Proceedings of the Jangjeon Mathematical Society
29 (2026), No. 2, pp. 287 - 302

www.jangjeon.or.kr
http://dx.doi.org/10.17777/pjms2026.29.2.011

A CLASS OF PROJECTIVE LINEAR CODES AND ITS APPLICATIONS

J. PRABU, J. MAHALAKSHMI, AND S. SANTHAKUMAR

Abstract. This paper presents families of q-ary projective linear codes, where q represents a prime power. Certain classes of linear codes obtained over $\mathbb{F}_q$ yield optimal projective codes that meet the Griesmer bound. Building upon the properties of our constructed codes, we explored their applicability in constructing strongly regular graphs and secret-sharing schemes.

2000 Mathematics Subject Classification 11T71, 94B05, 94B25.
Keywords and phrases. Simplex codes, weight distribution, Gray map, secret sharing schemes, strongly regular graphs.

Submission Date: 30 January 2024

1. Introduction

Researchers have dedicated significant research efforts to explore error-correcting codes over finite fields, particularly emphasising their practical applications in computer and communication systems, data storage devices, and consumer electronics across various domains. Codes with few weights over Galois fields gained significant attention due to their remarkable utility in secret sharing schemes [1], association schemes [2], authentication codes [3], and other related domains. One noteworthy connection that has been established is the natural relationship between projective two-weight codes and strongly regular graphs. A partial census was presented in the seminal paper by Calderbank et al. [4] to provide an overview of existing constructions based on the arithmetic of finite fields. Delsarte first explored the interplay between these two concepts in 1972 [5], and further solidified in the comprehensive work by Brouwer et al. [6].

*J. Mahalakshmi.

Fisher's significant research in 1942, as published in [7], represented the first discovery of the binary simplex code while studying statistical designs. A few years later in 1945 [8], Fisher extended the parameters of the code for any prime powers. MacDonald developed the binary MacDonald codes in 1960 [9]. The investigation of the generalized q-ary form of the MacDonald code over the finite field $\mathbb{F}_q$ was discussed in [10].

Let q be a prime power and, let $\mathbb{F}_q$ be a finite field of order q. A k-dimensional subspace of the vectors space $\mathbb{F}_q^n$ is called an $[n,k]$ linear code over $\mathbb{F}_q$. Let $x, y \in \mathbb{F}_q^n$, then the *Hamming distance* between the vectors x and y is the number of positions where their corresponding entries differ. It is represented by $d(x,y)$. Clearly, $d(x,y) = wt(x-y)$, the number of non-zero entries in $x-y$. The minimum distance d of a code C is the smallest possible Hamming distance between any two distinct codewords within C, that is,

$$d = \min\{d(x,y) \mid x, y \in C,\ x \neq y\}.$$

The minimum Hamming distance of a code plays a crucial role in its error-correcting performance with nearest neighbour decoding. It dictates the maximum number of errors that can be successfully corrected, which is given by $\left\lfloor \frac{(d-1)}{2} \right\rfloor$ errors using nearest neighbourhood decoding. Almost all codes in classical coding theory are defined for the Hamming distance.

Balanced channels, where individual symbol errors occur with equal likelihood, provide the ideal playground for Hamming distance codes to showcase their effectiveness. The weight distribution of code C is represented by the sequence $(1, A_1, A_2, \cdots, A_n)$, where A_i indicates the number of codewords of Hamming weight i and its weight enumerator is $1+A_1x+A_2x^2+\cdots+A_nx^n$. The study of weight distribution holds great interest as it offers valuable insights into the error detection and correction capabilities of a code and it enables the calculation of error probabilities associated with the aforementioned detection and correction processes for a given code. If the code C weight distribution has t non-zero terms, then C is called t-weight code. A linear code C is projective if its generator matrix has projectively distinct columns, leading to a minimum distance of at least 3 in its dual code. Recent studies have explored the Hamming metric parameters of Simplex codes, Macdonald codes, and punctured $\mathbb{Z}_q$-linear codes [11–21].

Inspired by the previous work, we present the following results. In section 2, we define some punctured codes of Simplex codes and analyse their weight distribution. In section 3, we constructed the Macdonald code of type u and proved their weight distribution by induction method. In section 4, we determine the parameters of strongly regular graphs corresponding to the constructed two-weight projective linear codes over $\mathbb{F}_q$. Also, we consider applications of projective two-weight linear codes and projective three-weight linear codes in secret sharing schemes. Section 5, We interpret the conclusions based on the results.

2. Punctured codes of Simplex codes over $\mathbb{F}_q$

In this section, we have constructed punctured codes of Simplex codes over $\mathbb{F}_q$ by their generator matrices.

Let G_k be a $k \times \frac{q^k-1}{q-1}$ matrix over $\mathbb{F}_q$ in which any two columns are linearly independent. The matrix G_k generates Simplex code, denoted as S_k. Clearly, the parameters of Simplex code is $\left[\frac{q^k-1}{q-1}, k, q^{k-1}\right]$. Any code with these parameters is equivalent to Simplex code [22]. Thus G_k can be defined inductively by

$$G_2 = \left[\begin{array}{c|c|cccc} 1 & 0 & 1 & \alpha & \alpha^2 & \cdots & \alpha^{q-2} \\ \hline 0 & 1 & 1 & 1 & 1 & \cdots & 1 \end{array}\right]$$

where $\alpha^i \in \mathbb{F}_q$.

$$G_k = \left[\begin{array}{c|c|c|c|c} 00\cdots0 & 1 & 11\cdots1 & \alpha\alpha\cdots\alpha & \cdots & \alpha^{q-2}\alpha^{q-2}\cdots\alpha^{q-2} \\ \hline G_{k-1} & \begin{array}{c}0\\ \vdots \\ 0\end{array} & G_{k-1} & G_{k-1} & \cdots & G_{k-1} \end{array}\right]$$

for $k > 2$.

