Computational and Applied Mathematics (2019) 38:169
https://doi.org/10.1007/s40314-019-0937-y

MacDonald codes over the ring $\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p$

Yongkang Wang[1] · **Jian Gao**[1,2]

Received: 15 October 2018 / Revised: 11 February 2019 / Accepted: 24 September 2019 /
Published online: 5 October 2019

Abstract
In this paper, we consider MacDonald codes over the finite non-chain ring $\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p$ and their applications in constructing secret sharing schemes and association schemes, where p is an odd prime and $v^3 = v$. We give some structural properties of MacDonald codes first. Then, we study the weight enumerators of torsion codes of these MacDonald codes. As some applications, constructing secret sharing schemes and association schemes is also investigated.

Keywords MacDonald codes · Torsion codes · Secret sharing schemes · Association schemes

Mathematics Subject Classification 94B05 · 11T71

1 Introduction

MacDonald codes are a class of linear codes with two nonzero weights. Two weights linear codes have many wide applications in authentication codes, association schemes and secret sharing schemes. Two weights codes are also closely related to objects in different areas of mathematics such as strongly regular graphs, partial geometries, and projective point sets. Therefore, the construction of two weights linear codes has become a hot topic of coding theory, such as Shi et al. constructed some two weights projective $\mathbb{Z}_4$-codes in Shi et al. (2017b) gave two new families of two weights codes by codes over finite non-chain rings in Shi et al. (2017a).

Communicated by Thomas Aaron Gulliver.

✉ Jian Gao
dezhougaojian@163.com; jiangao@mail.nankai.edu.cn

Yongkang Wang
zcyongkang@163.com

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

[2] School of Mathematics and Statistics, Changsha University of Science and Technology, Changsha 410114, People's Republic of China

MacDonald codes have such good properties, so they have attracted the attention of coding scholars. The binary MacDonald codes were introduced in MacDonald (1960). And MacDonald codes over finite field $\mathbb{F}_q$ were studied in Patel (1975). In 2003, Colbourn and Gupta obtained two families of MacDonald codes over the ring $\mathbb{Z}_4$ from $\mathbb{Z}_4$-simplex codes of types α and β (see Colbourn and Gupta 2003). Dertli and Cengellenmis (2011) studied the MacDonald codes over the finite non-chain ring $\mathbb{F}_2 + v\mathbb{F}_2$ with $v^2 = v$. In 2016, Wang et al. studied MacDonald codes over $\mathbb{F}_p + v\mathbb{F}_p$ with $v^2 = v$. They also determined the access structure of secret sharing schemes based on these codes (see Wang et al. 2016).

In Delsarte (1973), the association schemes approach was firstly used to deal with a collection of topics involving the weight distribution of a code. Association schemes are closely related to coding theory, graph theory and finite fields theory. Especially, they provide a framework to study codes and designs. Luo et al. (2018) constructed a class of linear codes with two weights over $\mathbb{F}_q$ by linear codes over the finite chain ring $\mathbb{F}_q + u\mathbb{F}_q$ with $u^2 = 0$. They also employed these linear codes to construct association schemes.

The finite non-chain ring $\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p$ is the generalization of the ring $\mathbb{F}_p + v\mathbb{F}_p$. Shi et al. (2013) firstly studied the cyclic codes and the weight enumerator of linear codes over $\mathbb{F}_2 + v\mathbb{F}_2 + v^2\mathbb{F}_2$ with $v^3 = v$. As an open problem in Shi et al. (2013), Gao studied the structural properties of linear codes and cyclic codes over $\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p$ with $v^3 = v$ and p an odd prime. Some optimal linear codes over finite fields were also constructed (see Gao 2015). To the best of our knowledge, MacDonald codes over the finite non-chain ring $\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p$ with $v^3 = v$ and p an odd prime have not been considered by any other coding scholars. In this paper, we will study this issue. The rest of this paper is organized as follows. In Sect. 2, we give the structural properties of MacDonald codes over $\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p$, where p is an odd prime and $v^3 = v$. The torsion codes and their weight enumerators are also studied in this section. In Sect. 3, as an application of torsion codes, secret sharing schemes are constructed. In Sect. 4, as another application of torsion codes, we employ them to construct some association schemes.

