Two Classes of Three weight Linear Codes:

Srirekha.K (Assistant Professor)
PG Department of Mathematics
Vellalar College for Women, Erode,
TamilNadu, India.
rekha@vcw.ac.in

Arthivasundhra.A.S
PG Department of Mathematics,
Vellalar College for Women, Erode,
TamilNadu, India
22pms107@vcw.ac.in

Pratheusha.P
PG Department of Mathematics,
Vellalar College for Women, Erode,
TamilNadu, India
22pms127@vcw.ac.in

ABSTRACT

In many communication systems, linear codes are employed to transmit and receive data with little error. Here, we provide a technique for converting two classes of two-weight linear codes into two classes of three-weight linear codes. We specifically offer a building method that keeps the linearity condition while adding a third weight to the original two-weight codes. The resulting three-weight codes are suited for use in applications that need higher dependability because it has been demonstrated that they have stronger error-correcting capabilities than the original two weight codes. Our work aims in the creation of stronger, more reliable linear codes to use in many communication and storage applications

I INTRODUCTION

Let u be a power of $\wp$ and $\wp$ be a prime. Let F_u stand for the u-element finite fields. A t-dimensional subspace of $F_{\wp}^{m}$ with a minimum Hamming distance E is a [m, t, E] linear code C over F_p. If the parameters of a [m, t, E] linear code satisfy a bound on linear codes, the code is optimal; if [m, t, E + 1] satisfy the bound on linear codes, it is almost optimal. The number of codewords with Hamming weight i in a D code is indicated by the letter B_j. The D weight enumerator, which is defined as

$$1+B_{1y}+\ldots\ldots\ldots+B_nY^n.$$

The weight distribution of the code C is the sequence $(1,B_1+\ldots\ldots+B_n)$.The weight distribution of a code can be used to determine a code's capacity for mistake correction and its likelihood of error detection. Suppose F=$(E_1,E_2\ldots,E_n)\subseteq F_u$.The tracing function from F_u onto $F_{\wp}$ is represented by T_u. The formula is used to define a $\wp$-ary linear code of length n.

$$D_F=\{(\mathrm{Tu}(yE_1),\mathrm{Tu}(yE_2),\ldots\mathrm{Tu}(yE_n)): y\in F_u\}$$

F is the defining set of this code D_F.

In the field of coding theory, three weight linear codes hold a lot of attention. Strongly regular graphs and partial geometrics are two objects in several branches of mathematics that are closely related to three-weight linear codes.

II.PRELIMINARIES

In this research, we obtain two classes of three-weight binary or ternary linear codes, which can be generated using novel parameters. In this correspondence, we use the following notations.

$\wp$	prime number,
s	positive integer such that gcd (s,p) = 1,
n	positive integer which is no less than 2,
t	the least integer such that $p^t\equiv -1\ (mod\ n)$,
T_u	trace function from F_r onto F_p,
$\mathcal{R}(y)$	real part of y

$Z_{\wp}$ primitive $\wp - th\, root\; of\; complex\; unity,$

$\gamma_j^{(M,r)}$ Gauss periods of order M over F_u

$q = \wp^{2t},$

u = $q^s,$

E = $\frac{r-1}{n}$

We give a succinct overview of the main characters, Gaussian periods and Walsh transform

Given that u is a power of a prime $\wp$. Let F_u be a finite field with u elements. Let T_u be the tracing function from F_u to $F\wp$. and ζ_p be a $\wp$ -th primitive root of unity. The definition of F_u canonical additive character is

$$\varphi : \text{Fu} \to D^*$$

$$y \longmapsto \zeta_{\wp}^{Tr(y)}$$

Given by is the orthogonal property of additive characters.

$$\sum_{y \epsilon F_u} \varphi(ay) = \begin{cases} 0, if\; a \epsilon F_u^* \\ u, if\; a = 0 \end{cases}$$

Let u-1 = M_n and $F_u^* = \langle \beta \rangle$ Define cyclotomic classes of order M of F_u by

$$D_i^{(M,u)} = \beta^j \langle \beta^m \rangle, j = 0,1, \dots \dots ., M - 1.$$

The Gauss periods of order M are defined by

$$\gamma_j^{(M,u)} = \sum_{y \epsilon D_j{}^{(M,u)}} \varphi(x),$$

Where φ is the canonical additive characters of F_u. For M = 2,3,4, the semi primitive case, the index 2 case.

