

## Good Additive Cyclic Quantum Codes

Ai Luo and M. Reza. Soleymanni

Abstract - The paper presents all the best additive cyclic quantum codes of length up to 23 qubits, as well as a table showing the existed additive cyclic quantum codes of length up to 31 qubits.

### 1. Introduction

Calderbank's paper [1] turned the problem of finding additive quantum codes to the problem of finding self-orthogonal codes over  $GF(4)^n$ . In [1], many methods were presented. In this paper, we use one of those methods in [1] to do a thorough research.

### 2. Some theorems

Calderbank's paper [1] presented the following theorem about the additive cyclic codes over  $GF(4)^n$ :

#### Theorem 1:

a) Any  $(n, 2^k)$  additive cyclic code  $C$  has two generators which can be represented as

$\langle wp(x)+q(x), r(x) \rangle$ , where  $p(x), q(x), r(x)$  are binary polynomials,  $p(x)$  and  $r(x)$  divide  $x^n - 1 \pmod{2}$ ,  $r(x)$  divides  $\frac{q(x)(x^n - 1)}{p(x)} \pmod{2}$ , and

$$k = 2n - \deg p - \deg r .$$

b) If  $\langle wp'(x)+q'(x), r'(x) \rangle$  is another such representation, then

$$p'(x) = p(x), r'(x) = r(x) \text{ and } q'(x) \equiv q(x) \pmod{r(x)} .$$

c)  $C$  is self-orthogonal if and only if

$$p(x)r(x^{n-1}) \equiv p(x^{n-1})r(x) \equiv 0 \pmod{x^n - 1}$$

$$p(x)q(x^{n-1}) \equiv p(x^{n-1})q(x) \pmod{x^n - 1}$$

This theorem enables us to search all of the self-orthogonal additive cyclic codes over

$GF(4)^n$ . In order to find the corresponding  $[[n, n-k, d]]$  additive cyclic quantum codes, we need the following theorem, which is also mentioned in [1]:

**Theorem 2:** If  $C$  is an  $(n, 2^k)$  additive code with weight enumerator  $W_C(x, y)$  [2], then the weight enumerator of  $C^\perp$  is given by:

$$W_{C^\perp}(x, y) = 2^{-k} W(x + 3y, x - y)$$

We can find the minimum distance of  $C^\perp - C$  by comparing the coefficients of  $W_C(x, y)$  with those of  $W_{C^\perp}(x, y)$ .

The search ranges for the polynomials  $p(x), q(x), r(x)$  are the following:

1) The arrange for  $p(x)$  is between 1 and  $x^n - 1$ , not including  $x^n - 1$ .  $p(x)$  can not be 0, for if  $p(x)$  is 0, the code  $C$  will be a binary code.

2) The arrange for  $r(x)$  is between 1 and  $x^n - 1$ , including  $x^n - 1$ . When  $r(x)$  is  $x^n - 1$ ,  $r(x)$  can not be considered as a generator, for  $r(x)$  is actually 0 (mod  $x^n - 1$ ).

In this case, the generator of the code is simply  $\langle wp(x) + q(x) \rangle$ .

3) The arrange for  $q(x)$  is between 1 and  $r(x)$ , including  $r(x)$ . Note that  $q(x) = r(x)$  is equivalent to  $q(x) = 0$ , for the generators  $\langle wp(x) + r(x), r(x) \rangle$  and  $\langle wp(x), r(x) \rangle$  generate same code.

### 3. The search algorithm

1) Find all of the irreducible binary factors of  $x^n - 1$  over  $GF(2)$ . These factors will help us in the next step – finding  $p(x)$  and  $r(x)$ .

2) Consider all of the pairs of  $p(x)$  and  $r(x)$  which satisfy the equation

$$p(x)r(x^{n-1}) \equiv p(x^{n-1})r(x) \equiv 0 \pmod{x^n - 1}$$

3) For each pair of  $p(x)$  and  $r(x)$  coming from step 2), consider all of the possible

$q(x)$  which satisfy

a)  $q(x)(x^n - 1) \equiv 0 \pmod{p(x)r(x)}$

b)  $p(x)q(x^{n-1}) \equiv p(x^{n-1})q(x) \pmod{x^n - 1}$

4) For each set of qualified polynomials  $p(x), q(x), r(x)$ , we calculate the weight enumerators of the code and its dual code to find  $d$ .