2 MacDonald codes over $\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p$

Let $R = \mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p$, where p is an odd prime and $v^3 = v$. It is clear that R is a finite commutative ring with characteristic p. The ring R is also a semi-local ring with three maximal ideals $\langle v\rangle$, $\langle v-1\rangle$ and $\langle v+1\rangle$. Any element of R can be uniquely expressed as $r = a + bv + cv^2$, where $a, b, c \in \mathbb{F}_p$. Clearly, $v^3 - v = v(v-1)(v+1)$ over $\mathbb{F}_p$. Let $f_0 = v$, $\widehat{f_0} = v^2 - 1$, $f_1 = v - 1$, $\widehat{f_1} = v^2 + v$ and $f_2 = v + 1$, $\widehat{f_2} = v^2 - v$. Then f_i and $\widehat{f_i}$ are coprime, where $i = 0, 1, 2$. In other words, there exist $a_i, b_i \in R$ such that $a_i f_i + b_i \widehat{f_i} = 1$ for $i = 0, 1, 2$. Let $e_i = b_i \widehat{f_i} + \langle v^3 - v\rangle$. Then, $e_0 = 1 - v^2$, $e_1 = \frac{v^2+v}{2}$, $e_2 = \frac{v^2-v}{2}$, and $e_i^2 = e_i$, $\sum_{i=0}^{2} e_i = 1$. Further, we obtain $e_i e_j = 0$ for any $i \neq j$, which implies that e_0, e_1 and e_2 are primitive idempotent elements of R. Therefore, $R = e_0R \oplus e_1R \oplus e_2R = e_0\mathbb{F}_p \oplus e_1\mathbb{F}_p \oplus e_2\mathbb{F}_p$. It means that any $r \in R$ can also be uniquely expressed as $r = e_0r_0 + e_1r_1 + e_2r_2$, where $r_i \in \mathbb{F}_p$, $i = 0, 1, 2$. By the Chinese remainder theorem, we also have that $R \cong R/\langle v\rangle \times R/\langle v-1\rangle \times R/\langle v+1\rangle \cong \mathbb{F}_p \times \mathbb{F}_p \times \mathbb{F}_p$.

A code C of length n over R is a nonempty subset of R^n. If the subset is also an R-submodule of R^n, then C is called a linear code. For any $x = (x_0, x_1, \ldots, x_{n-1})$, $y = (y_0, y_1, \ldots, y_{n-1}) \in R^n$, we define the Euclidean inner product as $x \cdot y = \sum_{i=0}^{n-1} x_i y_i$. The dual code of C is defined as $C^{\perp} = \{x \in R^n \mid x \cdot y = 0, \forall\, y \in C\}$. If $C \subseteq C^{\perp}$, then C is called self-orthogonal. If $C = C^{\perp}$, then C is called self-dual.

Let C be a linear code of length n over R. Define

$$H_1 = \left\{ a \in \mathbb{F}_p^n \mid \exists\, b, c \in \mathbb{F}_p^n, (1-v^2)a + \frac{v^2+v}{2}b + \frac{v^2-v}{2}c \in C \right\},$$

$$H_2 = \left\{ b \in \mathbb{F}_p^n \mid \exists\, a, c \in \mathbb{F}_p^n, (1-v^2)a + \frac{v^2+v}{2}b + \frac{v^2-v}{2}c \in C \right\}$$

and

$$H_3 = \left\{ c \in \mathbb{F}_p^n \mid \exists\, a, b \in \mathbb{F}_p^n, (1-v^2)a + \frac{v^2+v}{2}b + \frac{v^2-v}{2}c \in C \right\}.$$

Then, we have $C = (1-v^2)H_1 \oplus \frac{v^2+v}{2}H_2 \oplus \frac{v^2-v}{2}H_3$, and H_1, H_2, H_3 are all linear codes of length n over $\mathbb{F}_p$. The linear codes H_1, H_2 and H_3 are defined to be the torsion codes of C.

2.1 MacDonald codes of type α

A type α simplex code S_k^α is a linear code over R. Its generator matrix G_k^α is constructed inductively as follows.

