Cyclic Codes of Prime Power Length from Generalized Cyclotomic Classes of Order 4 and 8

Pankaj[#1], Manju Pruthi[#2]
 # Department of Mathematics, Indira Gandhi University,
Meerpur (Rewari)-122502, Haryana, India

Abstract: *In this paper, we first introduce generalized cyclotomic classes of order 4 and 8 and then present a special class of cyclic codes with length p^m. We also obtain lower bound on the minimum odd weight of these codes.*

Keywords: *Cyclotomy, Generator Polynomial, Cyclic code*
MSC 2010: *11Txx, 11T22, 11T71, 68P30, 94Bxx, 94B15*

1. INTRODUCTION

Cyclic Codes are a small but highly structured subclass of linear codes. Cyclic codes have been studied for decades and a lot of progress has been made and many important results in the field of cyclic codes have been found (for example, see [2]-[4], [7]-[13], [15] etc). Recently, several classes of cyclic codes using two-prime Whiteman's generalized cyclotomic sequences and cyclotomic sequences of order 4 have been presented by C. Ding in [9] and [8] respectively and lower bounds on the nonzero minimum hamming weight of some cyclic codes were developed at the same time. In [35] and [37], several classes of cyclic codes have been constructed by employing Whiteman's generalized cyclotomic sequences of order 4 and 6 respectively. In [17], Pramod Kumar Kewat and Preeti Kumari employed Whiteman's generalized cyclotomic sequences of order 6 to construct several classes of cyclic codes. In [25], [26] and [27], several classes of cyclic codes over the finite field $GF(q)$ with length $n_1 n_2$ have been obtained using the two-prime Whiteman's generalized cyclotomic sequences of order 8, $2^r, r \geq 2$ and $2l, l \geq 2$ respectively and the lower bounds of the minimum distance of these cyclic codes are also obtained.

Quadratic residue codes [23, ch. 6] of prime length are a class of interesting error-correcting codes due to a high minimum distance. Those codes have a "square-root bound" which roughly asserts that the square of the minimum distance is greater than the block length. A more general class of codes with the square-root bound on their minimum odd weight is the duadic codes defined by Leon, Masley and Pless [19], [28].
Let n be a positive composite integer. A partition $\{D_0, D_1, D_2, \cdots, D_{d-1}\}$ of Z_n^* is a family of sets with

$$D_i \cap D_j = \emptyset, \text{ for all } i \neq j, \bigcup_{i=0}^{d-1} D_i = Z_n^*$$

If D_0 is a multiplicative subgroup of Z_n^* and there are elements $g_1, \cdots, g_{d-1}$ of Z_n^* such that $D_i = g_i D_0$ for all i, these D_i are called generalized cyclotomic classes of order d. When n is a prime, it is referred to as classical cyclotomy. For a generalized cyclotomy of order 2, the cyclotomic classes D_0 and D_1 form a splitting of n, i.e., there exists an element μ such that $\mu D_0 = D_1$ and $\mu D_1 = D_0$ (for details about splitting, see [18], [28], [29], [30]). However, a splitting may not give a generalized cyclotomy of order 2.
The generalized cyclotomic numbers of order d are defined to be

$$(i,j)_d = \left|(D_i + 1) \cap D_j\right|, \qquad i,j = 0,1,\cdots,d-1.$$

Classical cyclotomy was considered in detail by Gauss in his Disquisitions Arithmeticae [16], where he introduced so-called Gaussian periods, and then cyclotomic numbers. Both Gaussian periods and some cyclotomic numbers are

related to irreducible cyclic codes [22], [24]. In fact, the weight distribution of binary irreducible cyclic codes is completely determined by Gaussian periods or cyclotomic numbers. As for classical cyclotomy, cyclotomic numbers with respect to p of order upto 24 are known. For information about classical cyclotomy refer to [3], [6] and [34].