In S_k every nonzero codeword has weight q^{k-1}. The dual of the Simplex code is the well known $\left[\frac{q^k-1}{q-1}, \frac{q^k-1}{q-1} - k, 3\right]$.

An excellent way to construct a new code from a given code is by puncturing coordinates.

In [10,23], they have defined MacDonald code over $\mathbb{F}_q$ by deleting the matrix

$$\begin{bmatrix} \mathbf{0} \\ G_u \end{bmatrix}$$

where $2 \le u \le k-1$ and $\mathbf{0}$ is $(k-u) \times \frac{q^u-1}{q-1}$ zero matrix, from G_k, that is

$$G_{k,u} = \left(G_k \setminus \begin{pmatrix} \mathbf{0} \\ G_u \end{pmatrix} \right)$$

for $2 \le u \le k-1$. By [10], $G_{k,u}$ generates q-ary code with parameters $\left[\frac{q^k-q^u}{q-1}, k, q^{k-1}-q^{u-1} \right]$ where all non-zero codewords have Hamming weights of q^{k-1} or $q^{k-1}-q^{u-1}$.

We delete the column $[1\ 1\ ]^T$ from G_2, and the obtained matrix is denoted as G_2', that is,

$$G_2' = \left[\begin{array}{c|c|cccc} 1 & 0 & \alpha & \alpha^2 & \cdots & \alpha^{q-2} \\ \hline 0 & 1 & 1 & 1 & \cdots & 1 \end{array} \right]$$

By inductively,

$$G_k' = \left[\begin{array}{c|c|c|c|c} 00\cdots0 & 11\cdots1 & \alpha\alpha\cdots\alpha & \cdots & \alpha^{q-2}\alpha^{q-2}\cdots\alpha^{q-2} \\ \hline G_{k-1}' & G_{k-1}' & G_{k-1}' & \cdots & G_{k-1}' \end{array} \right]$$

for $k > 2$.

Clearly, G_k' is a $k \times q^{k-1}$ matrix over $\mathbb{F}_q$. The code generated by G_k' is called a punctured Simplex code of type α, denoted by S_k'.

Let $q > 2$. We delete the column $[\alpha\ 1]^T$ from G_2', and the obtained matrix is denoted as G_2'', that is,

$$G_2'' = \left[\begin{array}{c|c|cccc} 1 & 0 & \alpha^2 & \alpha^3 & \cdots & \alpha^{q-2} \\ \hline 0 & 1 & 1 & 1 & \cdots & 1 \end{array} \right]$$

By inductively,

$$G_k'' = \left[\begin{array}{c|c|c|c|c} 00\cdots0 & 11\cdots1 & \alpha\alpha\cdots\alpha & \cdots & \alpha^{q-2}\alpha^{q-2}\cdots\alpha^{q-2} \\ \hline G_{k-1}'' & G_{k-1}'' & G_{k-1}'' & \cdots & G_{k-1}'' \end{array} \right]$$

for $k > 2$.

Clearly, G_k'' is a $k \times q^{k-1} - q^{k-2}$ matrix over $\mathbb{F}_q$. The code generated by G_k'' is called a punctured Simplex code of type β, denoted by S_k''.

In the following lemma, for any $x \in \mathbb{F}_q$, the notation $N_x(c)$ denotes the number of positions in codeword c which are additive inverse of x.

Lemma 2.1. *Consider an $[n,k,d]$ linear code C over $\mathbb{F}_q$ and $c_1 \in C$, $\alpha,\beta \in \mathbb{F}_q\backslash\{0\}$. Define $\overline{c_1} = \beta(\mathbf{0\,1\,\alpha\,\alpha^2}\cdots\boldsymbol{\alpha^{q-2}}) + (c_1\,c_1\,c_1\,\,c_1\cdots c_1)$, $\boldsymbol{x}$ denotes n-tuple $xxx\cdots x$, for any $x \in \mathbb{F}_q$. Then $wt(\overline{c_1}) = n(q-1)$.*

Proof. It is clear that, the codeword $\overline{c_1}$ has length nq. Consider

$$\begin{aligned} wt(\overline{c_1}) &= nq - \{N_0(c_1) + N_1(c_1) + N_\alpha(c_1) + N_{\alpha^2}(c_1) + \ldots + N_{\alpha^{q-2}}(c_1)\} \\ &= nq - \sum_{x\in\mathbb{F}_q} N_x(c_1) \\ wt(\overline{c_1}) &= n(q-1) \end{aligned}$$

That is, the Hamming weight of $\overline{c_1}$ is $n(q-1)$. □

Theorem 2.2. *The weight distribution of Simplex codes of type α is listed below.*

Weight	*Multiplicity*
0	*1*
$q^{k-2}(q-1)$	$q\left(q^{k-1}-1\right)$
q^{k-1}	$q-1$

Proof. First, we prove the result for $k = 2$.

$$S_2' = \{\beta(10\alpha\alpha^2\cdots\alpha^{q-2}) + \gamma(0111\cdots1) \mid \beta,\gamma \in \mathbb{F}_q\}$$

is a code of length q. We have the following cases.

Case i When $\gamma = -\beta$, every codeword c has weight q. That is, $wt(c) = q$. Thus, there are $q-1$ codewords of weight q.

Case ii If $\gamma \neq -\beta$ then $wt(c) = q-1$. Thus, the code contains $q^2 - q$ distinct codewords of weight $q-1$.