The function f(y) should range from F_u to $F\wp$. You can specify the Walsh transform of f(y) with

$$\hat{f}(\text{c}) = \sum_{y \epsilon F_u} \zeta_{\wp}^{f(y) - T_u(cy)},\; c \,\epsilon\, F_u\,,$$

Where $F\wp$ components are regarded as integers modulo $\wp$. The relationship between a class of linear code and Boolean functions was established using the Walsh transform.

1.1 The First Construction

Let t be the least positive integer such that $\wp^t \equiv -1 (mod\; n)$. With gcd$(\wp, s) = 1, let\; f(y) = T_u(y^E)$ be linear code a function from F_u to $F\wp$ For u=q^s=p^{2km} and E = $\frac{r-1}{n}$. Determine the location defining of the set of define a class of $\wp$ - ary

$$D_F = \left\{ \left(T_u(y_{E_1}), \dots \dots \dots, T_u(y_{E_s}) \right) : y \epsilon F_u \right\},$$

Where the defining set is

$$\text{F} = \{e_1 \dots \dots \dots \dots e_n\} = \{y \epsilon F_u^* : f(y) = 0\},$$

We start computing $\hat{f}(0)$ to the length of D_F. Since E|(u-1), we get

$$\hat{f}(0) = 1+ \sum_{y\varepsilon F_u^*} \zeta_{\wp}^{H_r(b^d)}$$
$$= 1 + E \sum_{y\epsilon H_0^{(E,u)}} \zeta_{\wp}^{T_u(y)}$$
$$= 1 + E_{\gamma_0^{(E,U)}}$$

We get where $y_0^{(E,u)}$ is an ordered E Gauss period. The method to find the values of $\gamma_0^{(E,u)}$ for a particular special number n is provided in the sections that follow.

1.1.1 Lemma

Let $\wp$, u, E, t be $y_0^{(E,u)}$ are listed for several cases in table 1.1.1.1

Proof

The trace function from F_u to $F_{\wp}$ and from F_u to F_q are denoted by T_q and $T_{r\backslash q}$ respectively, and we than have

$$T_u(y) = T_q(T_{u\backslash q}(y)) \text{ for } y \epsilon F_u$$

$$y_0^{(E,u)} = \sum_{y\epsilon D_0^{(E,u)}} \zeta_{\wp}^{T_u(y)}$$

$$= \sum_{y\varepsilon D_0^{\left(\frac{q-1}{h},q\right)}} \zeta_{\wp}^{sT_q(y)}$$

We only provide the proof in the following for the the of following for the value of $\wp = 2, n = 3$. In other situations, we can provide the value for $y_0^{(E,u)}$

Let $\wp = 2, t = 3$, then z = 1 and q = 4. The smallest polynomial of a 3rd element is ξ_3 $over$ F_2

$$\xi_3 = x^2 + x + 1$$

This suggests that $T_4(\xi^3) = -1$. S is unusual because gcd(S,2) = 1

$$y_0^{\left(\frac{4^m-1}{3},4^m\right)} = \sum_{y\varepsilon D_0^{(1,4)}} (-1)^{sT_4(y)} = 1-1-1 = -1$$

Table 1.1.1.1 Values of $\gamma_0^{(E,u)}$

$\wp$	n	u	$\gamma_0^{(E,u)}$
2	3	2^{2s}	-1
2	5	2^{4s}	-3
2	9	2^{6s}	5
2	11	2^{10s}	-9
3	4	3^{2s}	1
3	5	3^{4s}	$\xi_3^s + 4\xi_3^{2s}$
3	7	3^{6s}	$1+6\xi_3^{2s}$
3	14	3^{6s}	$1+6\xi_3^s + 7\xi_3^{2s}$

Case $\wp = 2$

For the sections when $\wp = 2, D_F\ is\ defined\ as\ D_F = \left\{\left(T_u\left(y_{E_1}\right), \dots \dots \dots, T_u\left(y_{E_s}\right)\right) : y\epsilon F_u\right\}$, and its weight distribution is given.

Let $\gamma_0 = |\{y \in F_u : f(y) = 0\}|$.

$$\gamma_0 = \frac{1}{2}\sum_{y_1\epsilon F_u}\sum_{y_2\epsilon F_2}\sum_{y_3\epsilon F_2}(-1)^{y_2 f(y_1)}(-1)^{y_3 f(y_1)}$$

$$= \frac{u}{2}+\frac{u}{2}+\frac{1}{2}\sum_{y\epsilon F_u}(-1)^{f(y)}$$

$$= \frac{u}{2}+\frac{u}{2}+\frac{1}{2}\hat{f}(0)$$

$$= \frac{2u}{2}+\frac{1}{2}(1+E\gamma_0^{(E,u)})$$

$$= u+\frac{1}{2}(1+E\gamma_0^{(E,u)})$$

The length m = $m_0 - 1$. Hence, from lemma 1.1.1, we obtain the length of the linear code D_F in the following.