Let G_1^α be a $1 \times p^3$ matrix consisting of all the elements of R. In other words, $G_1^\alpha = [0\ 1\ 2\ \cdots\ p-1\ v\ 2v\ \cdots\ 1+(p-1)v\ \cdots\ (p-1)v^2\ 1+(p-1)v^2\ 2+(p-1)v^2\ \cdots\ (p-1)+(p-1)v^2\ v+(p-1)v^2\ 2v+(p-1)v^2\ \cdots\ 1+(p-1)v+(p-1)v^2]$. Note that the elements of G_1^α can be sorted arbitrarily.

Let G_k^α be a $k \times p^{3k}$ matrix over R, where

$$G_k^\alpha = \begin{bmatrix} 0\cdots 0 & 1\cdots 1 & \cdots & 1+(p-1)v+(p-1)v^2\cdots 1+(p-1)v+(p-1)v^2 \\ G_{k-1}^\alpha & G_{k-1}^\alpha & \cdots & G_{k-1}^\alpha \end{bmatrix}.$$

Let $G(S_k)$, columns consisting of all nonzero p-ary k-tuples, be a generator matrix for an $[n,k]_p$ simplex code S_k over $\mathbb{F}_p$. Then, the extended simplex code $\widehat{S}_k$ is generated by $G(\widehat{S}_k) = [0|G(S_k)]$, where

$$G(\widehat{S}_k) = \begin{bmatrix} 0\cdots 0 & 1\cdots 1 & \cdots & (p-1)\ \ldots\ (p-1) \\ G(\widehat{S}_{k-1}) & G(\widehat{S}_{k-1}) & \cdots & G(\widehat{S}_{k-1}) \end{bmatrix}$$

and $G(\widehat{S}_1) = \begin{bmatrix} 0 & 1 & 2 & \cdots & p-1 \end{bmatrix}$.

Lemma 1 *The torsion codes H_i $(i = 1, 2, 3)$ of S_k^α are permutation equivalent to p^{2k} copies of $\widehat{S}_k$.*

Proof We prove the H_1 case by induction on k. The generator matrix of H_1 is obtained by replacing $(1-v^2)$ by 1 in the matrix rows $(1-v^2)G_k^\alpha$. For $k = 1$, we can easily verify it. Suppose that the matrix $(1-v^2)G_{k-1}^\alpha$ is permutation equivalent to $p^{2(k-1)}$ copies of $(1-v^2)G(\widehat{S}_{k-1})$, then the matrix $(1-v^2)G_k^\alpha$ is $(1-v^2)G_k^\alpha = [\underbrace{G\ G\ \cdots\ G}_{p^2}]$, where $G = \begin{bmatrix} G_0 & G_1 & \cdots & G_{p-1} \end{bmatrix}_{k \times p^{3k-2}}$ and

$$G_j = \begin{bmatrix} (1-v^2)j & \cdots & (1-v^2)j \\ (1-v^2)G(\widehat{S}_{k-1}) & \cdots & (1-v^2)G(\widehat{S}_{k-1}) \end{bmatrix}, \quad j = 0, 1, \ldots, p-1.$$

The size of G_j is $k \times p^{3k-3}$. Regrouping the columns, we have the desired result. The proof of H_2 and H_3 is similar to the above. □

In the following, we define the MacDonald codes of type α over R. It can be constructed from the generator matrix G_k^α of the simplex code S_k^α. For $1 \le u \le k-1$, let $G_{k,u}^\alpha$ be the matrix obtained from G_k^α by deleting columns corresponding to the columns of G_u^α, i.e.

$$G_{k,u}^\alpha = \left[G_k^\alpha \backslash \begin{matrix} \mathbf{0} \\ G_u^\alpha \end{matrix} \right],$$

where $[A \backslash B]$ denotes the matrix obtained from the matrix A by deleting the matrix B, and the size of the matrix $\mathbf{0}$ is $(k-u) \times p^{3u}$.

Definition 1 The code $C_{k,u}^\alpha$ generated by $G_{k,u}^\alpha$ is called a type α MacDonald code.

Clearly, the code $C_{k,u}^\alpha$ is a linear code over R of length $p^{3k} - p^{3u}$. Let $M_{k,u}^\alpha$ be the torsion code of $C_{k,u}^\alpha$. That is the generator matrix of $M_{k,u}^\alpha$ obtained by replacing $(1-v^2)$ by 1 in the matrix $(1-v^2)G_{k,u}^\alpha$. Meanwhile, we can get other torsion codes of $C_{k,u}^\alpha$ by replacing $\frac{v^2+v}{2}$ by 1 in $\frac{v^2+v}{2}G_{k,u}^\alpha$ and by replacing $\frac{v^2-v}{2}$ by 1 in $\frac{v^2-v}{2}G_{k,u}^\alpha$, respectively. From Lemma 1, we can see that these three torsion codes are equivalent to each other. Therefore, we only need to study the first case, i.e. we only consider the torsion code $M_{k,u}^\alpha$. In the following, we give the Hamming weight enumerator of $M_{k,u}^\alpha$ first.

