

SOLE CLASS OF MULTIFOLD WEIGHT THREEFOLD LINEAR CODES

K. Sreekha¹, P. Shakila Banu²

¹Department of Mathematics, Vellalar College for Women, Erode, India e-mail: rekhakarathi@gmail.com

²Department of Mathematics, Vellalar College for Women, Erode, India e-mail: shakimeeran10@gmail.com

Abstract: In this paper, the weight distributions of the multifold weight classes of threefold linear codes over GF (Q) are established and given. The irreducible cyclic codes are the source of the optimal codes in these codes. Additionally, they feature multiple codes that are optimal. AMS Subject Classification: 94B05, 68R01, 44A05. Key Words and Phrases: Cyclotomic Classes; Gaussian Periods; Linear Codes; Trace Function; Irreducible Cyclic Codes

Keywords: Cyclotomic Classes; Gaussian Periods; Linear Codes; Trace Function; Irreducible Cyclic Codes

1. INTRODUCTION

Let $Q = P^s$ and $\mu = Q^m$ in this paper, where P is a prime and m and s are positive integers. Let $l = (\mu - 1) / N$. Let $N \nmid l$ be a positive integer that divides $P - 1$. A linear $[l; k; d]$ code over Q is a k -dimensional subspace of Q^l with the lowest distance d . Let N be a primitive element of $GF(\mu)$. The set

$$C = \text{Tr}(\gamma), \text{Tr}(\gamma\theta), \dots \in \text{Tr}(\gamma\theta)^{l-1} : \gamma \in GF(\mu) \quad (1.1)$$

It is known as an irreducible cyclic $[l, m_0]$ code over GFQ when m_0 divides. The tracing function from GF (i) onto GFQ is represented by the symbols m and Tr . The weight distribution of irreducible cyclic codes is usually somewhat complicated [13]. In certain special circumstances, the weight distribution is known. the following list of cases.

- The codes have two weights when $N/(Q^i + 1)$ for some i being a divisor of $m/2$. This is known as the semi positive case. Goethals and Delsarte examined these codes [5]. McEliece [15], and McEliece and Baumert [2].
- $\text{Ord}_Q(N) = (N - 1)$, and N is a prime with $N \equiv 3 \pmod{4}$. The weight distribution was established by Mykkeltveit and Baumert [2].
- $Q \equiv 1 \pmod{N}$ and $\gcd(m, N - 1) = 1$, the weight distributions is known [6].
- N is even, $\gcd(n, N - 1) = 1$, $Q - 1 \equiv -N/2 \pmod{N}$ and $\gcd((r-1)/(Q-1) \pmod{N}, N) = 2$, the weight distribution is known [6].
- $N = 2$, the weight distribution was found by Baumert and McEliece [1].
- When $N=3$ and $N=4$, the distribution of weights is determined [6]. You may find the irreducible cyclic codes in [5, 9, 11, 12, 16, 18, 20, 21, 24].

Let

$$D = \{d_1, d_2, \dots, d_n\} \subseteq GF(\mu)^*.$$



Define a linear code of length n over $GF(q)$ by letting D be the defining set.

$$C = \{ \text{Tr}(y d_1), \text{Tr}(y d_2), \dots, \text{Tr}(y d_n) : y \in GF(\mu) \}. \quad (1.2)$$

Since every linear code over $GF(Q)$ may be formed in this manner, it is in fact a generic construction of linear codes. Depending on whatever defining set D is chosen, it can generate either excellent or terrible code.

The irreducible cyclic code of [1] is punctured from C_D up to coordinator permutations when D is a subset of the subgroups generated by β^N , where β is a generator of $GF(\mu)^*$.

The codes C_D punctured from the irreducible cyclic code in the semi-primitive case were addressed in [8], [7], and [23]. In addition to presenting a class of two weight codes, a class of three weight codes, and a class of four weight codes, the purpose of this work is to investigate the punctured code C_D in two more non-semi-primitive situations. Optimal codes are included in the two groups of codes discussed in this study.