#### 4. The results

Table 1.1

Additive cyclic quantum codes with highest minimum distance

Parameters	Generators
$[[5,0,3]]$	$\langle w w 0 1 0 \rangle \langle 1 1 1 1 1 \rangle$
$[[5,1,3]]$	$\langle \bar{w} \bar{w} 1 0 1 \rangle$
$[[5,4,1]]$	$\langle \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \rangle$
$[[7,0,3]]$	$\langle w w w 0 w 0 0 \rangle \langle 1 0 1 1 0 0 0 \rangle$
$[[7,1,3]]$	$\langle \bar{w} \bar{w} 1 0 0 0 1 \rangle$
$[[7,3,2]]$	$\langle \bar{w} w 0 \bar{w} 0 1 1 \rangle$
$[[7,4,2]]$	$\langle \bar{w} 1 w w \bar{w} 0 1 \rangle$
$[[7,6,1]]$	$\langle \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \rangle$
$[[9,0,4]]$	$\langle \bar{w} \bar{w} w 1 0 1 0 0 0 \rangle \langle 1 1 0 1 1 0 1 1 0 \rangle$
$[[9,1,3]]$	$\langle \bar{w} \bar{w} 1 0 0 0 0 0 1 \rangle$
$[[9,2,3]]$	$\langle \bar{w} \bar{w} \bar{w} 1 0 1 1 0 1 \rangle$



$[[9,3,3]]$	$\langle \bar{w} 0 0 \bar{w} 1 1 0 1 1 \rangle$
$[[9,6,2]]$	$\langle \bar{w} 1 1 \bar{w} 1 1 \bar{w} 1 1 \rangle$
$[[9,7,1]]$	$\langle \bar{w} \bar{w} 0 \bar{w} \bar{w} 0 \bar{w} \bar{w} 0 \rangle$
$[[9,8,1]]$	$\langle \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \rangle$
$[[11,0,4]]$	$\langle \bar{w} \bar{w} 0 0 0 1 0 1 0 0 0 \rangle \langle 1 1 1 1 1 1 1 1 1 1 1 \rangle$
$[[11,1,3]]$	$\langle \bar{w} \bar{w} 1 0 0 0 0 0 0 0 1 \rangle$
$[[11,10,1]]$	$\langle \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \rangle$
$[[13,0,5]]$	$\langle w w 0 0 1 0 1 1 1 0 1 0 0 \rangle \langle 1 1 1 1 1 1 1 1 1 1 1 1 1 \rangle$
$[[13,1,5]]$	$\langle \bar{w} \bar{w} 1 0 0 1 1 0 1 1 0 0 1 \rangle$
$[[13,12,1]]$	$\langle \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \rangle$
$[[15,0,6]]$	$\langle w 1 w \bar{w} w 1 w 0 0 0 0 0 0 0 0 \rangle \langle 1 0 1 1 0 0 1 1 0 1 0 0 0 0 0 \rangle$
$[[15,1,5]]$	$\langle \bar{w} \bar{w} 1 0 0 1 1 0 0 0 1 1 0 0 1 \rangle$
$[[15,2,5]]$	$\langle \bar{w} \bar{w} \bar{w} 1 1 0 1 1 0 0 1 1 0 1 1 \rangle$
$[[15,3,5]]$	$\langle \bar{w} 0 0 \bar{w} 0 1 1 0 1 0 1 0 1 1 0 \rangle$
$[[15,4,4]]$	$\langle \bar{w} w 1 0 w 1 0 0 1 1 1 0 1 1 1 \rangle$
$[[15,5,4]]$	$\langle \bar{w} 0 w 1 w \bar{w} 0 0 1 1 1 1 0 0 1 \rangle$
$[[15,6,4]]$	$\langle \bar{w} 0 0 \bar{w} \bar{w} w \bar{w} 1 0 1 0 1 0 0 1 \rangle$
$[[15,7,3]]$	$\langle \bar{w} \bar{w} 0 w 0 0 1 w 0 1 0 1 1 1 1 \rangle$
$[[15,8,3]]$	$\langle \bar{w} 1 1 1 w 0 \bar{w} \bar{w} w 0 0 1 1 0 1 \rangle$
$[[15,9,3]]$	$\langle \bar{w} w 0 0 \bar{w} w w 1 1 w 1 0 1 1 1 \rangle$



