & M'_{f_1,T} \\ I_{\sum_{i=1}^{p} l_i} & \vdots \\ & M'_{f_p,T} \end{array} \right). \quad (3)$$

There are two major obstacles while applying directly (2) to constructing self-orthogonal codes. Firstly, the fact that the number of candidates for each f_i equals to 2^{l_i} results in huge computation complexity. Secondly, suppose that there are some same l_i's, for instance $l_1 = l_2 = l$, and $k \geq \lceil l/2 \rceil$. If there exists some integer t such that $x^t f_1(x) = f_2(x) \bmod (x^l - 1)$, then $d(C^{\perp})$ might be smaller according to (3). It's unattractive for constructing quantum codes. On the other hand, exchanging f_1 and f_2 can produce equivalent codes. These problems can be relieved by introducing an equivalent relation and a total ordering relation on each different $F_2[x]/(x^{l_i} - 1)$.

A binary equivalent relation ~ on $F_2[x]/(x^{l_i} - 1)$ is defined by $f(x) \sim g(x)$ if and only if there exists some integer t such that $x^t f_1(x) = f_2(x) \bmod (x^l - 1)$. One can prove that the number of those equivalence classes in $\left(F_2[x]/(x^{l_i} - 1)\right)/\sim$ equals $M_{l_i} = \sum_{d \mid l_i} \frac{1}{d} \sum_{j \mid d} \mu(j) 2^{d/j}$ and M_{l_i} is near to $2^{l_i}/l_i$ for larger l_i, where $\mu(\cdot)$ is the Möbius function.

A total ordering relation on $F_2[x]/(x^{l_i} - 1)$ is defined by $f(x) \leq g(x)$ if and only if $D(f) \leq D(g)$, where $D(f)$ is the decimal representation for coefficient vector of $f(x)$. For a given $f \in F_2[x]/(x^{l_i} - 1)$, let $[f] = \{g \mid g \sim f\}$ and $f_{min} \in [f]$ such that $D(f_{min}) \leq D(g)$ for any $g \in [f]$.

Suppose

$$\hat{F}_i = \left\{ f_{i,1}, \cdots, f_{i,M_{l_i}} \right\}. \quad (4)$$

where $f_{i,j}$ is the element with minimal decimal representation in equivalence class $[f_{i,j}]$.

Our strategies for building generalized quasi-cyclic self-orthogonal codes with form in (2) can be summarized as follows. For $1 \le i \le p$, each f_i comes from $\hat{F}_i$ in (4), which can reduce the number of candidate polynomials dramatically. If there exist some same l_i's, for example $l_{i_1}, \cdots, l_{i_s}$, then select $f_{i_1}, \cdots, f_{i_s}$ such that $D(f_{i_1}) < \cdots < D(f_{i_s})$, which can avoid smaller $d(C^{\perp})$ and equivalent codes. If dual distance $d(C^{\perp}) \ge d^{\perp}$ is expected, then $wt(f_i) \ge d^{\perp} + \sigma_i$, where $\sigma_i > 0$ is a controlling parameter. Aiming at constructing binary self-orthogonal codes, $1 + \sum_{i=1}^{p} wt(f_i)$ must be even.

Based on construction strategies above, some binary generalized quasi-cyclic self-orthogonal codes with dual distance five can are built, see Theorem 2. Details on these codes are listed in Table I. In Table I, the dimensional of generalized quasi-cyclic self-orthogonal codes depends on the subscript of the first part $(1\cdots0)_k$ in second column, and the rest $f_i = (f_{i1}\cdots f_{il_i})_{l_i}$ stands for binary circulant matrix M_{f_i} if $l_i = k$ or partial circulant matrix $M_{f_i,T}$ if $l_i > k$ and $T = \{1, \cdots, k\}$.

Theorem 2 There exist binary generalized quasi-cyclic self-orthogonal codes [*n*, 16] with dual distance five for length *n* = 50, 52, 66, 68, 70, 82, 84 and 86.

Remark. One can prove that $1_n \notin C = [n,16]$ in Theorem 2. Furthermore, $1_n \notin C' \subset C = [n,16]$.

