Int J Theor Phys (2018) 57:682–686
https://doi.org/10.1007/s10773-017-3599-9

Quantum Codes Derived from Negacyclic Codes

Jian Gao[1] · **Yongkang Wang**[1]

Received: 7 June 2017 / Accepted: 13 November 2017 / Published online: 18 November 2017

Abstract Recently, La Guardia constructed some new quantum codes from cyclic codes (La Guardia, Int. J. Theor. Phys., 2017). Inspired by this work, we consider quantum codes construction from negacyclic codes, not equivalent to cyclic codes, with only one cyclotomic coset containing at least two odd consecutive integers of even length. Some new quantum codes are obtained by this class of negacyclic codes.

Keywords Quantum codes · Negacyclic codes · Cyclotomic coset

1 Introduction

Cyclic codes form an important class of linear codes due to their good algebraic structures in coding theory and decoding theory. Recently, there are some papers on quantum codes construction from cyclic codes [1, 6–9]. Negacyclic codes are generalizations of cyclic codes, and also have good algebraic structures. If the length of negacyclic codes is odd, then negacyclic codes are cyclic codes actually [2]. Based on the good structural properties of negacyclic codes, there have been some papers on quantum codes construction from negacyclic codes [4, 5, 10, 11]. In [4], the authors Kai et al. constructed some new quantum MDS codes from negacyclic codes. Lately, the authors constructed some new classes of nonbinary quantum codes from negacyclic codes in [5]. Chen et al. studied the optimal asymmetric quantum codes construction and nonbinary quantum convolutional codes construction from negacyclic codes in [10] and [11], respectively. These results show that quantum codes can be constructed by nagacyclic codes effectively.

✉ Jian Gao
dezhougaojian@163.com

Yongkang Wang
zcyongkang@163.com

[1] School of Science, Shandong University of Technology, Zibo, 255000, People's Republic of China

Let q be a power of some prime number. A q-ary quantum code C of length n is a K-dimension subspace of the q^n-dimension Hilbert space $(\mathbb{C}^q)^{\otimes n}$. If $K = q^k$, then the quantum code C is denoted by $[[n, k, d]]_q$, where d is the minimum distance. For a quantum code $[[n, k, d]]_q$, there is a Singleton bound for parameters n, k and d satisfying $k + 2d \leq n+2$. If the equality holds, then the quantum code C is called a maximum distance separable (MDS) code.

In this short correspondence, we present a quantum codes construction from negacyclic codes with only one cyclotomic coset of even code length. Some new quantum codes, in sense of the Singleton bound, are obtained by this class of negacyclic codes.

2 Quantum Codes from Negacyclic Codes

Let $\mathbb{F}_q$ be a finite field with q elements, where q is a power of an odd prime number. The parameters of a linear code over $\mathbb{F}_q$ is denoted by $[n, k, d]_q$, where n is the code length, k is the dimension and d is the minimum Hamming distance. A linear code C is called a negacyclic code if for any codeword $(c_0, c_1, \ldots, c_{n-1}) \in C$, the vector $(-c_{n-1}, c_0, \ldots, c_{n-2})$ is also a codeword of C. A negacyclic code C is an ideal of the quotient ring $\mathbb{F}_q[x]/(x^n + 1)$. Therefore C can be generated by a monic divisor of $x^n + 1$. This polynomial is called the generator polynomial of C.

Let $\gcd(n, q) = 1$ and β be a primitive $2n$th root of unity. Then the roots of $x^n + 1$ are β^{1+2i}, where $i = 0, 1, \ldots, n - 1$. Let $\mathscr{O}_{2n}$ be the set of odd integers from 1 to $2n$, and C_x be the q-cyclotomic coset modulo $2n$ containing x. Let m^* be the size of this coset. Then $C_x = \{x, xq, \ldots, xq^{m^*-1}\}$ and $g(x) = \prod_{j \in C_x}(x - \beta^j)$ is an irreducible polynomial over $\mathbb{F}_q$. If $g(x)$ is the generator polynomial of the negacyclic code C, then C is called a maximum negacyclic code, i.e. C is with only one q-cyclotomic coset. The q-cyclotomic coset C_x is called the defining set of C, which implies that the dimension of C is $n - m^*$.