Now, let $k > 2$, by Lemma 2.1, the code S_k' has $q-1$ codewords of weight q^{k-1} and $q^k - q$ codewords of weight $q^{k-2}(q-1)$. □

Theorem 2.3. *The weight distribution of Simplex codes of type β is listed below.*

Weight	*Multiplicity*
0	*1*
$q^{k-2}(q-2)$	q^2-2q+1
$q^{k-1}-2q^{k-2}+q^{k-3}$	q^k-q^2
$q^{k-2}(q-1)$	$2(q-1)$

Proof. First, we prove the result for $k = 2$.

$$S_2'' = \{\beta(10\alpha^2\cdots\alpha^{q-2}) + \gamma(011\cdots1) \mid \beta,\gamma \in \mathbb{F}_q\}$$

is a code of length $q-1$. We have the following two cases.

Case i When $\gamma = -\beta$ or $\gamma = -\alpha\beta$, every codewords c has weight $q-1$. That is $wt(c) = q-1$. Thus, there are $2(q-1)$ codewords of weight $q-1$.

Case ii If $\gamma \neq -\alpha\beta$ then $wt(c) = q-2$. Thus, the code contains q^2-2q+1 codewords of weight $q-2$.

By Lemma 2.1, the code S_k'' contains q^2-2q+1 codewords of weight $q^{k-2}(q-2)$ and q^k-q^2 codewords of weight $q^{k-1}-2q^{k-2}+q^{k-3}$, and $2(q-1)$ codewords of weight $q^{k-2}(q-1)$. □

3. Macdonald codes of type u

Let $\boldsymbol{u} = (k_1, k_2, \cdots k_r)$. Then we define Macdonald codes of type u over $\mathbb{F}_q$ by deleting the matrix

$$G_{\boldsymbol{u}} = \begin{bmatrix} \mathbf{0}_{s_1} & \mathbf{0}_{s_2} & \mathbf{0}_{s_3} & \cdots & \mathbf{0}_{s_r} \\ G_{k_1} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & G_{k_2} & \mathbf{0} & \cdots & \mathbf{0} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & G_{k_r} \end{bmatrix}$$

where $1 \leq k_1 \leq k_2 \leq \cdots \leq k_r \leq k-1$, $k_1+k_2+\cdots+k_r \leq k$ and $\mathbf{0}_{s_i}$ is $s_i \times \frac{q^{k_i}-1}{q-1}$ zero matrix, from G_k, that is

$$G_{k,\boldsymbol{u}} = \left(G_k \setminus \begin{pmatrix} \mathbf{0} \\ G_{\boldsymbol{u}} \end{pmatrix} \right)$$

Here $s_i = k-(k_1+k_2+\cdots+k_r)$.

Clearly, $G_{k,u}$ is a $k \times n$ matrix over $\mathbb{F}_q$, where $n = \frac{q^k-(q^{k_1}+q^{k_2}\cdots+q^{k_r}-r+1}{q-1}$). The code associated with $G_{k,u}$ is called Macdonald code of type u.

Theorem 3.1. *The weight distribution of MacDonald codes of type u is listed below.*

When $s = 0$,

Weight	*Multiplicity*
0	*1*
$q^{k-1}-(q^{k_{i_1}-1}+q^{k_{i_2}-1}\cdots+q^{k_{i_j}-1})$	$(q^{k_{i_1}}-1)(q^{k_{i_2}}-1)\cdots(q^{k_{i_j}}-1)$

When $s \neq 0$,

Weight	*Multiplicity*
0	*1*
$q^{k-1}-(q^{k_{i_1}-1}+q^{k_{i_2}-1}\cdots+q^{k_{i_j}-1})$	$q^s(q^{k_{i_1}}-1)(q^{k_{i_2}}-1)\cdots(q^{k_{i_j}}-1)$
q^{k-1}	(q^s-1)

for $1 \le j \le r$, $\left\{(i_1, i_2, \cdots i_j) \in \mathbb{N}^j \text{ and } i_1 < i_2 < i_3 \cdots < i_j \le r\right\}$.

Proof. The proof of this theorem will be established using the method of mathematical induction on r. For $r = 2$ and $s = 0$, we have two blocks in the matrix G_u that is,

$$G_u = \begin{bmatrix} G_{k_1} & \mathbf{0} \\ \mathbf{0} & G_{k_2} \end{bmatrix}$$

The code generated by G_u has $q^{k_1}-1$ codewords of weight q^{k_1-1} and $q^{k_2}-1$ codewords of weight q^{k_2-1} and $(q^{k_1}-1)(q^{k_2}-1)$ codewords of weight $q^{k_1-1}+q^{k_2-1}$. Thus, the code generated by the matrix $G_{k,u}$ has $q^{k_1}-1$ codewords of weight $q^{k-1}-q^{k_1-1}$ and $q^{k_2}-1$ codewords of weight $q^{k-1}-q^{k_2-1}$ and $(q^{k_1}-1)(q^{k_2}-1)$ codewords of weight $q^{k-1}-(q^{k_1-1}+q^{k_2-1})$.

Similarly, for $r = 2$ and $s \neq 0$, by the matrix $G_{k,u}$ has $q^s(q^{k_1}-1)$ codewords of weight $q^{k-1}-q^{k_1-1}$ and $q^s(q^{k_2}-1)$ codewords of weight $q^{k-1}-q^{k_2-1}$, and $q^s(q^{k_1}-1)(q^{k_2}-1)$ codewords of weight $q^{k-1}-(q^{k_1-1}+q^{k_2-1})$, and q^s-1 codewords of weight q^{k-1}. Therefore, the theorem is valid for $r = 2$.

Suppose that the theorem holds for the case $r-1$.