2. PRELIMINARIES

The introduction of the multifold weight codes requires cyclotomic classes and Gaussian periods. We also give some supplementary results that are required for the sequel.

Assume that a primitive element of $GF(\mu)$ is B . For $j=0,1,\dots, N-i$, de-fine $C^{(N,\mu)}_j = B^+(B^N)$, where (B^N) denotes the subgroup of $GF(\mu)^*$ created by

$B^N A$. In $GF(\mu)$, the cyclotomic classes of order N are represented by $C^{(N,\mu)}_j A$.

The definition of the order N cyclotomic numbers is

$$(j, l)^{N,\mu} = [(C^{N,\mu}_j + 1) \cap C^{N,\mu}_l]$$

for all $0 \leq j \leq N-1$ [22]. The Gaussian period are defined by

$$\eta_j^{N,\mu} = \sum_{y \in C^{N,\mu}_j} \chi(y), \quad i = 0, 1, \dots, N-1$$

where the canonical additive character of $GF(\mu)$ is χ . We must ascertain the values of the Gaussian periods for our future applications. Although it is often highly difficult, there are some unique situations in which it is possible.

The definition of the period polynomials $\psi(N, \mu)(Y)$ is

$$\psi_{(N,\mu)}(Y) = \sum_{j=0}^{N-1} Y - \eta_j^{(N,\mu)}$$

According to [14], $\psi_{(N,\mu)}(Y)$ is a polynomial with integer coefficients. The proofs of the following six lemmas are available in [14].

3. The Weight formula for the code C_D

For every $y \in GF(\mu)$, it is convenient to define the weights in the code C_D of (1.2).

$$C_y = \{(Tr(yd_1), Tr(yd_2), \dots, Tr(yd_n))\}$$

The Hamming weight $W(C_y)$ of C_y is $n - N_y(0)$, where

$$N_y(0) = |\{1 \leq i \leq n : Tr(yd_i) = 0\}|$$

for each $y \in GF(\mu)$.

It is easily seen that for any $D = \{d_1, d_2, \dots, d_n\} \subseteq GF(\mu)$. We have

$$\begin{aligned} QN_y(0) &= \sum_{j=1}^n \sum_{\chi \in GF(Q)^*} B(\chi Tr(yd_j)) \\ &= n + \sum_{j=1}^n \sum_{\chi \in GF(Q)} \chi(xy d_j) \end{aligned} \quad (3.1)$$

where χ represents the canonical additive character of $GF(\mu)$ and B represents the canonical additive character of $GF(Q)$.

The dimension of C_D for arbitrary $D \subseteq GF(\mu)$ relies on the choice of D and can be found as follows [8].

4. The Class of Two Wight Codes

Lemma 4.1. Let $N = 2^3$, and define C_1 and d_1 as $\mu = C^2 + 4d^2$, $C \equiv 1 \pmod{2^3}$ and $P \equiv 1 \pmod{2^3}$, $\gcd(C, P) = 1$. These constraints determine C_1 and d_1 uniquely up to sign.

$$\psi_{2^3, \mu}(\chi) = \chi^2 - C\chi + d^2$$

Theorem 4.1. Let $P \equiv 1 \pmod{2^3}$ and $m \equiv 0 \pmod{2^3}$. Let C_1 and d_1 be given by $Q^{-12} = C^2 + 4d^2$, with $C_1 \equiv 1 \pmod{2^3}$ and $\gcd(C_1, P) = 1$. The code with the following weight distributive is then the set C_D .