Generalized cyclotomy with respect to p^2 was considered in [7] for cryptographic purpose, where the corresponding generalized cyclotomic numbers of order 2 were presented. Generalized cyclotomy with respect to pq was introduced by Whiteman [36], where the motivation was to search for residue difference sets. Many new generalized cyclotomies of order 2 and the corresponding cyclotomic numbers were studied by C. Ding and T. Helleseth in [13].

This paper is organized as follows. In section 2, we extend the classical cyclotomy with respect to p into a generalized cyclotomy of order 4 with respect to p^m. In section 3, we describe a special class of cyclic codes with length p^m with this generalized cyclotomy. We also obtain lower bound on the minimum odd weight of these codes. In section 4, we define generalized cyclotomic classes of order 8 with respect to p^m. In section 5, we describe a special class of cyclic codes with length p^m with this generalized cyclotomy. We also obtain lower bound on the minimum odd weight of these codes.

2. GENERALIZED CYCLOTOMIC CLASSES OF ORDER 4

We start with the following assumption:
All the primes mentioned in this paper are congruent to $1 \pmod 8$ (hence 2 is a quadratic residue modulo such a prime).

An integer a is called a primitive root modulo n if the multiplicative order of a modulo n, denoted by $ord_n(a)$, is equal to $\phi(n)$ where ϕ is the Euler phi function and $\gcd(a,n) = 1$. It is well known that the only integers having primitive roots are $p^e, 2p^e, 1, 2$ and 4, where p is an odd prime.

If g is a primitive root modulo p^2, then g is primitive root modulo p^i for all i. But g is a primitive root modulo p does not imply that it is primitive root modulo p^2, but this situation is rare. These facts are well known. For details, we refer to [1].

Let $l \geq 1$ be an integer and g_l be a primitive root modulo p^l, where p is an odd prime. We now fix some notations for this and later sections. We use Z_n to denote the ring $Z_n = \{0,1,2,\cdots,n-1\}$ with integer addition modulo n and integer multiplication modulo n as the ring operations. Here and hereafter a mod n denotes the least nonnegative integer that is congruent to a modulo n. As usual, we use Z_n^* to denote all the invertible elements of Z_n, where $n \geq 2$ is a positive integer.
Let S be a subset of Z_n and a an element of Z_n. Define

$$a + S = S + a = \{a + s : s \in S\}, \quad aS = Sa = \{as : s \in S\}$$

The generalized cyclotomic classes of order 4 with respect to p^l are defined by

$$D_0^{(p^l)} = (g_l^4), \quad D_1^{(p^l)} = g_l D_0^{(p^l)},$$
$$D_2^{(p^l)} = g_l^2 D_0^{(p^l)}, \quad D_3^{(p^l)} = g_l^3 D_0^{(p^l)},$$

where (g_l^4) denotes the subgroup generated by g_l^4 of $Z_{p^l}^*$. It is obvious that

$$D_0^{(p^l)} \cup D_1^{(p^l)} \cup D_2^{(p^l)} \cup D_3^{(p^l)} = Z_{p^l}^*$$

and

$$D_i^{(p^l)} \cap D_j^{(p^l)} = \emptyset$$

for all $0 \leq i, j \leq 3, i \neq j$, where $\emptyset$ denotes the empty set.
We say that $D_0^{(p^l)}, D_1^{(p^l)}, D_2^{(p^l)}$ and $D_3^{(p^l)}$ form a partition of the set $Z_{p^l}^*$.

2.1. Lemma: $D_0^{(p^l)}$ is a subgroup of $Z_{p^l}^*$ with $\left|D_0^{(p^l)}\right| = \frac{p^{l-1}(p-1)}{4}$

and

$$aD_i^{(p^l)} = D_{i+j\,(\mathrm{mod}\ 4)}^{(p^l)} \quad \text{if} \quad a \in D_j^{(p^l)} \text{ for all } 0 \le i, j \le 3.$$

Since $p \equiv 1(\mathrm{mod}\ 8)$, we also have $2 \in D_0^p \cup D_2^p$ i.e., 2 is a quadratic residue modulo p [1].