The code generated by $G_{k,u}$ has $(q^s-1)(q^{k_{i_1}}-1)(q^{k_{i_2}}-1)\cdots(q^{k_{i_j}}-1)$ codewords of weight $q^{k-1}-(q^{k_{i_1}-1}+q^{k_{i_2}-1}\cdots+q^{k_{i_j}-1})$, and (q^s-1) codewords of weight q^{k-1}, for $1 \le j \le r-1$, $\{(i_1, i_2, \cdots i_j) \in \mathbb{N}^j$ and $i_1 < i_2 < i_3 \cdots < i_j \le r-1\}$ if $s \neq 0$.

Now, we are going to prove the theorem for r.

Case (i): when $s = 0$.

If $j = 1$, then by induction assumption, there are $(q^{k_i}-1)$ codewords of weight $q^{k-1}-q^{k_i-1}$ for $1 \le i \le r-1$. Also, there are $q^{k_r}-1$ codewords of weight $q^{k-1}-q^{k_r-1}$. Therefore, there are $(q^{k_i}-1)$ codewords of weight $q^{k-1}-q^{k_i-1}$ for $1 \le i \le r$.

If $j = 2$, then by induction assumption, there are $(q^{k_{i_1}}-1)(q^{k_{i_2}}-1)$ codewords of weight $q^{k-1}-(q^{k_{i_1}-1}+q^{k_{i_2}-1})$. Also, there are $(q^{k_t}-1)(q^{k_r}-1)$ codewords of weight $q^{k-1}-(q^{k_t-1}+q^{k_r-1})$ for $1 \le t, i_1, i_2 \le r-1$ and $i_1 < i_2$. Therefore, there are $(q^{k_{i_1}}-1)(q^{k_{i_2}}-1)$ codewords of weight $q^{k-1}-(q^{k_{i_1}-1}+q^{k_{i_2}-1})$ for $1 \le i_1, i_2 \le r$ and $i_1 < i_2$.

In general for j, by induction assumption, the code generated by $G_{k,u}$ has $(q^{k_{i_1}}-1)(q^{k_{i_2}}-1)\cdots(q^{k_{i_j}}-1)$ codewords of weight $q^{k-1}-(q^{k_{i_1}-1}+q^{k_{i_2}-1}\cdots+q^{k_{i_j}-1})$. Also, there are $(q^{k_{t_1}}-1)(q^{k_{t_2}}-1)\cdots(q^{k_{t_{j-1}}}-1)(q^{k_r}-1)$ codewords of weight $q^{k-1}-(q^{k_{t_1}-1}+q^{k_{t_2}-1}\cdots+q^{k_{t_{j-1}}-1}+q^{k_r-1})$, for $1\le i_1,i_2,\cdots,i_j,t_1,t_2,\cdots,t_{j-1}\le r-1$ and $i_1<i_2<i_3\cdots<i_j\le r-1$, $t_1<t_2<t_3\cdots<t_{j-1}\le r-1$.

Thus, the code generated by $G_{k,u}$ has $(q^{k_{i_1}}-1)(q^{k_{i_2}}-1)\cdots(q^{k_{i_j}}-1)$ codewords of weight $q^{k-1}-(q^{k_{i_1}-1}+q^{k_{i_2}-1}\cdots+q^{k_{i_j}-1})$ for $1\le j\le r$, $\left\{(i_1,i_2,\cdots i_j)\in\mathbb{N}^j \text{ and } i_1<i_2<i_3\cdots<i_j\le r\right\}$.

Case (ii): when $s\neq 0$.

If $j=1$, then by induction assumption, there are $q^s(q^{k_i}-1)$ codewords of weight $q^{k-1}-q^{k_i-1}$ for $1\le i\le r-1$. Also, there are $q^s(q^{k_r}-1)$ codewords of weight $q^{k-1}-q^{k_r-1}$. Therefore, there are $q^s(q^{k_i}-1)$ codewords of weight $q^{k-1}-q^{k_i-1}$ for $1\le i\le r$.

If $j=2$, then by induction assumption, there are $q^s(q^{k_{i_1}}-1)(q^{k_{i_2}}-1)$ codewords of weight $q^{k-1}-(q^{k_{i_1}-1}+q^{k_{i_2}-1})$. Also, there are $q^s(q^{k_t}-1)(q^{k_r}-1)$ codewords of weight $q^{k-1}-(q^{k_t-1}+q^{k_r-1}+q^{k_r-1})$ for $1\le t,i_1,i_2\le r-1$ and $i_1<i_2$. Therefore, there are $q^s(q^{k_{i_1}}-1)(q^{k_{i_2}}-1)$ codewords of weight $q^{k-1}-(q^{k_{i_1}-1}+q^{k_{i_2}-1})$ for $1\le i_1,i_2\le r$ and $i_1<i_2$.

In general for j, by induction assumption, the code generated by the matrix $G_{k,u}$ has $q^s(q^{k_{i_1}}-1)(q^{k_{i_2}}-1)\cdots(q^{k_{i_j}}-1)$ codewords of weight $q^{k-1}-(q^{k_{i_1}-1}+q^{k_{i_2}-1}\cdots+q^{k_{i_j}-1})$. Also, there are $q^s(q^{k_{t_1}}-1)(q^{k_{t_2}}-1)\cdots(q^{k_{t_{j-1}}}-1)(q^{k_r}-1)$ codewords of weight $q^{k-1}-(q^{k_{t_1}-1}+q^{k_{t_2}-1}\cdots+q^{k_{t_{j-1}}-1}+q^{k_r-1})$, for $1\le i_1,i_2,\cdots,i_j,t_1,t_2,\cdots,t_{j-1}\le r-1$ and $i_1<i_2<i_3\cdots<i_j\le r-1$, $t_1<t_2<t_3\cdots<t_{j-1}\le r-1$.