Weight	Frequency
0	1
$\frac{\mu-1}{2} - c$	$\frac{\mu-1}{2} - d$
$\frac{\mu-1}{2} + c$	$\frac{\mu-1}{2} + d$

The dual code $C_D^\perp$ of the code C_D has parameters

$$\left(\frac{\mu-1}{2(Q-1)}, \frac{\mu-1}{2(Q-1)} - m, d^\perp \right), \quad d^\perp \geq 3$$

Proof. From (3), we have

$$Q N_y(0) - n = \sum_{j=1}^n \sum_{\chi \in GF(Q^*)} \chi(xy d_j) = \eta_i^{(N, \mu)}$$

whenever $y \in C_i^{(N, \mu)}$. Hence

$$W(C_y) = n - N_y(0)$$

The weight distribution from lemma 4.1 follows. m is the code's dimension. $d_1 \neq$

0 since $\gcd(C_1, P) = 1$. Consequently, $C^2 < \sqrt{\mu}$. As a result, C_D has a dimension of m , and $W(C_y) > 0$ for each nonzero $y \in GF(\mu)$. All we have to show is that $d^\perp \geq 3$. Any point of distinct d_j and d_i is linearly independent over $GF(q)$ since they represent separate cosets of the factor group $C^{(N, \mu)}/GF(Q^*)$.

Example 4.1 Let $Q = 17$ and $m = 2$. The C_D is a $[8, 2, 6]$ code over $GF(17)$ with the following weight distribution $1.16x^2 + 10x^9$

5. The class of Three Weight Distribution

Lemma 5.1. Let $N = 2^3$. Let c and d be defined by $4\mu = C^2 + 27d^2$, $C \equiv 1 \pmod{8}$, and if $P \equiv 1 \pmod{8}$, then $\gcd(C, P) = 1$. These limitations uniquely identify C and d up to sign, therefore we have

$$\chi_{2^3, \mu} = x^3 - \frac{c}{\gamma} x^2 + \left(3\mu - \frac{9}{4} x - c\mu - \frac{27d}{8}\right)$$

Assume that $P \equiv 1 \pmod{8}$, $m \equiv 0 \pmod{8}$, and $N = 2^3$. Next, we get

$$\frac{r-1}{g-1} \pmod{N} \equiv m \pmod{2^3} \equiv 0.$$

Observe that any element of $GF(Q^*)$ may be written as $\gamma^i(\mu-1)/(Q-1)$, where γ is a fixed primitive element of $GF(\mu)$. Thus, $GF(Q)^* \subseteq C^{(N, \mu)}$

Theorem 5.1. Let $P \equiv 1 \pmod{2^3}$ and $m \equiv 0 \pmod{2^3}$. Let C and d be given by

$$4Q^{m/3} = C^2 + 27d^2, \quad C \equiv 1 \pmod{2^3},$$

and $\gcd(C, P) = 1$. The code having the following weight distribution is then represented by the code

Weight	Frequency
0	1
$\mu + \frac{c-3-9d}{6}$	$\frac{\mu-1}{5}$
$\mu + \frac{c-3+9d}{6}$	$\frac{\mu-1}{5}$
$\mu - \frac{c+6}{6}$	$\frac{\mu-1}{5}$

The dual code $C^\perp$ of the code C_D has parameters

$$\left[\frac{\mu-1}{3(Q-1)}, \frac{r-1}{3(Q-1)}, m, d^\perp \right]$$

where $d^\perp \geq 3$.

Proof. Since $d_1, d_2, \dots, d_n$ form a complete set of coset representation of the factor group $C^{(N,\mu)}/GF(Q)^*$, we have

$$\bigcup_{x \in GF(Q)^*} \{xd_1, xd_2, \dots, xd_n\} = C_0 \quad N, \mu \quad By(3)$$

we have

$$Q \ N_y(0) - n = \sum_{j=1}^n \sum_{x \in GF(Q)^*} \chi(xy d_j) = \sum_{z \in C^{(N,\mu)}} \chi(xz) = z = \eta^{(N,\mu)}_i$$

whenever $y \in C^{(N,\mu)}_i$

The equation is $W(C_y) = n - N_y(0)$. from lemma 5.1.