Theorem 1 *The torsion code $M_{k,u}^\alpha$ is a p-ary two weights linear code with parameter $[p^{3k} - p^{3u}, k, (p-1)(p^{3k-1} - p^{3u-1})]$. The number of codewords with Hamming weight $(p-1)p^{3k-1}$ is $p^{k-u}-1$, and the number of codewords with Hamming weight $(p-1)(p^{3k-1} - p^{3u-1})$ is $p^k - p^{k-u}$.*

Proof Clearly, the result holds for the case $k=2$ and $u=1$. Suppose that the result holds for the case $k-1$ and $1 \le u \le k-2$. Then for the case k and $1 \le u \le k-1$, the matrix $(1-v^2)G_{k,u}^\alpha$ takes the form

$$(1-v^2)G_{k,u}^\alpha = \left[(1-v^2)G_k^\alpha \backslash \begin{matrix} \mathbf{0} \\ (1-v^2)G_u^\alpha \end{matrix} \right],$$

where

$$G_k^\alpha = \begin{bmatrix} 0 \cdots 0 & 1 \cdots 1 & \cdots & 1 + (p-1)v + (p-1)v^2 \cdots 1 + (p-1)v + (p-1)v^2 \\ G_{k-1}^\alpha & G_{k-1}^\alpha & \cdots & G_{k-1}^\alpha \end{bmatrix}.$$

Therefore, we have that each nonzero codeword of $(1-v^2)G_{k,u}^\alpha$ has Hamming weight $(p-1)p^{3k-1}$ or $(p-1)(p^{3k-1} - p^{3u-1})$ and the dimension of $M_{k,u}^\alpha$ is k. By the computation, there are $p^{k-u}-1$ codewords of Hamming weight $(p-1)p^{3k-1}$ and $p^k - p^{k-u}$ codewords of Hamming weight $(p-1)(p^{3k-1} - p^{3u-1})$. □

2.2 MacDonald codes of type β

The code length of simplex codes of type α is large and increases fast. We can omit some columns from S_k^α. A type β simplex code S_k^β is a linear code over R constructed by omitting some columns from G_k^α. Specifically, after deleting some columns of G_k^α, no two columns are multiplied in the generating matrix G_k^β of S_k^β.

Let δ_k be a matrix of size $k \times \frac{p^{3k}-p^{2k}}{p-1}$ over R. Let

$\delta_1 = [1\ 2\ \cdots\ p-1\ 1+v\ 2+2v\ \cdots\ (p-1)+(p-1)v\ 2+v\ 4+2v\cdots\ 2(p-1)+(p-1)v\ 3+v\ 6+2v\ \cdots\ 3(p-1)+(p-1)v\cdots\ (p-1)+v\ 2(p-1)+2v\cdots\ 1+(p-1)v\ 1+(p-2)v+(p-1)v^2\ 2+2(p-2)v+2(p-1)v^2\cdots\ (p-1)+2v+v^2\ (p-1)+v^2]$ and

$$\delta_2 = \begin{bmatrix} 0 & A & B & C & D & E & \cdots & F \\ \delta_1 & G_1^{\alpha} & \delta_1 & \delta_1 & \delta_1 & \delta_1 & \cdots & \delta_1 \end{bmatrix},$$