Lemma 1 [5, BCH bound] *Let C be a negacyclic code of length n over $\mathbb{F}_q$ and $g(x)$ be its generator polynomial. If $g(x)$ has roots $\{\beta^{1+2i} | 0 \leq i \leq r\}$, then the minimum Hamming distance of C is at least $r + 2$.*

For any negacyclic code C of length n, the Euclidean dual code $C^\perp$ of C is also a negacyclic code of length n. Further, $C^\perp \subseteq C$ if and only if $g(x)$ divides $h(x)$, which implies that $C_x \cap C_{-x} = \emptyset$, where $h(x)$ is the generator polynomial of $C^\perp$ and C_{-x} is the q-cyclotomic coset containing $-x$ modulo $2n$.

In the following, we show how to guarantee the existence of a negacyclic code whose defining set containing only one q-cyclotomic coset with at least two consecutive odd integers.

Theorem 1 *Let $q \geq 3$ be a power of some prime number and $q \not\equiv 1 \bmod 4$, $n > m$ be a positive integer such that $\gcd(q, 2n) = 1$ and $\gcd(\frac{q^{a_i}-1}{2}, n) = 1$ for each $i = 1, 2, \cdots, r$, where $m = ord_{2n}(q)$, $r \geq 1$ and $1 \leq a_1, a_2, \ldots, a_r < m$ are odd positive integers. If $n \mid \gcd(t_2, \ldots, t_r)$, where $t_j = [(j - (j - 1)q^{a_j})(\frac{q^{a_j}-1}{2})^{-1} - (\frac{q^{a_1}-1}{2})^{-1}]$ for each $j = 2, \ldots, r$ (the operations are performed modulo n), then there exists an $[n, n-m^*, \geq r+2]_q$ negacyclic code, where m^* is the size of the q-cyclotomic coset containing $r+1$ consecutive odd positive integers.*

Proof We want to investigate the following system of congruences

$$\begin{aligned} xq^{a_1} &\equiv (x+2) \bmod 2n \\ (x+2)q^{a_2} &\equiv (x+4) \bmod 2n \\ (x+4)q^{a_3} &\equiv (x+6) \bmod 2n \\ &\vdots \\ [x+2(r-1)]\,q^{a_r} &\equiv (x+2r) \bmod 2n, \end{aligned}$$

where $r \geq 1$ and $1 \leq a_1, a_2, \ldots, a_r < m$ are odd positive integers. Since $\gcd(\frac{q^{a_i}-1}{2}, n) = 1$ for each $i = 1, 2, \ldots, r$, it follows that the above system is equivalent to

$$\begin{aligned} x &\equiv (\tfrac{q^{a_1}-1}{2})^{-1} \bmod n \\ x &\equiv (2-q^{a_2})(\tfrac{q^{a_2}-1}{2})^{-1} \bmod n \\ x &\equiv (3-2q^{a_3})(\tfrac{q^{a_3}-1}{2})^{-1} \bmod n \\ &\vdots \\ x &\equiv [r-(r-1)q^{a_r}](\tfrac{q^{a_r}-1}{2})^{-1} \bmod n, \end{aligned}$$

where $(\frac{q^{a_i}-1}{2})^{-1}$ denotes the multiplicative inverse of $\frac{q^{a_i}-1}{2}$ modulo n.

The system has a solution if only and only if

$$[j-(j-1)q^{a_j}](\frac{q^{a_j}-1}{2})^{-1} \equiv [i-(i-1)q^{a_i}](\frac{q^{a_i}-1}{2})^{-1} \bmod n$$

for all $i, j = 2, \ldots, r$ and

$$(\frac{q^{a_1}-1}{2})^{-1} \equiv [i-(i-1)q^{a_i}](\frac{q^{a_i}-1}{2})^{-1} \bmod n$$

for all $i = 2, \ldots, r$. This means that

$$n \mid [(j-(j-1)q^{a_j})(\frac{q^{a_j}-1}{2})^{-1} - (\frac{q^{a_1}-1}{2})^{-1}]$$

for all $j = 2, \ldots, r$, i.e., $n \mid \gcd(t_2, \ldots, t_r)$, where $t_j = [(j-(j-1)q^{a_j})(\frac{q^{a_j}-1}{2})^{-1} - (\frac{q^{a_1}-1}{2})^{-1}]$ for each $j = 2, \ldots, r$.