The code's dimension C_D is denoted by m . $gcd(C, P) = 1$ yields $\mu - C^{y^2} \neq 0$. μ

Notably, $4\mu^{y^2} = C^2 + 27d^2$, $C \equiv 1 \pmod{2^3}$, and $gcd(C, P) = 1$. Therefore, for every nonzero $y \in GF(\mu)$, $W(C_y) > 0$ and C_D has dimension m . They to show that it is sufficient that $d^4 \geq 3$. Since they represent separate cosets of the factor group $C^{(N,\mu)}/GF(Q)^*$, each pair of distinct d_j and d_i is linearly independent over $GF(Q)$.

Example 5.1 Let $Q = 19$ and $m = 3$, then C_D is a $[45, 3, 10, 10]$ code over $GF(19)$ using the weight distributions listed below $W(x) = 1 + 6x^{109/6} + 66x^{127/6} + 6x^{13/6}$ $\square$

6. The class of Four Weight Distribution

Lemma 6.1. Let $N = 2^3$, and let C_2 and d_2 be defined by $\mu = C^2 + 4d^2$, with $C_2 \equiv 1 \pmod{2^3}$ and $P \equiv 1 \pmod{2^3}$. Consequently, $gcd(C_2, P) = 1$. These limitations determine d_2 up to sign and C_2 uniquely..

$$\psi_{2^3, \mu^4} x^4 - 2C_2 x^2 + (2\mu - 4d_2) x - 4C_2 \mu x - 4\mu^2$$

Theorem 6.1. Think about $P \equiv 1 \pmod{2^3}$ and $m \equiv 0 \pmod{2^3}$. Assume that $Q^{m/2} = C^2 + 4d^2$, $C_2 \equiv 1 \pmod{2^3}$ provides C_2 and d_2 , and that $gcd(C_2, P) = 1$. The code C_D has the weight distribution shown below. The dual code $C^\perp$ of the code C_D has parameters,

$$\frac{\mu-1}{4(Q-1)} \quad \frac{\mu-1}{4(Q-1)} \quad -m \quad 4^1$$

where $d^4 \geq 3$

Weight	Frequency
0	1
$\frac{\mu-1}{4} - \frac{C_2}{4} - d_2$	$\frac{\mu-1}{4} - d_2$
$\frac{\mu-1}{4} - \frac{C_2}{4} + d_2$	$\frac{\mu-1}{4} + d_2$
$\frac{\mu-1}{4} + \frac{C_2}{4} - d_2$	$\frac{\mu-1}{4} - d_2$
$\frac{\mu-1}{4} + \frac{C_2}{4} + d_2$	$\frac{\mu-1}{4} + d_2$

Proof. By (3) we have

$$W(C_y) = \sum_{j=1}^n \sum_{x \in GF(Q)^*} \chi(xy d_j) = \eta^{(N, \mu)}$$

where $y \in C^{(N, \mu)}$. Hence $W(C_y) = n - N(0)$.

from lemma 6.1.

Since $\gcd(C_2, P) = 1$, $d_2 = 0$, the code has dimension m .

? The dimension of C_D is m , and for each nonzero y in $GF(\mu)$, $W(C_y) >$

0. To show that $d^{\perp} \geq 3$ is sufficient, any pair of distinct d_j is linearly independent over $GF(Q)^*$ since they represent different cosets of the factor group $C^{(N, \mu)}/GF(Q)^*$.

Example 6.1 Let $Q = 17$ and $m = 4$. Then C_D is a $[24, 4]$ code over $GF(17)$ with the following weight distribution $1 + 2x^{0.5} + 6x^{0.5} + 2x^{3.5} + 6x^{4.5}$

7. Conclusion

We infer that the optimality of secret sharing schemes is accelerated by implementing the single class of two weight, three weight, and four weight triple binary linear codes [22].