δ_k is constructed inductively as follows:

$$\delta_k = \begin{bmatrix} 0 & A & B & C & D & E & \cdots & F \\ \delta_{k-1} & G_{k-1}^{\alpha} & \delta_{k-1} & \delta_{k-1} & \delta_{k-1} & \delta_{k-1} & \cdots & \delta_{k-1} \end{bmatrix},$$

where

$$\begin{aligned} A &= [1\ 2\ \cdots\ p-1\ 1+v\ 2+2v\cdots\ (p-1)+2v+v^2\ (p-1)+v^2], \\ B &= [v\ 2v\ 3v\ \cdots\ (p-1)v],\ C = [v^2\ 2v^2\ 3v^2\ \cdots\ (p-1)v^2], \\ D &= [v+v^2\ 2v+2v^2\ 3v+3v^2\ \cdots\ (p-1)v+(p-1)v^2], \\ E &= [2v+v^2\ 4v+2v^2\ 6v+3v^2\ \cdots\ 2(p-1)v+(p-1)v^2], \\ F &= [(p-1)v+v^2\ 2(p-1)v+2v^2\ 3(p-1)v+3v^2\ \cdots\ v+(p-1)v^2]. \end{aligned}$$

Notice that the points between E and F indicate that the first element is from $(2+v)v$ to $((p-1)+v)v$.

Let λ_k be a matrix of size $k \times \frac{p^{3k}-p^{2k}}{p-1}$ over R. Let $\lambda_1 = [1\ 2\ \cdots\ p-1\ v\ 2v\ \cdots\ (p-1)v\ 2+v\ 4+2v\cdots\ 2(p-1)+(p-1)v\ 3+v\ 6+2v\cdots\ 3(p-1)+(p-1)v\ \cdots(p-1)+v\ 2(p-1)+2v\cdots\ 1+(p-1)v\ (p-1)+(p-2)v+v^2\ 2(p-1)+2(p-2)v+2v^2\cdots\ 1+2v+(p-1)v^2\ (p-1)v+v^2]$ and

$$\lambda_2 = \begin{bmatrix} 0 & A & B & C & D & E & \cdots & F \\ \lambda_1 & G_1^{\alpha} & \lambda_1 & \lambda_1 & \lambda_1 & \lambda_1 & \cdots & \lambda_1 \end{bmatrix},$$

λ_k is constructed inductively as follows:

$$\lambda_k = \begin{bmatrix} 0 & A & B & C & D & E & \cdots & F \\ \lambda_{k-1} & G_{k-1}^{\alpha} & \lambda_{k-1} & \lambda_{k-1} & \lambda_{k-1} & \lambda_{k-1} & \cdots & \lambda_{k-1} \end{bmatrix},$$

where

$$\begin{aligned} A &= [1\ 2\ \cdots\ p-1\ v\ 2v\ \cdots\ 1+2v+(p-1)v^2\ (p-1)v+v^2], \\ B &= [1+v\ 2+2v\ 3+3v\ \cdots\ (p-1)+(p-1)v], \\ C &= [v+v^2\ 2v+2v^2\ 3v+3v^2\ \cdots\ (p-1)v+(p-1)v^2], \\ D &= [1+2v+v^2\ 2+4v+2v^2\ 3+6v+3v^2\ \cdots\ (p-1)+2(p-1)v+(p-1)v^2], \\ E &= [2+3v+v^2\ 4+6v+2v^2\ 6+9v+3v^2\ \cdots\ 2(p-1)+3(p-1)v+(p-1)v^2], \\ F &= [(p-1)+v^2\ 2(p-1)+2v^2\ 3(p-1)+3v^2\ \cdots\ 1+(p-1)v^2]. \end{aligned}$$

Notice that the points between E and F indicate that the first element is from $(2+v)(1+v)$ to $((p-1)+v)(1+v)$.

Let σ_k be a matrix of size $k \times \frac{p^{3k}-p^{2k}}{p-1}$ over R. Let $\sigma_1 = [1\ 2\ \cdots\ p-1\ v\ 2v\ \cdots\ (p-1)v\ 1+v\ 2+2v\cdots\ (p-1)+(p-1)v\ 2+v\ 4+2v\ \cdots\ 2(p-1)+(p-1)v\ 3+v\ 6+2v\cdots\ 3(p-1)+(p-1)v\ \cdots\ (p-2)+v\ 2(p-2)+2v\cdots\ 2+(p-1)v\ 1+v^2\ 2+2v^2\cdots\ (p-1)+(p-1)v^2\ v+v^2]$ and

$$\sigma_2 = \begin{bmatrix} 0 & A & B & C & D & E & \cdots & F \\ \sigma_1 & G_1^{\alpha} & \sigma_1 & \sigma_1 & \sigma_1 & \sigma_1 & \cdots & \sigma_1 \end{bmatrix},$$