1.1.2 Lemma

For $\wp = 2$,the length the linear code D_F equals to

$$m = u - \frac{1}{2} + \frac{u-1}{2n}\gamma_0^{(E,u)}$$

In particular, for $n = 3,5,9,11$ obtained below:

When n = 3

$$m = u - \frac{1}{2} + \frac{u-1}{2n}\gamma_0^{(E,u)}$$

$$= u - \frac{1}{2} + \frac{1}{6}(u-1)(-1)$$

$$= u - \frac{1}{2} + \frac{1}{6}(-u+1)$$

$$= u - \left(\frac{1}{2} - \frac{1}{6}\right)(u - 1)$$

$$= u - \left(\frac{3+1}{6}\right)\text{(u-1)}$$

$$= u - \frac{2}{3}(u - 1)$$

$$= u - \frac{2u}{3} + \frac{2}{3}$$

$$= \frac{3u-2u}{3} + \frac{2}{3}$$

$$= \frac{u}{3} + \frac{2}{3}$$

$$= \frac{u + 2}{3}$$

when n = 5

$$m \quad = u - \frac{1}{2} + \frac{u - 1}{2n}\gamma_0^{(E,u)}$$

$$= \ u - \frac{1}{2} + \frac{1}{10}(u - 1)(-3)$$

$$= u - \frac{1}{2} + \frac{1}{10}(-3u + 3)$$

$$= u - \left(\frac{1}{2} - \frac{1}{10}\right)(u - 3)$$

$$= u - \left(\frac{5+1}{10}\right)\text{(3u-3)}$$

$$= u - \frac{3}{5}(3u - 3)$$

$$= u - \frac{9u}{5} + \frac{9}{5}$$

$$= \frac{5u-9u}{5} + \frac{9}{5}$$

$$= \frac{-4u}{5} + \frac{9}{5}$$

$$= \frac{-4u + 9}{5}$$

when n = 9

$$m = u - \frac{1}{2} + \frac{u-1}{2n}\gamma_0^{(E,u)}$$

$$= u - \frac{1}{2} + \frac{1}{18}(u-1)(5)$$

$$= u - \frac{1}{2} + \frac{1}{18}(-5u+5)$$

$$= u - \left(\frac{9-1}{18}\right)(5u - 5)$$

$$= u - \frac{4}{9}(5u-5)$$

$$= u - \frac{20u}{9} + \frac{20}{9}$$

$$= \frac{9u-20u}{9} + \frac{20}{9}$$

$$= \frac{-11u}{9} + \frac{20}{9}$$

$$= \frac{-11u+20}{9}$$

when n = 11

$$m = u - \frac{1}{2} + \frac{u-1}{2n}\gamma_0^{(E,u)}$$

$$= u - \frac{1}{2} + \frac{1}{22}(u-1)(-9)$$

$$= u - \frac{1}{2} + \frac{1}{22}(-9u+9)$$

$$= u - \left(\frac{1}{2} - \frac{1}{22}\right)(9u+9)$$

$$= u - \left(\frac{11+1}{22}\right)(9u-9)$$

$$= u - \frac{6}{11}(9u-9)$$

$$= u - \frac{54u}{11} + \frac{54}{11}$$

$$= \frac{11u-54u}{11} + \frac{54}{11}$$

$$= \frac{-43u}{11} + \frac{54}{11}$$

$$= \frac{-43u+54}{11}$$

Table 1.1.2.1 Values of m

$\wp$	n	u	m
2	3	2^{2s}	$\frac{u+2}{3}$
2	5	2^{4s}	$\frac{-4u+9}{5}$
2	9	2^{6s}	$\frac{-11u+20}{9}$
2	11	2^{10s}	$\frac{-43u+54}{11}$

Case $\wp = 3$

Consider the case $\wp = 3$ and determine the weight distribution of this ternary code.