2.2. Lemma: $a \bmod p \in D_i^p$ if and only if $a \bmod p^l \in D_i^{(p^l)}$ for any $l \ge 1$, where $1 \le a \le p-1,\ i = 0,1,2,3$.

3. CYCLIC CODES FROM GENERALIZED CYCLOTOMIC CLASSES OF ORDER 4

Let θ_l be a primitive p^lth root of unity over a field containing $GF(2)$. We define the generalized cyclotomic polynomials of order 4 with respect to p^l as

$$d_i^{(p^l)}(x) = \prod_{h \in D_i^{(p^l)}} \left(x - \theta_l^h\right), \quad i = 0,1,2,3$$

3.1. Lemma: $d_i^{(p^l)}(x) \in GF(2)[x]$ for all $i = 0,1,2,3$.

Let m be a positive integer, g primitive root modulo p^m and θ a primitive p^mth root of unity over a field containing $GF(2)$ (let s be the order of 2 modulo p^m, such a primitive p^mth root of unity exists in $GF(2^s)$).
Define

$$g_l \equiv g(\bmod p^l),\ \ \theta_l = \theta^{p^{m-l}},\ \ l = 1,2,\cdots,m$$

Then g_l is a primitive root modulo p^l and θ_l is a primitive p^lth root of unity.

3.2. Lemma:

$$x^{p^m} - 1 = (x-1)\prod_{i=0}^{3}\prod_{l=1}^{m} d_i^{(p^l)}(x)$$

For any set of $i_1, i_2, \cdots, i_m$, where $i_l \in \{0,1,2,3\},\ l = 1,2,\cdots,m$, let

$$g_{i_1,i_2,\cdots,i_m}(x) = d_{i_1}^{(p)}(x) d_{i_2}^{(p^2)}(x) \cdots d_{i_m}^{(p^m)}(x)$$

Let $C_{i_1,i_2,\cdots,i_m}$ denote the cyclic code of length p^m generated by the polynomial $g_{i_1,i_2,\cdots,i_m}(x)$.

3.3. Theorem: For each set of $i_1, i_2, \cdots, i_m \in \{0,1,2,3\}$, $C_{i_1,i_2,\cdots,i_m}$ is a $[p^m, (3p^m+1)/4]$ code with minimum odd weight $d \ge \sqrt[4]{p^m}$.

Proof: Let $2 < s \le p-1$ be a quadratic non-residue modulo p. By Lemma 2.2, $s \in D_1^{(p^l)} \cup D_3^{(p^l)}$ for all $l = 1,2,\cdots,m$. Let

$$u_j(x) = g_{i_1+j\,(\mathrm{mod}\ 4),i_2+j\,(\mathrm{mod}\ 4),\cdots,i_m+j\,(\mathrm{mod}\ 4)}(x)$$

for all $0 \le j \le 3$. By the definition of the polynomial $d_i^{(p^l)}$ and Lemma 2.1,

$$d_{i_l+j\,(\mathrm{mod}\ 4)}^{(p^l)} \mid u_j(x) \qquad (1)$$

for all $0 \le j \le 3,\ 1 \le l \le m$.
Let $a_0(x)$ be a codeword of $C_{i_1,i_2,\cdots,i_m}$ with minimum odd weight d and define $a_j(x) = a_0(x^s) \bmod p^m - 1,\ j = 1,2,3$. Here and hereafter $g(x)$ mod $h(x)$ denotes the unique polynomial of degree less than the degree of $h(x)$ that is congruent to $g(x)$ modulo $h(x)$. By (1), $a_j(x)$ is a codeword of $C_{i_1+j\,(\mathrm{mod}\ 4),i_2+j\,(\mathrm{mod}\ 4),\cdots,i_m+j\,(\mathrm{mod}\ 4)}$ with odd weight d.
Similarly, if $a_j(x)$ is a codeword of $C_{i_1+j\,(\mathrm{mod}\ 4),i_2+j\,(\mathrm{mod}\ 4),\cdots,i_m+j\,(\mathrm{mod}\ 4)}$ with minimum odd weight d, then $a_j(x^s) \bmod p^m - 1$ is a codeword of $C_{i_1,i_2,\cdots,i_m}$ with odd weight d. Thus these codes have same minimum odd weight.