Therefore, there are $q^s(q^{k_{i_1}}-1)(q^{k_{i_2}}-1)\cdots(q^{k_{i_j}}-1)$ codewords of weight $q^{k-1}-(q^{k_{i_1}-1}+q^{k_{i_2}-1}\cdots+q^{k_{i_j}-1})$ for $1\le i_1,i_2,\cdots,i_j\le r$ and $i_1<i_2<i_3\cdots<i_j\le r$.

Additionally, there are q^s-1 codewords of weight q^{k-1} that corresponds to the block of zero matrix in G_u.

Thus, the code generated by the matrix $G_{k,u}$ has $q^s(q^{k_{i_1}}-1)(q^{k_{i_2}}-1)\cdots(q^{k_{i_j}}-1)$ codewords of weight $q^{k-1}-(q^{k_{i_1}-1}+q^{k_{i_2}-1}\cdots+q^{k_{i_j}-1})$ for $1\le j\le r$, $\left\{(i_1,i_2,\cdots i_j)\in\mathbb{N}^j \text{ and } i_1<i_2<i_3\cdots<i_j\le r\right\}$ and q^s-1 codewords of weight q^{k-1}. □

Corollary 3.2. *Let $s \neq 0$, $r = 1$ and k any positive integer then the weight distribution of (two-weight codes) Macdonald codes of type 1 is $A_{wt_1} = q^k - q^{k-k_1}$, $A_{wt_2} = q^{k-k_1} - 1$ and $wt_1 = q^{k-1} - q^{k_1-1}$, $wt_2 = q^{k-1}$.*

Corollary 3.3. *Let $s = 0$, $r = 2$, k is even and $k_1 = k_2$ then the weight distribution of (two-weight codes) Macdonald codes of type 2 is $A_{wt_1} = 2q^{k_1} - 2$, $A_{wt_2} = q^k - 2q^{k_1} + 1$ and $wt_1 = q^{k-1} - q^{k_1-1}$, $wt_2 = q^{k-1} - 2q^{k_1-1}$.*

Corollary 3.4. *Let $s = 0$, $r = 2$, k is odd and $k_1 < k_2$ then the weight distribution of (three-weight codes) Macdonald codes of type 2 is $A_{wt_1} = q^{k_1} - 1$, $A_{wt_2} = q^{k_2} - 1$, $A_{wt_3} = q^k - q^{k_1-1} - q^{k_2-1} + 1$, and $wt_1 = q^{k-1} - q^{k_1-1}$, $wt_2 = q^{k-1} - q^{k_2-1}$, $wt_3 = q^{k-1} - (q^{k_1-1} + q^{k_2-1})$.*

4. Projective linear codes over $\mathbb{F}_q$ and their applications

In this section, we will discuss the optimal Projective linear codes over the finite field $\mathbb{F}_q$ along with their applications in secret sharing schemes and strongly regular graphs.

4.1. **Optimal projective linear codes over $\mathbb{F}_q$.** An $[n,k,d]$ code is referred to as a *projective code* if $d^\perp \geq 3$, where $d^\perp$ denotes the minimum distance of dual code. Let $n_q(k,d)$ denote the least value of n such that a code with the parameters $[n_q(k,d),k,d]$ exists. An $[n_q(k,d),k,d]$ code is said to be (length)-*optimal.*

The important problem in coding theory is to obtain $n_q(k,d)$ for all values of k and d. Griesmer has shown a general lower bound on $n_q(k,d)$ in [24] and it is hereunder

$$n_q(k,d) \geq g_q(k,d) = \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil,$$

where $\lceil x \rceil$ denotes the least integer $\geq x$. The code with the parameters $[g_q(k,d),k,d]$ is called an optimal code.

Remark 4.1. *The Simplex code of type α is an $[q^{k-1},\ k,\ q^{k-2}(q-1)]$ optimal projective linear code over $\mathbb{F}_q$ with respect to Griesmer bound.*

Remark 4.2. *The Simplex code of type β is an $[q^{k-1}-q^{k-2},\ k,\ q^{k-2}(q-2)]$ optimal projective linear code over $\mathbb{F}_q$ with respect to Griesmer bound.*

Remark 4.3. *The MacDonald code type u is an* $\left[\frac{q^k-(q^{k_1}+q^{k_2}\cdots+q^{k_r}-r+1)}{q-1},\ k,\ q^{k-1}-(q^{k_{i_1}-1}+q^{k_{i_2}-1}\cdots+q^{k_{i_j}-1})\right]$ *optimal projective linear code over* $\mathbb{F}_q$ *with respect to Griesmer bound.*

Example 4.1. *If* $q=3$ *and* $k=5$*, then the Simplex code of type* α *is an* $[81,5,54]$ *optimal projective two weight code over* $\mathbb{F}_3$ *with weight enumerator* $1+240X^{54}+2X^{81}$.

Example 4.2. *If* $q=4$ *and* $k=5$*, then the Simplex code of type* β *is an* $[81,5,128]$ *optimal projective two weight code over* $\mathbb{F}_4$ *with weight enumerator* $1+9X^{128}+1008X^{144}+6X^{192}$.

Example 4.3. *If* $q=5$, $s=0$, $r=2$, $k=6$ *and* $k_1=k_2=3$ *then the MacDonald code type u is an* $[15376,6,3075]$ *optimal projective two weight code over* $\mathbb{F}_5$ *with weight enumerator* $1+15375X^{3075}+248X^{3100}$.