$[[15,10,2]]$	$\langle \bar{w} 1 1 1 1 \bar{w} 1 1 1 1 \bar{w} 1 1 1 1 \rangle$
$[[15,11,2]]$	$\langle \bar{w} \bar{w} 1 0 1 \bar{w} \bar{w} 1 0 1 \bar{w} \bar{w} 1 0 1 \rangle$
$[[15,12,2]]$	$\langle \bar{w} 1 1 \bar{w} 1 1 \bar{w} 1 1 \bar{w} 1 1 \bar{w} 1 1 \rangle$
$[[15,13,1]]$	$\langle \bar{w} \bar{w} 0 \bar{w} \bar{w} 0 \bar{w} \bar{w} 0 \bar{w} \bar{w} 0 \bar{w} \bar{w} 0 \rangle$
$[[15,14,1]]$	$\langle \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \rangle$
$[[17,0,7]]$	$\langle w w 0 0 1 1 0 1 1 1 1 1 0 1 1 0 0 \rangle \langle 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 \rangle$
$[[17,1,7]]$	$\langle \bar{w} \bar{w} 1 0 1 1 1 0 1 0 1 0 1 1 1 0 1 \rangle$
$[[17,8,4]]$	$\langle \bar{w} 1 0 \bar{w} w \bar{w} 0 1 \bar{w} 1 1 1 0 0 1 1 1 \rangle$
$[[17,9,4]]$	$\langle \bar{w} \bar{w} 1 w 1 1 w 1 \bar{w} \bar{w} 0 0 1 0 1 0 0 \rangle$
$[[17,16,1]]$	$\langle \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \rangle$
$[[19,0,7]]$	$\langle w w 0 0 0 0 0 1 0 1 1 1 0 1 0 0 0 0 0 \rangle \langle 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 \rangle$
$[[19,1,7]]$	$\langle \bar{w} \bar{w} 1 0 0 0 0 1 0 1 0 1 0 1 0 0 0 0 1 \rangle$
$[[19,18,1]]$	$\langle \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \bar{w} \rangle$
$[[21,0,8]]$	$\langle w w 0 1 0 \bar{w} 0 0 1 1 1 0 1 1 0 0 0 0 0 0 0 \rangle, \langle 1 0 0 0 1 1 0 0 1 0 1 0 1 1 1 1 1 0 0 0 0 \rangle$
$[[21,1,7]]$	$\langle \bar{w} \bar{w} 1 0 0 0 0 1 0 1 1 0 1 1 0 1 0 0 0 0 1 \rangle$
$[[21,2,6]]$	$\langle \bar{w} w \bar{w} 1 0 1 1 1 1 1 1 0 0 1 1 1 1 1 1 0 1 \rangle$
$[[21,3,6]]$	$\langle \bar{w} w 0 w 0 0 0 0 1 0 0 0 0 1 1 1 1 1 0 1 1 \rangle$
$[[21,4,6]]$	$\langle \bar{w} 0 w \bar{w} w 1 0 1 0 0 1 0 0 1 0 1 0 1 1 0 1 \rangle$
$[[21,5,6]]$	$\langle \bar{w} 1 1 0 w \bar{w} 1 1 0 0 1 1 1 1 0 0 0 0 1 0 1 \rangle$
$[[21,6,5]]$	$\langle \bar{w} w w 0 \bar{w} 1 \bar{w} 0 0 0 1 0 1 1 1 0 1 0 0 1 1 \rangle$