TABLE I Binary Generalized Quasi-cyclic Self-orthogonal Codes [*n*, 16] with Dual Distance Five

n	Generator polynomials
50	$(1000000000000000)_{16}$ $(1100010101100000)_{17}(11111101011010100)_{17}$
52	$(1000000000000000)_{16}$ $(1100100010001100000)_{18}(101101110110111000)_{18}$
66	$(1000000000000000)_{16}(1001011111000000)_{16}$ $(1110011111010000)_{17}(10111110011100000)_{17}$
68	$(1000000000000000)_{16}(1001011111000000)_{16}$ $(101110011010011000)_{18}(110010101010110100)_{18}$
70	$(1000000000000000)_{16}(111011011100100000)_{18}$ $(100011110110000000)_{18}(100110011011000000)_{18}$
82	$(1000000000000000)_{16}(1101101110110000)_{16}$ $(1111101111011100)_{16}(11001110111110100)_{17}$ $(11011110010111100)_{17}$
84	$(1000000000000000)_{16}$ $(1100010101100000)_{17}(11111101011010100)_{17}$ $(11100011010100000)_{17}(10110111111100100)_{17}$
86	$(1000000000000000)_{16}$ $(1100010101100000)_{17}(11111101011010100)_{17}$ $(11000010010100000)_{18}(111101110111110000)_{18}$

4. Pair of Codes and Quantum Codes

Let G be a generator matrix for a code $C = [n,k]$ and $k' < k$. The code $C' = [n,k']$ is a k'-dimension subcode of C if and only if there exists a binary row full rank matrix $T_{k' \times k}^{(n)}$ such that $G' = T_{k' \times k}^{(n)} G$ generates C'. For $k' < k$, the number of all row full rank binary $k' \times k$ matrices equals to

$$N(k',k) = 2^{\frac{k'(k'-1)}{2}} \prod_{i=0}^{k'-1} \left(2^{k-i} - 1\right). \tag{5}$$

The number $N(k',k)$ is too numerous for larger k and k' to mention all $T_{k' \times k}^{(n)}$.

In this section, a method in a stepwise manner is used to find subcodes with better dual distance. For a given binary self-orthogonal code $C = [n,k]$, we design the subcode chain with the form in (6) such that these codes C_{k_i}'s have better dual distance.

$$C = C_{k_1} \supset \cdots \supset C_{k_i} = [n,k_i] \cdots \supset C_{k_m} = C'. \tag{6}$$

Considering the efficiency for searching subcodes and the fact that there are many equivalent codes in these C_{k_i}'s, we adopt the dimensionality deduction matrix with the form in (7).

$$T_{k_{i+1} \times k_i}^{(n)} = \left(I_{k_{i+1}} \quad X\right). \tag{7}$$

where X is a binary $k_{i+1} \times (k_i - k_{i+1})$ matrix for $i = 1, \cdots, m$.

Applying the idea to binary generalized quasi-cyclic self-orthogonal codes in Table I, some subcode chains or pairs of codes can be obtained, see Table II below. Consider an example, two dimensionality deduction matrices $T_{14\times16}^{(50)}$ and $T_{7\times14}^{(50)}$ are selected for $n = 50$, and subcode chain $[50,16,14] \supset [50,14,14] \supset [50,7,16]$ with dual distance 5, 5 and 3 is built. For simplicity, only X's in $T_{14\times16}^{(50)}$ and $T_{7\times14}^{(50)}$ are showed in (8) and here the rest dimensionality deduction matrices are omitted.

TABLE II Basic Pairs of Nested Self-orthogonal Codes and Their Dual Counterparts

n	$C_k \supset \cdots \supset C_{k'}$	$C_k^{\perp} \subset \cdots \subset C_{k'}^{\perp}$
50	[50,16,14]⊃[50,14,14]⊃[50,7,16]	[50,34,5]⊂[50,36,5]⊂[50,43,3]
52	[52,16,16]⊃[52,15,16]⊃[52,7,18]	[52,36,5]⊂[52,37,5]⊂[52,45,3]
66	[66,16,20]⊃[66,7,26]	[66,50,5]⊂[66,59,3]
68	[68,16,20]⊃[68,8,22]	[68,52,5]⊂[68,60,3]
70	[70,16,24]⊃[70,8,24]	[70,54,5]⊂[70,62,3]
82	[82,16,24]⊃[82,8,28]	[82,66,5]⊂[82,74,3]
84	[84,16,28]⊃[84,8,32]	[84,68,5]⊂[84,76,3]
86	[86,16,28]⊃[86,8,32]	[86,70,5]⊂[86,78,3]

$$X_{14\times 2}=\begin{pmatrix}00011111111101\\00101101011001\end{pmatrix}',X_{7\times 7}=\begin{pmatrix}1101110\\0000101\\1010111\\1111001\\0000000\\1011100\\1010001\end{pmatrix}. \quad (8)$$

Based on Lemma, revised pairs of codes with dual distance six and four can be constructed from pairs of codes in Table II. Binary quantum stabilizer codes with distance six by steane construction are summarized in Theorem 3.