Let C be a negacyclic code, which has the q-cyclotomic coset C_x as its defining set. Then C_x contains the sequence $x, x+2, \ldots, x+2r$ of $r+1$ consecutive odd integers. Therefore, by the BCH bound, the minimum Hamming distance d of C satisfies $d \geq r+2$. Since $|\, C_x \,| = m^*$, then the dimension of C is $n - m^*$. Thus, we have an $[n, n-m^*, d \geq r+2]_q$ negacyclic code. □

The following Calderbank-Shor-Steane (CSS) construction gives a connection between classical error-correcting codes and quantum codes.

Lemma 2 [3, Calderbank-Shor-Steane (CSS) construction] *If there exists a classical linear* $[n, k, d]_q$ *code* C *such that* $C^{\perp} \subseteq C$, *then there exists an* $[[n, 2k-n, \geq d]]_q$ *stabilizer quantum code that is pure to* d.

By Theorem 1, Lemmas 1 and 2, we have the following result directly.

Corollary 1 *Assume all the hypotheses of Theorem 1 hold. Let C be a maximum negacyclic code with the defining set C_x. If C_x has elements $\{1 + 2i | 0 \leq i \leq r\}$ and $C_x \neq C_{-x}$, then there exists an $[[n, n - 2m^*, \geq r + 2]]_q$ quantum code.*

Example 1 Assume that $q = 23$ and $n = 60$. Then $2n = 120$ and $m = \mathrm{ord}_{120}(23) = 4$. In the 23-cyclotomic cosets, we can find $C_1 = \{1, 23, 47, 49\}$. If C is a negacyclic code of length 60 over $\mathbb{F}_{23}$ with the defining set C_1, then it has parameters $[60, 56, \geq 3]_{23}$. So there exists an $[[60, 52, \geq 3]]_{23}$ quantum code. This quantum code has the same minimum distance as the known quantum code $[[63, 51, \geq 3]]_{23}$ appeared in [6], but our code has the larger code rate than that code.

Example 2 Assume that $q = 27$ and $n = 28$. Then $2n = 56$ and $m = \mathrm{ord}_{56}(27) = 2$. In the 27-cyclotomic cosets, we can find $C_{41} = \{41, 43\}$. If C is a negacyclic code of length 28 over $\mathbb{F}_{27}$ with the defining set C_{41}, then it has parameters $[28, 26, \geq 3]_{27}$. So there exists an $[[28, 24, \geq 3]]_{27}$ quantum code. The quantum Singleton bound asserts that the quantum code $[[n, k, d]]_q$ satisfies $k + 2d \leq n + 2$. This quantum code has parameters satisfying it, hence, $[[28, 24, 3]]_{27}$ is a quantum MDS code.

Example 3 Assume that $q = 23$ and $n = 24$. Then $2n = 48$ and $m = \mathrm{ord}_{48}(23) = 2$. In the 23-cyclotomic cosets, we can find $C_{11} = \{11, 13\}$. If C is a negacyclic code of length 24 over $\mathbb{F}_{23}$ with the defining set C_{11}, then it has parameters $[24, 22, \geq 3]_{23}$. So there exists an $[[24, 20, \geq 3]]_{23}$ quantum code. This quantum code has parameters satisfying the quantum Singleton bound, hence, $[[24, 20, 3]]_{23}$ is a quantum MDS code.

The Table 1 contains some new q-ary quantum codes, where q is an odd prime power. The first column of the table denotes the length of negacyclic codes over $\mathbb{F}_q$, C_x is the defining set of negacyclic codes, column three denotes the parameters of the negacyclic codes over $\mathbb{F}_q$, the last column denotes the new q-ary quantum codes. Note that the parameters of all new q-ary quantum codes appeared in Table 1 satisfy $n + 2 - k - 2d \leq 4$.