[[21,7,5]]	$\langle \bar{w} 0 0 w w \bar{w} \bar{w} \bar{w} 0 0 0 1 1 0 1 0 1 0 1 0 1 \rangle$
[[21,8,4]]	$\langle \bar{w} 0 w 1 0 \bar{w} 0 w w 0 1 1 1 0 0 1 1 1 0 0 1 \rangle$
[[21,9,4]]	$\langle \bar{w} 0 0 0 1 1 w 1 1 w 0 0 1 0 0 0 0 0 1 1 1 \rangle$
[[21,10,4]]	$\langle \bar{w} 0 w 1 \bar{w} 0 w w 0 1 w 0 1 0 0 1 1 0 1 1 1 \rangle$
[[21,11,4]]	$\langle \bar{w} 0 1 w w 0 1 1 1 w 0 w 1 1 0 0 0 0 0 1 1 \rangle$
[[21,12,3]]	$\langle \bar{w} 1 w \bar{w} 1 1 w 0 \bar{w} 0 0 w w 0 0 1 1 0 0 0 1 \rangle$
[[21,13,3]]	$\langle \bar{w} \bar{w} w 0 w 1 \bar{w} \bar{w} \bar{w} \bar{w} 0 w 0 w 0 0 1 0 0 1 1 \rangle$
[[21,14,3]]	$\langle \bar{w} w 0 0 0 \bar{w} w w 1 w \bar{w} w 1 0 w 0 1 0 1 1 1 \rangle$
[[21,15,3]]	$\langle \bar{w} 1 \bar{w} 1 1 w 0 1 \bar{w} \bar{w} 0 0 w 1 w w 0 1 1 0 1 \rangle$
[[21,16,2]]	$\langle \bar{w} \bar{w} w \bar{w} w 1 w 0 \bar{w} 1 0 w w 1 0 0 w 0 1 1 1 \rangle$
[[21,17,2]]	$\langle \bar{w} w 0 \bar{w} 0 1 1 \bar{w} w 0 \bar{w} 0 1 1 \bar{w} w 0 \bar{w} 0 1 1 \rangle$
[[21,18,2]]	$\langle \bar{w} 1 1 \bar{w} 1 1 \bar{w} 1 1 \bar{w} 1 1 \bar{w} 1 1 \bar{w} 1 1 \bar{w} 1 1 \bar{w} 1 1 \rangle$
[[21,19,1]]	$\langle \bar{w} \bar{w} 0 \bar{w} \bar{w} 0 \bar{w} \bar{w} 0 \bar{w} \bar{w} 0 \bar{w} \bar{w} 0 \bar{w} \bar{w} 0 \bar{w} \bar{w} 0 \bar{w} \bar{w} 0 \rangle$
[[21,20,1]]	$\langle \bar{w} \rangle$
[[23,0,8]]	$\langle w w 0 0 0 0 1 1 1 0 0 0 1 0 0 0 1 1 1 0 0 0 0 \rangle,$ $\langle 1 \rangle$
[[23,1,7]]	$\langle w w w w w 0 0 w 0 0 w 0 w 0 0 0 0 0 0 0 0 0 0 \rangle,$ $\langle 1 1 1 1 1 0 0 1 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 \rangle$
[[23,11,4]]	$\langle w w \bar{w} w w 0 0 \bar{w} 0 1 \bar{w} 0 \bar{w} 1 1 1 0 0 0 0 0 0 0 \rangle,$ $\langle 1 \rangle$
[[23,12,4]]	$\langle w \bar{w} w w \bar{w} 1 0 \bar{w} 0 1 w 0 \bar{w} 1 0 0 1 0 0 0 0 0 0 \rangle$
[[23,22,1]]	$\langle \bar{w} \rangle$

Table 1.2

All of the valid  $[[25 \leq n \leq 31, k]]$  for additive cyclic quantum codes

("E" means exist)

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

Table 1.3  
Some additive cyclic code with highest minimum distance for  $n = 31$

Parameters	Generators
$[[31,15,5]]$	$\langle \bar{w} w \bar{w} w 0 0 \bar{w} 1 w \bar{w} 1 w 0 \bar{w} 1 1 w 0 0 \bar{w} 1 w 0 0 0 0 0 0 0 0 \rangle,$ $\langle 1 1 0 0 1 0 1 1 0 1 1 1 1 0 1 0 1 0 0 0 1 0 0 1 1 1 0 0 0 0 \rangle$
$[[31,16,5]]$	$\langle w \bar{w} \bar{w} \bar{w} 1 0 w 1 w \bar{w} 1 w 1 w 1 0 w 1 0 w 1 w 1 0 0 0 0 0 0 0 0 \rangle,$ $\langle 1 0 1 0 1 1 1 0 1 1 0 0 0 1 1 1 1 1 0 0 1 1 0 1 0 0 1 0 0 0 0 \rangle$
$[[31,20,4]]$	$\langle \bar{w} 1 0 0 1 w \bar{w} 0 1 \bar{w} 0 \bar{w} w 0 1 \bar{w} w \bar{w} 0 \bar{w} w 0 0 0 1 1 0 1 0 0 1 \rangle$
$[[31,21,4]]$	$\langle \bar{w} w 0 0 1 \bar{w} 0 \bar{w} 1 w w w 1 \bar{w} 1 w 0 1 w \bar{w} 1 \bar{w} 1 0 1 1 1 1 1 1 1 \rangle$

### 5. Conclusion

All of the codes listed in table 1.1, except the codes  $[[11,0,4]]$ ,  $[[11,1,3]]$ , meet the lower bounds in the table of [1], which are the best additive quantum codes we can achieve now. Thus, to a great degree, searching the best quantum codes can be replaced by searching the best additive cyclic quantum codes. The search complexity will therefore be greatly reduced.

- [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. on Info. Theory*, vol. 44, no. 4, pp. 1369-1387, July 1998.
- [2]. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes* (NorthHolland, Amsterdam, 1977).