4.2. **Strongly regular graph corresponds to projective two-weight codes over $\mathbb{F}_q$.** Let $G=(V,E)$ be a K-regular simple graph with vertex set V, edge set E and $|V|=v$, $|E|=e$. If there exists a pair of positive integers λ and μ such that every pair of vertices which are adjacent in G shares λ common neighbours, and every pair of non-adjacent vertices has μ common neighbours, then G is termed a strongly regular graph. The parameters of the strongly regular graph can be expressed as (v,K,λ,μ).

Consider an $[n,k]$ linear code C over $\mathbb{F}_q$, which can be represented by the generator matrix $G=[\boldsymbol{g_1}\ \boldsymbol{g_2}\ \boldsymbol{g_3}\cdots\boldsymbol{g_n}]$, where $\boldsymbol{g_i}$ denotes a column vector of G for all i. Let $\boldsymbol{V}=\mathbb{F}_q^k$, $\boldsymbol{O}=\{\langle \boldsymbol{g_i}\rangle : i=1,2,\ldots,n\}$, and $\Omega=\{\boldsymbol{u}\in\boldsymbol{V}:\langle\boldsymbol{u}\rangle\in\boldsymbol{O}\}$. We define a graph $G(\Omega)$ with vertices as a collection of vectors from $\boldsymbol{V}$, where two vertices are connected if and only if their difference belongs to Ω.

In 1985, Calderbank and Kantor proved in [4, Theorem 3.2] that the graph $G(\Omega)$ is a strongly regular graph if and only if the code C is a projective two-weight code. Let wt_1 and wt_2 represent the nonzero weights of a projective two-weight linear code C over $\mathbb{F}_q$. Then, by [4, corollary 3.7], the parameters of $G(\Omega)$ are

$$\begin{aligned} v &= q^k,\ K=n(q-1),\\ \lambda &= K^2+3K-q(wt_1+wt_2)-Kq(wt_1+wt_2)+q^2wt_1wt_2,\\ \mu &= \frac{q^2wt_1wt_2}{q^k}=K^2+K-Kq(wt_1+wt_2)+q^2wt_1wt_2. \end{aligned}$$

Remark 4.4. *The parameters of the strongly regular graph associated with the Macdonald codes of type* 1 *with parameters length* $n = q^{k-1}$, *dimension* k *and the weights* $wt_1 = q^{k-1} - q^{k_1-1}$, $wt_2 = q^{k-1}$ *is given by*

$$\begin{aligned} v &= q^k,\ K = q^{k-1}(q-1), \\ \lambda &= q^{2(k-1)} + q^k + q^{k_1} - 3q^{k-1} - q^{k+k_1-1}, \\ \mu &= q^k - q^{k_1}. \end{aligned}$$

The obtained parameters of the strongly regular graph correspond to the projective two-weight codes of type SU1 in the sense of [4].

Remark 4.5. *The parameters of the strongly regular graph associated with the (two-weight codes) Macdonald codes of type* 2 *with length* $n = \frac{q^k - 2q^{k_1}+1}{q-1}$, *dimension* k *and the weights* $wt_1 = q^{k-1} - q^{k_1-1}$, $wt_2 = q^{k-1} - 2q^{k_1-1}$ *is given by*

$$\begin{aligned} v &= q^k,\ K = q^k - 2q^{k_1} + 1, \\ \lambda &= q^k + 2q^{2k_1} - 6q^{k_1} - q^{k+k_1} + 4, \\ \mu &= q^k - 3q^{k_1} + 2q^{2k_1-k}. \end{aligned}$$

The obtained parameters of the strongly regular graph correspond to the projective two-weight codes of type SU2 in the sense of [4].

4.3. **Application of projective linear codes in secret sharing schemes.** The work by Massey in [25] and [26] provides a detailed explanation of the construction of secret sharing schemes (SS-Schemes) using linear codes. In this particular section, we aim to interpret and analyze the SS-Schemes that are based on projective linear codes over $\mathbb{F}_q$.

4.3.1. **Secret Sharing Schemes (SS-Schemes).** Let C be a linear code over $\mathbb{F}_q$, then $C^\perp$ denotes the dual of C. The support of a codeword $\boldsymbol{c}$ is a set of all non-zero positions in a codeword $\boldsymbol{c} = (c_0, c_1, \cdots c_{n-1}) \in C$ and its denoted by

$$\{0 \le i \le n-1 : c_i \neq 0\}.$$

If a support of a codeword $\boldsymbol{c_1}$ is a proper subset support of a codeword $\boldsymbol{c_2}$, then we can say that, the codeword $\boldsymbol{c_2}$ covers $\boldsymbol{c_1}$. If a nonzero codeword $\boldsymbol{c} \in C$ does not cover any other nonzero codeword of C except for $u\boldsymbol{c}$ where $u \in \mathbb{F}_q^*$, then it is called a minimal

codeword of C. A minimal linear code has all nonzero codewords are minimal codewords.

A minimal access set refers to a collection of participants capable of recovering the secret using their shares, while none of its proper subsets can achieve this. If SS-Schemes has a monotone access structure then any superset of an access set is an access set. The access structure in SS-Schemes with the monotone access structure is accomplished through its minimal access sets [27]. In general, the linear code-based SS-Schemes have a fairly complicated access structure. It was established in [28, 29] that if the linear codes are minimal, it is possible to determine the access structures of the SS-Schemes from the duals of linear codes. Therefore, SS-Schemes with intriguing access structures can be constructed with minimal linear codes.

Generally, an SS-Schemes based on the linear code C has a complicated access structure. However, it can be determined for some particular class of codes that satisfies the following theorem, and it is a simple modification in [30, Theorem 12].