$$\text{Let } \gamma_0 = \ |\{y \varepsilon F_u : T_u(y^E) = 0\}|.$$

$$\gamma_0 = \ \frac{1}{3} \sum_{y_1 \epsilon F_u} \sum_{y_2 \epsilon F_3} \sum_{y_3 \epsilon F_3} \zeta_3^{y_2 T_u(y_1^E)} \zeta_3^{y_3 T_u(y_1^E)}$$

$$= \frac{u}{3} + \frac{u}{3} + \frac{1}{3} \textstyle\sum_{y \varepsilon F_u} \zeta_3^{T_u(y^E)} + \frac{1}{3} \textstyle\sum_{y \varepsilon F_u} \zeta_3^{-T_u(y^E)}$$

$$= \frac{u}{3} + \frac{u}{3} + \frac{1}{3}\ \hat{f}(0) + \frac{1}{3} \overline{\hat{f}(0)}$$

$$= \frac{2u}{3} + \frac{1}{3} + \frac{1}{3} + \frac{1}{3}\ E\gamma_0^{(E,u)} + \frac{1}{3}\ E\gamma_0^{(E,u)}$$

$$= \frac{2u+2}{3} + \frac{2E}{3} \mathcal{R}(\gamma_0^{(E,u)})$$

Where the symbol denotes the complex conjugate and the symbol $\mathcal{R}(y)$ represents the real part of y. The length m=$m_0 - 1$. By Lemma 1.1.5 we have the following result.

1.1.3 Lemma

For $\wp = 3$, the length of the ternary linear code D_F equals to

$$m = \frac{u-1}{3} + \frac{2(u-1)\mathcal{R}(\gamma_0^{(E,u)})}{3n}$$

In particular, when n = 4,5,7,14 are derived as same as in section (1.1.3)

1.2 The Second Construction

Let t be the least positive integer such that $p^t \equiv -1(mod\ t)$. For u = $q^s = q^{2ts}$ and $E = \frac{r-1}{n}$ with gcd$(\wp, s) = 1$, let f (y) = $T_u(x^E)$ be a function from $F_u\ to\ f_\wp$. Define a class of $\wp - ary$ linear code by

$$D_F = \left\{\left(T_u\left(y_{E_1}\right), \dots \dots \dots, T_u\left(y_{E_s}\right)\right) : y \epsilon F_u\right\},$$

In which the defining set is

$$\text{F} = \{E_1 \dots \dots \dots \dots E_n\} = \left\{y \epsilon F_u\ : T_u(y^E) = 1\right\},$$

Case $\wp = 2$

The binary linear code D_F has a length of

$$\begin{aligned} m &= |\{y \epsilon F_u : T_u(y^E) = 1\}| \\ &= \frac{1}{2} \sum_{y_1 \epsilon F_u} \sum_{y_2 \epsilon F_2} \sum_{y_3 \epsilon F_2} (-1)^{y_2(T_u(y^d)-1)} (-1)^{y_3(T_u(y^E)-1)} \\ &= \frac{u}{2} + \frac{u}{2} - \frac{1}{2} \sum\nolimits_{y \epsilon f_u} (-1)^{T_r(y^E)} \\ &= \frac{u}{2} + \frac{u}{2} - \frac{1}{2} \hat{f}(0) \\ &= \frac{2u}{2} - \frac{1}{2} \hat{f}(0) \\ &= u - \frac{1}{2} - \frac{1}{2} E \gamma_0^{(E,u)} \\ &= u - \frac{1}{2} - \frac{u-1}{2n}\ \gamma_0^{(E,u)} \end{aligned}$$

Specially when n = 3,5,9,11 are derived below

Where n = 3

$$\begin{aligned} m &= u - \frac{1}{2} - \frac{u-1}{2n}\ \gamma_0^{(E,u)} \\ &= u - \frac{1}{2} - \frac{1}{6}(u-1)(-1) \\ &= u - \frac{1}{2} - \frac{1}{6}(-u+1) \\ &= u - \frac{1}{2} - \frac{1}{6}(u-1) \\ &= u - 1\left(\frac{3-1}{6}\right)(u-1) \\ &= u - \frac{1}{3}(u-1) \\ &= u - \frac{u}{3} + \frac{1}{3} \\ &= \frac{3u-u}{3} + \frac{1}{3} \end{aligned}$$