σ_k is constructed inductively as follows:

$$\sigma_k = \begin{bmatrix} 0 & A & B & C & D & \cdots & E \\ \sigma_{k-1} & G_{k-1}^{\alpha} & \sigma_{k-1} & \sigma_{k-1} & \sigma_{k-1} & \cdots & \sigma_{k-1} \end{bmatrix},$$

where

$$\begin{aligned}
A &= [1\ 2\ \cdots\ p-1\ v\ 2v\ \cdots\ (p-1)+(p-1)v^2\ v+v^2],\\
B &= [(p-1)+v\ 2(p-1)+2v\ 3(p-1)+3v\ \cdots\ 1+(p-1)v],\\
C &= [(p-1)v+v^2\ 2(p-1)v+2v^2\ 3(p-1)v+3v^2\ \cdots\ v+(p-1)v^2],\\
D &= [(p-1)+v^2\ 2(p-1)+2v^2\ 3(p-1)+3v^2\ \cdots\ 1+(p-1)v^2],\\
E &= [2(p-1)+v+v^2\ 4(p-1)+2v+2v^2\ \cdots\ 2+(p-1)v+(p-1)v^2],\\
F &= [1+2(p-1)v+v^2\ 2+4(p-1)v+2v^2\ \cdots\ (p-1)+2v+(p-1)v^2].
\end{aligned}$$

Notice that the points between E and F indicate that the first element is from $(2+v)((p-1)+v)$ to $((p-1)+v)((p-1)+v)$.

Let μ_k be a matrix of size $k \times \frac{p^k(p^k-1)^2}{(p-1)^2}$ over R. Let

$$\mu_1 = \begin{bmatrix} 1 & 2 & \cdots & p-1 & v \end{bmatrix}$$

and

$$\mu_2 = \begin{bmatrix} 0 & A & B & C & D \\ \mu_1 & G_1^{\alpha} & \lambda_1 & \sigma_1 & \mu_1 \end{bmatrix},$$

μ_k is constructed inductively as follows:

$$\mu_k = \begin{bmatrix} 0 & A & B & C & D \\ \mu_{k-1} & G_{k-1}^{\alpha} & \lambda_{k-1} & \sigma_{k-1} & \mu_{k-1} \end{bmatrix},$$

where

$$\begin{aligned}
A &= [1\ 2\ \cdots\ p-1\ v],\\
B &= [1+v\ 2+2v\ 3+3v\ \cdots\ (p-1)+(p-1)v\ v+v^2],\\
C &= [(p-1)+v\ 2(p-1)+2v\ \cdots\ 1+(p-1)v\ (p-1)v+v^2],\\
D &= [(p-1)+v^2\ 2(p-1)+2v^2\ 3(p-1)+3v^2\ \cdots\ 1+(p-1)v^2].
\end{aligned}$$

Let ν_k be a matrix of size $k \times \frac{p^k(p^k-1)^2}{(p-1)^2}$ over R. Let

$$\nu_1 = \begin{bmatrix} 1 & 2 & \cdots & p-1 & (p-1)+v \end{bmatrix}$$

and

$$\nu_2 = \begin{bmatrix} 0 & A & B & C & D \\ \nu_1 & G_1^{\alpha} & \delta_1 & \lambda_1 & \nu_1 \end{bmatrix},$$

ν_k is constructed inductively as follows:

$$\nu_k = \begin{bmatrix} 0 & A & B & C & D \\ \nu_{k-1} & G_{k-1}^{\alpha} & \delta_{k-1} & \lambda_{k-1} & \nu_{k-1} \end{bmatrix},$$

where

$$\begin{aligned}
A &= [1\ 2\ \cdots\ p-1\ (p-1)+v],\\
B &= [v\ 2v\ 3v\ \cdots\ (p-1)v\ (p-1)v+v^2],\\
C &= [1+v\ 2+2v\ 3+3v\ \cdots\ (p-1)+(p-1)v\ (p-1)+v^2],\\
D &= [v+v^2\ 2v+2v^2\ 3v+3v^2\ \cdots\ (p-1)v+(p-1)v^2].
\end{aligned}$$