Now consider the polynomial $c(x)$ defined by $c(x) = a_0(x)a_1(x)a_2(x)a_3(x) \bmod p^m - 1$. It is a codeword of $C_{i_1+j \pmod 4, i_2+j \pmod 4, \cdots, i_m+j \pmod 4}$ for all $0 \le j \le 3$, i.e., $c(x)$ is a multiple of $g_{i_1,i_2,\cdots,i_m}(x)$, $g_{i_1+1 \pmod 4, i_2+1 \pmod 4, \cdots, i_m+1 \pmod 4}(x)$, $g_{i_1+2 \pmod 4, i_2+2 \pmod 4, \cdots, i_m+2 \pmod 4}(x)$ and $g_{i_1+3 \pmod 4, i_2+3 \pmod 4, \cdots, i_m+3 \pmod 4}(x)$. Since $a_0(x), a_1(x), a_2(x)$ and $a_3(x)$ have odd weight, so $c(x)$ has odd weight. Hence

$$\begin{aligned} c(x) &= \prod_{j=0}^{3} g_{i_1+j \pmod 4, i_2+j \pmod 4, \cdots, i_m+j \pmod 4}(x) \\ &= \left(x^{p^m} - 1\right)/(x-1) \\ &= 1 + x + \cdots + x^{p^m - 1} \end{aligned}$$

Note that $c(x)$ has at most d^4 terms, it follows that

$$d^4 \ge p^m, \text{ i.e., } d \ge \sqrt[4]{p^m}.$$

Since $deg\left(g_{i_1+j \pmod 4, i_2+j \pmod 4, \cdots, i_m+j \pmod 4}(x)\right) = \frac{p^m-1}{4}$ for all $0 \le j \le 3$, the dimension of these codes is thus $\frac{3p^m+1}{4}$. ■

Note that since there are 4^m choices for the parameters $i_1, i_2, \cdots, i_m$, we have 4^m such different cyclic codes.

4. GENERALIZED CYCLOTOMIC CLASSES OF ORDER 8

The generalized cyclotomic classes of order 8 with respect to p^l are defined by

$$D_0^{(p^l)} = (g_l^8), \quad D_i^{(p^l)} = g_l^i D_0^{(p^l)},$$

$1 \le i \le 7$, where (g_l^8) denotes the subgroup generated by g_l^8 of $Z_{p^l}^*$. It is obvious that

$$\bigcup_{i=0}^{7} D_i^{(p^l)} = Z_{p^l}^*$$

and

$$D_i^{(p^l)} \cap D_j^{(p^l)} = \emptyset$$

for all $0 \le i, j \le 7, i \ne j$, where $\emptyset$ denotes the empty set.

We say that $D_0^{(p^l)}, D_1^{(p^l)}, \cdots, D_7^{(p^l)}$ form a partition of the set $Z_{p^l}^*$.

4.1. Lemma: $D_0^{(p^l)}$ is a subgroup of $Z_{p^l}^*$ with $\left|D_0^{(p^l)}\right| = \frac{p^{l-1}(p-1)}{8}$

and

$$aD_i^{(p^l)} = D_{i+j \pmod 8}^{(p^l)} \quad \text{if} \quad a \in D_j^{(p^l)} \text{ for all } 0 \le i, j \le 7.$$

Since $p \equiv 1 (\bmod 8)$, we also have $2 \in D_0^p \cup D_2^p \cup D_4^p \cup D_6^p$ i.e., 2 is a quadratic residue modulo p [1].

4.2. Lemma: $a \bmod p \in D_i^p$ if and only if $a \bmod p^l \in D_i^{(p^l)}$ for any $l \ge 1$, where $1 \le a \le p-1$, $0 \le i \le 7$.