Theorem 4.6. *Let C be an $[n,k,d]$ code over $\mathbb{F}_q$, and the minimum distance of its dual code $C^\perp$ denoted by $d^\perp$. If each codeword $c \neq 0$ in $C \setminus A$ is minimal, then the cardinality of the set of participants in the SS-Schemes based on $C^\perp$ is $n-1$, and the cardinality of the set of all minimal access sets is $q^{k-1} - \frac{|A|}{q-1}$ where $A = \{c \in C \mid wt(c) = wt_{max}\}$.*

- *In the case where $d^\perp \geq 3$, for every $1 \leq i \leq \min\{k-1, d^\perp - 2\}$, any group of i participants is included in $(q-1)^i q^{k-(i+1)} - \frac{|A|}{q-1}$ out of the total $q^{k-1} - \frac{|A|}{q-1}$ minimal access sets.*

It is natural to ask a question like what will be the condition for a linear code C to get all the nonzero codewords which are minimal in $C - A$. The following lemma gives a condition in this direction, and it is a simple modification in [31, Proposition 3].

Lemma 4.7. *[31] Let C be an $[n,k,d]$ code over $\mathbb{F}_q$. Assume wt_{min} and wt_{max} are the minimum and maximum nonzero Hamming weights of $C - A$ respectively. If*

$$\frac{wt_{min}}{wt_{max}} > \frac{q-1}{q},$$

then each nonzero codeword $c \in C - A$ is a minimal vector where $A = \{c \in C \mid wt(c) = wt_{max}\}$.

4.3.2. **SS-Schemes from projective linear codes**. In this subsection, we will construct SS-Schemes based on the dual code of Simplex code of type α and Simplex code of type β.

The class of codes generated by the matrix G'_k satisfies the Lemma 4.7. That is, by Theorem 2.2, we have

$$\frac{wt_{min}}{wt_{max}} = \frac{q^{k-2}(q-1)}{q^{k-2}(q-1)} = 1 > \frac{q-1}{q}.$$

When $k > 2$. The class of codes generated by the matrix G''_k satisfies the Lemma 4.7. That is, by Theorem 2.2, we have

$$\frac{wt_{min}}{wt_{max}} = \frac{q^{k-2}(q-2)}{q^{k-3}(q^2-2q+1)} = \frac{q(q-2)}{q^2-2q+1} > \frac{q-1}{q}.$$

By Lemma 4.7, the nonzero codewords of codes generated by the matrix G'_k and G''_k are minimal where $A = \{c \in C \mid wt(c) = q^{k-1}\}$ and $A = \{c \in C \mid wt(c) = q^{k-2}(q-1)\}$, respectively. Hence, SS-Schemes utilizing the dual codes of codes generated by the matrices G'_k and G''_k exhibit desirable access structures, as outlined in Theorem 4.6.

Corollary 4.8. *The SS-Scheme based on the dual codes of codes generated by the matrices G'_k and G''_k has $2q^k - 1$ participants, and $q^{k+1} - (1-1)^2$ minimal access sets. For each $1 \leq i \leq min\{k+1, 2q-2\}$, every set of i participants is involved in $(q-1)^i q^{k+2-(i+1)} - (q-1)^2$ out of $q^{k+1} - (q-1)^2$ minimal access sets.*

Example 4.4. *Let $p = 5$ and $k = 4$. Then the SS-Scheme based on the dual codes of codes generated by the matrices G'_k has 124 participants and 124 minimal access sets. each participant is involved in 100 out of 124 minimal access sets.*

5. Conclusion and Future work

In this article, we constructed punctured Simplex codes using their generator matrices. By their weight distribution, we confirmed they are projective two-weight and three-weight linear codes over $\mathbb{F}_q$. Also, we have given Macdonald codes of type u and analyzed their weight distributions. Moreover, we have provided optimal projective two-weight linear codes over $\mathbb{F}_q$, which achieved the Griesmer bound. From the perspective of the application, we have constructed the SS-Schemes from the projective two-weight linear codes and projective-three weight linear

codes over $\mathbb{F}_q$ and examined the parameters for strongly regular graphs associated with the projective two-weight linear codes over $\mathbb{F}_q$. In Information Theory and telecommunication domains, Error-Correcting codes (ECC) are used extensively. Specifically, the interconnection links in Network on Chip (NoC) employing error-correcting codes were examined in [32, 33]. In future research, the analysis of NoC could extend to include nonlinear error-correcting codes.

ACKNOWLEDGEMENTS

J. Prabu and J. Mahalakshmi extend their thanks to the National Board for Higher Mathematics (NBHM), Department of Atomic Energy (DAE), Government of India, for the generous financial assistance provided under reference number 02011/7/2019-R&D-II/1975.