$$= \frac{2u}{3} + \frac{1}{3}$$

$$m = \frac{2u+1}{3}$$

Where n = 5

$$m \quad = u - \frac{1}{2} - \frac{u-1}{2n}\ \gamma_0^{(E,u)}$$

$$= u - \frac{1}{2} - \frac{1}{10}(u-1)(-3)$$

$$= u - \frac{1}{2} - \frac{1}{10}(-3u+3)$$

$$= u - \frac{1}{2} - \frac{1}{10}(3u-3)$$

$$= u - \frac{1}{2}\left(\frac{5-1}{10}\right)(3u-3)$$

$$= u - \frac{2}{5}(3u-3)$$

$$= u - \frac{6u}{5} + \frac{6}{5}$$

$$= \frac{5u-6u}{5} + \frac{6}{5}$$

$$= \frac{-u}{5} + \frac{6}{5}$$

$$m \quad = \frac{-u+6}{5}$$

Where n =9

$$m \quad = u - \frac{1}{2} + \frac{u-1}{2n}\gamma_0^{(E,u)}$$

$$= \ u - \frac{1}{2} - \frac{1}{18}(u-1)(5)$$

$$= \ u - \frac{1}{2} + \frac{1}{18}(-5u+5)$$

$$= u - \left(\frac{9+1}{18}\right)(\ 5u - 5\ )$$

$$= u - \frac{5}{9}(5u-5)$$

$$= u - \frac{25u}{9} + \frac{25}{9}$$

$$= \frac{9u-25u}{9} + \frac{25}{9}$$

$$= \frac{-16u}{9} + \frac{25}{9}$$

$$m \quad = \frac{-16u+25}{9}$$

Where n = 11

$$m \quad = u - \frac{1}{2} - \frac{u-1}{2n}\gamma_0^{(E,u)}$$

$$= u - \frac{1}{2} - \frac{1}{22}(u-1)(-9)$$

$$= u - \tfrac{1}{2} + \tfrac{1}{22}(-9u+9)$$

$$= u - \left(\frac{1}{2} - \frac{1}{22}\right)(9u-9)$$

$$= u - \left(\tfrac{11-1}{22}\right)(9u\text{-}9)$$

$$= u - \frac{5}{11}(9u-9)$$

$$= u - \frac{45u}{11} + \frac{45}{11}$$

$$= \tfrac{11u-45u}{11} + \tfrac{45}{11}$$

$$= \frac{-34u}{11} + \frac{45}{11}$$

$$m \quad = \frac{-34u+45}{11}$$

Table 1.2.1.1 values of m of $D_F\ for\ \wp = 2$

$\wp$	n	u	m
2	3	2^{2s}	$\frac{2u+1}{3}$
2	5	2^{4s}	$\frac{-u+6}{5}$
2	9	2^{6s}	$\frac{-16u+25}{9}$
2	11	2^{10s}	$\frac{-34u+45}{11}$

CONCLUSION

It is possible to build secret sharing systems using any linear code over F$\wp$. We would like to have linear codes D such the we could obtain secret sharing schemes with intriguing access structures.

$$\frac{W_{min}}{W_{max}} > \frac{\wp - 1}{\wp}$$

Where W_{min} and W_{max} stands for the linear codes minimum and maximum nonzero weights, respectively. The codes that have been changed might be useful in fields like cryptography and data storage. Overall, our findings illustrate the possibility for additional search in this field and emphasize the significance and adaptability of linear codes in coding theory.

REFERENCES

1. A.R. Calderbank, J.M. Kantor, The geometry of two-weight codes,Bull.Lond. Math. Soc. 18 (1986)99-122.

2. F. De Clerk, M. Delanote, Two-weight codes, partial geometries and Steiner systems,Des. Codes Cryptogr. 21 (2000) 87-98.

3. K. Ding, C. Ding, Binary linear codes with three weights,IEEE Commun. Lett. 18 (11) (2014) 1879-1882.

4. Z. Heng, Q. Yue, A class of binary linear codes with at most three weights,IEEE Commun. Lett. 19 (9) (2015) 1488-1491.

5. C. Li, Q. Yue, F. Li, Hamming weights of the duals of cyclic codes with two zeros,IEEE Trans. Inf. Theory 56 (6) (2014) 25682570.

6. C. Li, Q. Yue, The Walsh transform of a class of monomial functions and cyclic codes, Cryptogr. Commun. 7 (2015) 217-228

7. J. Yuan, C. Ding, Secret sharing schemes from three classes of linear codes,IEEE Trans. Inf. Theory 52 (1) (January 2006) 206-212.

8. Z. Zhou, C. Ding A class of three-weight cyclic codesFinite Fields Appl., 25 (2014),pp. 79-93.

9. X. Zeng, L. Hu, W. Jiang, Q. Yue, X. Cao, The weight distribution of a class of p-arycyclic codes, Finite Fields Appl. 16 (1) (January 2010) 5673.