5. CYCLIC CODES FROM GENERALIZED CYCLOTOMIC CLASSES OF ORDER 8

Let θ_l be a primitive p^lth root of unity over a field containing $GF(2)$. We define the generalized cyclotomic polynomials of order 8 with respect to p^l as

$$d_i^{(p^l)}(x) = \prod_{h \in D_i^{(p^l)}} \left(x - \theta_l^h\right), \quad 0 \le i \le 7$$

5.1. Lemma: $d_i^{(p^l)}(x) \in GF(2)[x]$ for all $0 \le i \le 7$.

5.2. Lemma:

$$x^{p^m} - 1 = (x-1)\prod_{i=0}^{7}\prod_{l=1}^{m} d_i^{(p^l)}(x)$$

For any set of $i_1, i_2, \cdots, i_m$, where $i_l \in \{0,1,2,3,4,5,6,7\}$, $l = 1,2,\cdots,m$, let

$$g_{i_1,i_2,\cdots,i_m}(x) = d_{i_1}^{(p)}(x) d_{i_2}^{(p^2)}(x) \cdots d_{i_m}^{(p^m)}(x)$$

Let $C_{i_1,i_2,\cdots,i_m}$ denote the cyclic code of length p^m generated by the polynomial $g_{i_1,i_2,\cdots,i_m}(x)$.

5.3. Theorem: For each set of $i_1, i_2, \cdots, i_m \in \{0,1,2,3,4,5,6,7\}$, $C_{i_1,i_2,\cdots,i_m}$ is a $[p^m, (7p^m+1)/8]$ code with minimum odd weight $d \geq \sqrt[8]{p^m}$

Proof: Proof is similar as that of Theorem 3.3. ■

Note that since there are 8^m choices for the parameters $i_1, i_2, \cdots, i_m$, we have 8^m such different cyclic codes.

REFERENCES

[1] Apostol T. M., *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1976.

[2] Bakshi G. K. and Raka M., Minimal cyclic codes of length $p^n q$, *Finite Fields and Their Applications*, **9**, 432-448, 2003.

[3] Baumert L. D., *Cyclic Difference Sets, Lecture Notes in Mathematics*, Vol. **182**, Springer-Verlag, New York, 1971.

[4] Betti E. and Sala M., A new bound for the minimum distance of a cyclic code from its defining set, *IEEE Transactions on Information Theory*, **52(8)**, 3700-3706, 2006.

[5] Brouwer A. E., Bounds on the size of linear codes, *in Handbook of Coding Theory*, V. Pless and W. C. Huffman, Eds. Amsterdam, the Netherlands, Elsevier, 1998.

[6] Cusik T., Ding C. and Renvall A., *Stream Ciphers and Number Theory*, North-Holland Mathematical Lib., North-Holland, 2003.

[7] Ding C., Binary cyclotomic generators, *in Fast Software Encryption* (B. Preneel, Ed.), Lecture Notes in Computer Science, **1008**, 29-60, 1995.

[8] Ding C., Cyclic codes from cyclotomic sequence of order four, *Finite Fields and Their Applications*, **23**, 8-34, 2012.

[9] Ding C., Cyclic codes from the two-prime sequences, *IEEE Transactions on Information Theory*, **58(6)**, 3881-3891, 2012.

[10] Ding C., Cyclotomic constructions of cyclic codes with length being the product of two primes, *IEEE Transactions on Information Theory* **58(4)**, 2231-2236, 2012.

[11] Ding C., Du X., and Zhou Z., The bose and minimum distance of a class of BCH codes, *IEEE Transactions on Information Theory*, **61(5)**, 2351-2356, 2015.

[12] Ding C. and Helleseth, T., Generalized cyclotomic codes of length $p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$, *IEEE Transactions on Information Theory*, **45(2)**, 467-474, 1999.

[13] Ding C. and Helleseth T., New generalized cyclotomy and its applications, Finite Fields and Their Applications, **4(2)**, 140-166, 1998.

[14] Ding C., Pie D. and Salomaa A., Chinese Remainder Theorem, *Applications in Computing, Coding, Cryptography*, World Scientific, Singapore, 1996, chs. 2 and 6.