Table 1 New quantum codes

n	C_x	$[n, k, d]_q$	$[[n, k, d]]_q$
24	$C_5 = \{5, 7, 29, 31\}$	$[24, 20, \geq 3]_{11}$	$[[24, 16, \geq 3]]_{11}$
16	$C_3 = \{3, 5, 19, 21\}$	$[16, 12, \geq 3]_{23}$	$[[16, 8, \geq 3]]_{23}$
20	$C_1 = \{1, 7, 9, 23\}$	$[20, 16, \geq 3]_{23}$	$[[20, 12, \geq 3]]_{23}$
30	$C_1 = \{1, 23, 47, 49\}$	$[30, 26, \geq 3]_{23}$	$[[30, 22, \geq 3]]_{23}$
40	$C_{11} = \{11, 13, 59, 77\}$	$[40, 36, \geq 3]_{23}$	$[[40, 32, \geq 3]]_{23}$
48	$C_{11} = \{11, 13, 59, 61\}$	$[48, 44, \geq 3]_{23}$	$[[48, 40, \geq 3]]_{23}$
120	$C_{11} = \{11, 13, 59, 157\}$	$[120, 116, \geq 3]_{23}$	$[[120, 112, \geq 3]]_{23}$
40	$C_1 = \{1, 3, 9, 27\}$	$[40, 36, \geq 3]_{27}$	$[[40, 32, \geq 3]]_{27}$
56	$C_{41} = \{41, 43, 97, 99\}$	$[56, 52, \geq 3]_{27}$	$[[56, 48, \geq 3]]_{27}$
70	$C_{41} = \{41, 43, 69, 127\}$	$[70, 66, \geq 3]_{27}$	$[[70, 62, \geq 3]]_{27}$
52	$C_7 = \{7, 9, 17, 71\}$	$[52, 48, \geq 3]_{31}$	$[[52, 44, \geq 3]]_{31}$
128	$C_{95} = \{95, 97, 223, 225\}$	$[128, 124, \geq 3]_{63}$	$[[128, 120, \geq 3]]_{63}$
256	$C_{63} = \{63, 65, 319, 321\}$	$[256, 252, \geq 3]_{127}$	$[[256, 248, \geq 3]]_{127}$

Acknowledgements This research is supported by the National Natural Science Foundation of China (Grant Nos. 11701336, 11626144 and 11671235).

References

1. Aly, S.A., Klappenecher, A.: On quantum and classical quantum BCH codes. IEEE Trans. Inform. Theory **53**(3), 1183–1188 (2007)
2. Blackford, T.: Negacyclic duadic codes. Finite Fields Appl. **14**, 930–943 (2008)
3. Calderbank, A.R., Rains, E.M., Shor, P.W., Sloane, N.J.A.: Quantum error correction via GF(4). IEEE Trans. Inform. Theory **44**(4), 1369–1387 (1998)
4. Kai, X., Zhu, S.: New quantum MDS codes from negacyclic codes. IEEE Trans. Inform. Theory **59**(2), 1193–1197 (2013)
5. Kai, X., Zhu, S.: Quantum negacyclic codes. Phys. Rev. A **88**(1-5), 012326 (2013)
6. La Guardia, G.G.: Quantum codes derived from cyclic codes. Int. J. Theor. Phys., https://doi.org/10.1007/s10773-017-3399-2 (2017)
7. La Guardia, G.G.: New quantum MDS codes. IEEE Trans. Inform. Theory **57**(8), 5551–5554 (2011)
8. La Guardia, G.G.: On the construction of nonbinary quantum BCH codes. IEEE Trans. Inform. Theory **60**(3), 1528–1535 (2014)
9. Qian, J., Zhang, L.: Improved constructions for nonbinary quantum BCH codes. Int. J. Theor. Phys., https://doi.org/10.1007/s10773-017-3277-y (2017)
10. Chen, J.-Z., Li, J.-P., Lin, J.: New optimal asymmetric quantum codes derived from negacyclic codes. Int. J. Theor. Phys. **53**, 72–79 (2014)
11. Chen, J.-Z., Li, J.-P., Yang, F., Huang, Y.: Nonbinary quantum convolutional codes derived from negacyclic codes. Int. J. Theor. Phys. **54**, 198–209 (2015)