Theorem 3 There exist binary quantum stabilizer codes [[50,27,6]], [[52,28,6]], [[66,41,6]], [[68,42,6]], [[70,44,6]], [[82,56,6]], [[84,58,6]] and [[86,60,6]].

5. Conclusions and Remarks

Generalized quasi-cyclic codes have advantage in structural characteristics although there is less progress in construction methods. In this paper, we investigate a subclass of binary generalized quasi-cyclic self-orthogonal codes constructed from circulant or partial circulant matrices, and present a feasible construction approach. Based on obtained generalized quasi-cyclic self-orthogonal codes and their revised pairs of codes, we construct eight quantum stabilizer codes. Our quantum stabilizer codes are pure according to [7], and all of them are new ones by steane construction. Compared with quaternary additive construction of quantum codes in [20], these eight pure quantum stabilizer codes reach lower bound of quaternary additive construction and are best known ones.

Acknowledgment

This work is supported by National Natural Science Foundation of China under Grant No.11071255 and Science Foundation for young teachers in College of Science, Air Force Engineering University.

References

[1] P.W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Phys. Rev. A*, vol. 52, pp. 2493-2496, 1995.

[2] A.M. Steane, "Error correcting codes in quantum theory," *Phys. Rev. Lett.*, vol. 77, pp. 793-797, 1996.

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

[4] D. Gottesman, "Class of quantum error correcting codes saturating the quantum Hamming bound," *Phys. Rev. A*, vol. 54, pp. 1862-1868, 1996.

[5] A.R. Calderbank, E.M. Rains, P.W. Shor and N.J.A. Sloane, "Quantum error correction and orthogonal geometry," *Phys. Rev. Lett.*, vol. 78, pp. 405-408, 1996.

[6] 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*, vol. 44, pp. 1369-1387, 1998.

[7] A.M. Steane, "Enlargement of calderbank-shor-steane quantum codes," *IEEE Trans. Inform. Theory*, vol. 45, pp. 2492-2495, 1999.

[8] P. Heijnen, H.V. Tilborg, T. Verhoeff and S. Weijs, "Some New Binary Quasi-Cyclic Codes," *IEEE Trans. Inform. Theory*, vol. 44, no. 5, pp. 1994-1996, 1998.

[9] R. Daskalov and P. Hristov, "New Binary One-Generator Quasi-Cyclic Codes," *IEEE Trans. Inform. Theory*, vol. 49, no.11, pp. 3001-3005, 2003.

[10] E.Z. Chen, "New Quasi-Cyclic Codes from Simplex Codes," *IEEE Trans. Inform. Theory*, vol. 53, no. 3, pp. 1193-1196, 2007.

[11] M. Grassl and G.S. White, "New codes from chains of quasi-cyclic codes," *In Proc. 2005 IEEE Int. Symp. on Information Theory*, pp. 2095-2099, 2005.

[12] J. Conan and S. Séguin, "Structural properties and enumeration of quasi cyclic codes," *Applicable Algebra in Engineering, Communication and Computing*, vol. 4, pp. 25-39, 1993.

[13] K. Lally and P. Fitzpatrick, "Algebraic structure of quasicyclic codes," *Discrete Applied Mathematics*, vol. 111, pp. 157-175, 2001.

[14] S. Ling and P. Sole, "On the algebraic structure of quasi-cyclic codes I: finite fields," *IEEE Trans. Inform. Theory*, vol. 47, no. 7, pp. 2751-2759, 2001.

[15] P.L. Cayrel, C. Chabot and A. Necer, "Quasi-cyclic codes as codes over rings of matrices," *Finite Fields and Their Applications*, vol. 16, pp. 100-115, 2010.

[16] T.A. Gulliver and V.K. Bhargava, "Some Best Rate 1/*p* and Rate (*p*-1)/*p* Systematic Quasi-Cyclic Codes," IEEE Trans. Inform. Theory, vol. 37, no. 3, pp. 552-555, 1991.

[17] I. Siap and N. Kulhan, "The Structure of Generalized Quasi Cyclic Codes," *Applied Mathematics E-Notes*, vol. 5, pp. 24-30, 2005.

[18] M. Esmaeili and S. Yari, "Generalized quasi-cyclic codes: structural properties and code construction," *Applicable Algebra in Engineering, Communication and Computing*, vol. 20, no.2, pp. 159-173, 2009.

[19] Yonglin Cao, "Structural properties and enumeration of 1-generator generalized quasi-cyclic codes," *Designs, Codes and Cryptography*, Vol. 60, no. 1, pp. 67-79, 2011.

[20] M. Grassl, Bounds on the minimum distance of additive quantum codes. http://www.codetables.de/.