[15] Eupen M. and Lint J. van, On the minimum distance of ternary cyclic codes, *IEEE Transactions on Information Theory* **39(2)**, 409-416, 1993.

[16] Gauss C. F., *Disquisitions Arithmeticae*, Leipzig, Germany, 1801, English translation, New Haven, CT: Yale Univ. Press, 1966, reprinted, Berlin, Heidelberg and New York, Springer-Verlag, 1986.

[17] Kewat P. K. and Kumari Preeti, Cyclic codes from the second class two-prime whiteman's generalized cyclotomic sequence with order 6, *Cryptography and Communications*, **9(4)**, 475-499, 2017.

[18] Leon J. S., A probabilistic algorithm for computing minimum weight of large error-correcting codes, *IEEE Transactions on Information Theory*, **34**, 1354-1359, 1998.

[19] Leon J. S., Masley J. M. and Pless V., Duadic codes, *IEEE Transactions on Information Theory*, **30**, 709-714, 1984.

[20] Lidl R. and Niederreiter H., *Finite fields*, Cambridge Univ. Press, 1997.

[21] Lint J. van and Wilson R., On the minimum distance of cyclic codes, *IEEE Transactions on Information Theory* **32(1)**, 23-40, 1986.

[22] MacWilliams F.J., Cyclotomic numbers, coding theory and orthogonal polynomials, Discrete Math., **3**, 133-151, 1972.

[23] Macwilliams F. and Sloane N., *The theory of error correcting codes*, North-Holland Mathematical Lib., North-Holland, 1997.

[24] McEliece R. J. and Rumsey H., Euler product, cyclotomy and coding, *Journal of Number Theory*, **4**, 302-311, 1972.

[25] Pankaj and Pruthi M., Cyclic codes from generalized cyclotomic sequences of order 8, *Journal of Rajasthan Academy of Physical Sciences*, **15(3)**, 155-182, 2016.

[26] Pankaj and Pruthi M., Cyclic codes from generalized cyclotomic sequences of order 2^r, $r \geq 2$, *Journal of Information and Optimization Sciences*, **38(3-4)**, 621-646, 2017.

[27] Pankaj and Pruthi M., Cyclic codes from generalized cyclotomic sequences of order $2l$, $l \geq 2$, The *Journal of the Indian Academy of Mathematics*, **38(2)**, 183-209, 2016.

[28] Pless V., Q-codes, *Journal of Combinatorial Theory*, **43(2)**, 258-276. 1986.

[29] Pless V. and Huffman W. C., An introduction to algebraic codes, *in Handbook of Coding Theory*, V. Pless and W. C. Huffman, Eds. Amsterdam, the Netherlands, Elsevier, 1998.

[30] Pless V., Masley J. M. and Leon J. S., On weights in duadic codes, *Journal of Combinatorial Theory*, **44(1)**, 6-21, 1987.

[31] Pruthi M. and Arora S. K., Minimal Codes of Length $2p^n$ *Finite Fields and Their Applications* **5**, 177-187, 1999.

[32] Pruthi M. and Arora S. K., Minimal Codes of Prime-Power Length, *Finite Fields and Their Applications* **3**, 99-113, 1997.

[33] Pruthi M. and Pankaj, The minimum Hamming distances of the irreducible cyclic codes of length $l_1^{m_1} l_2^{m_2} \ldots l_r^{m_r}$, Journal of Discrete Mathematical Sciences and Cryptography, **19(5-6)**, 965–995, 2016.

[34] Storer T., Cyclotomy and difference sets, Markham, Chicago, 1967.

[35] Sun Y., Yan T. and Li H., Cyclic codes from the two-prime whiteman's generalized cyclotomic sequences with order 4, *CoRR* arxiv:1303.6378, 2013.

[36] Whiteman A. L., A family of difference sets, *Illionois J. Math* **6**, 107-121, 1962.

[37] Yan T., Lui Y., Sun Y., Cyclic codes from generalized cyclotomic sequences of order 6, Advances in Mathematics of Communications, **10(4)**, 707-723, 2016.