References

[1] R. Anderson, C. Ding, Helleseth T., T. Klove, How to build robust shared control systems. *Des. Codes Crytogr.* **15**(2)(1998) 111–124.
[2] C. Ding, X. Wang, A coding theory construction of new systematic authentication codes, *Theoretical computer science*, **330**(1)(2005) 81–99.
[3] A.R. Calderbank, J.M. Goethals, Three-weight codes and association schemes. *Philips J Res.* **39**(4-5)(1984) 143–152.
[4] R. Calderbank, W.M. Kantor, The geometry of two-weight codes, *Bull London Math Soc.* **18**(2)(1986) 97–122.
[5] P. Delsarte, Weights of linear codes and strongly regular normed spaces. *Discrete Math.* **3**(1-3)(1972) 47–64 .
[6] A.E. Brouwer, W.H. Haemers, Spectra of graphs, *New York, NY: Springer*, (2012).
[7] R.A. Fisher, The theory of confounding in factorial experiments in relation to the theory of groups. *Ann Eugenics.* **11**(1942) 341–353.
[8] R.A. Fisher, A system of confounding for factors with more than two alternatives giving completely orthogonal cubes and higher powers. *Ann Eugenics*. **12**(1945) 2283–2290.
[9] JE MacDonald, Design methods for maximum minimum distance error-correcting codes. *IBM J. Res. Dev.* **4**(1)(1960) 43–57 .
[10] A Patel, Maximal q-nary linear codes with large minimum distance (corresp.), *IEEE Trans. Inf. Theory* **21**(1)(1975) 106-110.
[11] C. Durairajan, J. Mahalakshmi, On codes over integers modulo q, *Advances and Applications in Discrete Mathematics* **15**(2), (2015)125-143.
[12] C. Durairajan, J. Mahalakshmi J, P. Chella Pandian, On the $\mathbb{Z}_q$-simplex codes and its weight distribution for dimension 2, *Discrete Mathematics, Algorithms and Applications* **7**(3)(2015) 1550030.

[13] P. Chella Pandian, C. Durairajan, On $\mathbb{Z}_q$-linear and $\mathbb{Z}_q$-simplex codes and its related parameters for q is a prime power, *Journal of Discrete Mathematical Sciences and Cryptography* **18**(1-2)(2015) 81-94.

[14] J. Prabu, J. Mahalakshmi, S. Santhakumar, Unit $\mathbb{Z}_q$-Simplex codes of type α and zero divisor $\mathbb{Z}_q$-Simplex codes. *Commun. Comb. Optim.* **8**(2)(2023) 327-348.

[15] J.Prabu, J. Mahalakshmi, S. Santhakumar, *A class of t-weight codes and its applications*, *J. Algebra Appl.*, (2023) 2550096. https://doi.org/10.1142/S0219498825500963

[16] J. Prabu, J. Mahalakshmi, C. Durairajan, S.Santhakumar, On some Punctured Codes of $\mathbb{Z}_q$-Simplex Codes. *Discrete Math. Algorithms Appl.* **14**(06)(2021) 2250012.

[17] J Charles CColbourn, K Manish Gupta, On quaternary MacDonald codes, *Proceedings ITCC 2003. International Conference on Information Technology, Coding and Computing.* (2003) 212–215.

[18] Abdullah Dertli, Yasemin Cengellenmis, MacDonald codes over the ring $\mathbb{F}_2 + v\mathbb{F}_2$. *Int. J. Algebra*, **5**(20)(2011) 985-991.

[19] Zhonghua Sun, Xinyue Liu, Several families of negacyclic BCH codes and their duals, *Des. Codes Cryptogr.* (2024): 1-26 https://doi.org/10.1007/s10623-024-01551-2.

[20] Wenbing Chen, Jindeng Zhang, Minjia Shi, A new family of p-ary self-orthogonal code from weakly regular plateaued functions, *J. Appl. Math.* (2024) 1-22 https://doi.org/10.1007/s12190-024-02316-9

[21] Congv Yu, Shixin Zhu, Construction of new linear codes with good parameters from group rings and skew group rings, *Discrete Math.* 348.4 (2025) 114349.

[22] M. S. Garg, On optimum codes and their covering radii. *Diss. PhD thesis*, *IIT Kanpur*, *India*, (1990).

[23] JE MacDonald, Design methods for maximum minimum-distance error-correcting codes, *IBM Journal of Research and Development*, **4**(1)(1960) 43-57.

[24] J.H. Griesmer, A bound for error-correcting codes, *IBM Journal of Research and Development*, **4**(5)(1960) 532–542.

[25] J.L. Massey, Minimal codewords and secret sharing. *In: Proceedings of the 6th joint Swedish-Russian international workshop on information theory*, *Citeseer*, (1993)276–279.

[26] J.L. Massey, Some applications of coding theory in cryptography, *Codes and Ciphers: Cryptography and Coding IV*, (1995) 33–47.

[27] A. Shamir, How to share a secret. *Communications of the ACM*, **22**(11)(1979) 612–613.

[28] A. Beimel, Secret-sharing schemes: A survey. *In: International conference on coding and cryptology. Springer*, (2011)11–46.

[29] G. Xu, X. Cao, J. Gao, G. Luo, Two Classes of Linear Codes with Two or Three Weights. *IEICE Trans. Fundamentals.*, **101**(12)(2018) 2366–2373.

[30] K. Ding, C. Ding, A class of two-weight and three-weight codes and their applications in secret sharing. *IEEE Trans. Inf. Theory*, **61**(11)(2015) 5835–5842.

[31] C. Ding, J. Yuan, Covering and secret sharing with linear codes. *In: International Conference on Discrete Mathematics and Theoretical Computer Science*, *Springer*, (2013) 11–25.
[32] M. Vinodhini, N.S. Murty, Reliable low power NoC interconnect, *Microprocessors and Microsystems*, **57**(2018) 15–22.
[33] K. Nimmy, S. Sankaran, K. Achuthan, A novel multi-factor authentication protocol for smart home environments, *In: International Conference on Information Systems Security*, *Springer*,(2018) 44–63.

Department of Mathematics, PSG Institute of Technology and Applied Research, Neelambur, Coimbatore, Tamilnadu, Pin Code - 641062, India
Email address: prabu11um47@gmail.com

Department of Mathematics, Amrita School of Physical Sciences, Coimbatore, Amrita Vishwa Vidyapeetham, India.
Email address: j_mahalakshmi@cb.amrita.edu

Department of Mathematics, Amrita School of Physical Sciences, Coimbatore, Amrita Vishwa Vidyapeetham, India.
Email address: s_santhakumar@cb.amrita.edu