References

1. L.D. Baumert, R.J. McEliece, Weights of irreducible cyclic codes, Information and Control, 20, 158–175 (1972).
2. L.D. Baumert, J. Mykkeltveit, Weight distributions of some irreducible cyclic codes, DSN Progress Report, 16, 128–131 (1973).
3. A.R. Calderbank, J.-M. Goethals, Three-weight codes and association schemes, Philips J. Res., 39, 143–152 (1984).
4. N.J. Calkin, J.D. Key, M.J. de Resmini, Minimum weight and dimension formulas for some geometric codes, Designs, Codes and Cryptography, 17, 105–120 (1999).
5. P. Delsarte, J.-M. Goethals, Irreducible binary cyclic codes of even dimension, Proc. Second Chapel Hill Conf. on Combinatorial Mathematics and Its Applications, Univ. North Carolina, Chapel Hill, NC, pp. 100–113 (1970).
6. C. Ding, The weight distribution of some irreducible cyclic codes, IEEE Trans. Inform. Theory (to appear).
7. C. Ding, J. Luo, H. Niederreiter, Two-weight codes punctured from irreducible cyclic codes, In: Y. Li, S. Ling, H. Niederreiter, H. Wang, H. Xing.
8. S. Zhang (eds.), Proc. First International Workshop on Coding Theory and Cryptography, World Scientific, Singapore, pp. 119–124 (2008).
9. C. Ding, H. Niederreiter, Cyclotomic linear codes of order 3, IEEE Trans. Inform. Theory, 53, 2274–2277 (2007).
10. J.M. Goethals, Factorization of cyclic codes, IEEE Trans. Inform. Theory, 13, 242–246 (1967).
11. M. Grieser, On s-sums-sets (s odd) and three-weight projective codes, Proc. AAECC, pp. 68–76 (1986).
12. T. Helleseth, T. Klve, J. Mykkeltveit, The weight distribution of irreducible cyclic codes with block length $n_1(q-1)/N$, Discrete Math., 18, 179–211 (1977).
13. P. Langevin, A new class of two-weight codes, In: S. Cohen, H. Niederreiter (eds.) Finite Fields and Applications, Cambridge University Press, pp. 181–187 (1996).
14. F. MacWilliams, J. Seery, The weight distributions of some minimal cyclic codes, IEEE Trans. Inform. Theory, 27, 796–806 (1981).
15. G. Myerson, Period polynomials and Gauss sums for finite fields, Acta Arith., 39, 251–264 (1981).
16. R.J. McEliece, A class of two-weight codes, Jet Propulsion Laboratory Space Program Summary, 37–41 IV, 264–266 (1966).
17. R.J. McEliece, Irreducible cyclic codes and Gauss sums, In: Combinatorics, Part 1: Theory of Designs, Finite Geometry, and Coding Theory, Math. Centrum Tracts, vol. 55, pp. 179–196, Amsterdam (1974).
18. R.J. McEliece, H. Rumsey Jr., Euler products, cyclotomy, and coding, J. Number Theory, 4, 302–311 (1972).
19. M.J. Moisio, K.O. Vninen, Two recursive algorithms for computing the weight distribution of certain irreducible cyclic codes, IEEE Trans. Inform. Theory, 45, 1244–1249 (1999).
20. D.K. Ray-Chaudhuri, Q. Xiang, New necessary conditions for abelian Hadamard difference sets, J. Statist. Plann. Inference, 62, 69–79 (1997).
21. B. Schmidt, C. White, All two-weight irreducible cyclic codes?, Finite Fields Appl., 8, 1–17 (2002).
22. R. Segal, R.L. Ward, Weight distributions of some irreducible cyclic codes, Mathematics of Computation, 46, 341–354 (1986).
23. P. Shakila Banu, K. Sirekha, Two classes of two weight threefold linear codes, J. Appl. Math. Informatics, 43, 151 – 161 (2025).
24. T. Storer, Cyclotomy and Difference Sets, Markham, Chicago (1967).
25. M. Van der Vlugt, On the weight hierarchy of irreducible cyclic codes, J. Combin. Theory Ser. A, 71, 159–167 (1995).