Let ω_k be a matrix of size $k \times \frac{p^k(p^k-1)^2}{(p-1)^2}$ over R. Let

$$\omega_1 = \begin{bmatrix} 1 & 2 & \cdots & p-1 & 1+v \end{bmatrix}$$

and

$$\omega_2 = \begin{bmatrix} 0 & A & B & C & D \\ \omega_1 & G_1^{\alpha} & \delta_1 & \sigma_1 & \omega_1 \end{bmatrix},$$

ω_k is constructed inductively as follows:

$$\omega_k = \begin{bmatrix} 0 & A & B & C & D \\ \omega_{k-1} & G_{k-1}^{\alpha} & \delta_{k-1} & \sigma_{k-1} & \omega_{k-1} \end{bmatrix},$$

where

$$\begin{aligned}
&A = [1\ 2\ \cdots\ p-1\ 1+v],\ B = [v\ 2v\ 3v\ \cdots\ (p-1)v\ v+v^2],\\
&C = [(p-1)+v\ 2(p-1)+2v\ \cdots\ 1+(p-1)v\ (p-1)+v^2],\\
&D = [(p-1)v+v^2\ 2(p-1)v+2v^2\ 3(p-1)v+3v^2\ \cdots\ v+(p-1)v^2].
\end{aligned}$$

Let G_k^{β} be the generator matrix of S_k^{β}, where $k \geq 2$. The size of G_k^{β} is $k \times \frac{(p^k-1)^3}{(p-1)^3}$. G_2^{β} is given as

$$G_2^{\beta} = \begin{bmatrix} 1 & 0 & v & 1+v & (p-1)+v & (p-1)+v^2 & v+v^2 & (p-1)v+v^2 \\ G_1^{\alpha} & 1 & \delta_1 & \lambda_1 & \sigma_1 & \mu_1 & \nu_1 & \omega_1 \end{bmatrix}.$$

G_k^{β} is constructed inductively as follows:

$$G_k^{\beta} = \begin{bmatrix} 1 & 0 & v & 1+v & (p-1)+v & (p-1)+v^2 & v+v^2 & (p-1)v+v^2 \\ G_{k-1}^{\alpha} & G_{k-1}^{\beta} & \delta_{k-1} & \lambda_{k-1} & \sigma_{k-1} & \mu_{k-1} & \nu_{k-1} & \omega_{k-1} \end{bmatrix}.$$

Then, we have the following result. The proof is similar to that of Lemma 1, so we omit it.

Lemma 2 *The torsion codes H_i ($i = 1, 2, 3$) of S_k^{β} are permutation equivalent to each other.*

We can construct type β MacDonald codes similarly to the construction of type α MacDonald codes. For $2 \leq u \leq k-1$, let $G_{k,u}^{\beta}$ be the matrix obtained from G_k^{β} by deleting columns corresponding to the columns of G_u^{β}, i.e.

$$G_{k,u}^{\beta} = \begin{bmatrix} G_k^{\beta} \backslash \mathbf{0} \\ G_u^{\beta} \end{bmatrix},$$

where $[A \backslash B]$ denotes the matrix obtained from the matrix A by deleting the matrix B, and the size of the matrix $\mathbf{0}$ is $(k-u) \times \frac{(p^u-1)^3}{(p-1)^3}$.

Definition 2 The code $C_{k,u}^{\beta}$ generated by $G_{k,u}^{\beta}$ is called a type β MacDonald code.

Let $M^{\beta}_{k,u}$ be the torsion code of $C^{\beta}_{k,u}$. That is the generator matrix of $M^{\beta}_{k,u}$ obtained by replacing $(1-v^2)$ by 1 in the matrix $(1-v^2)G^{\beta}_{k,u}$. Meanwhile, we can get other torsion codes of $C^{\beta}_{k,u}$ by replacing $\frac{v^2+v}{2}$ by 1 in $\frac{v^2+v}{2}G^{\beta}_{k,u}$ and by replacing $\frac{v^2-v}{2}$ by 1 in $\frac{v^2-v}{2}G^{\beta}_{k,u}$, respectively. From Lemma 1, we can see that these three torsion codes are equivalent to each other. Therefore, we only need to study the first case, i.e. we only consider the torsion code $M^{\beta}_{k,u}$. In the following, we give the Hamming weight enumerator of $M^{\beta}_{k,u}$ first.

Theorem 2 *The torsion code $M^{\beta}_{k,u}$ is a p-ary two weights linear code with parameters*

$$\left[\frac{(p^k-1)^3-(p^u-1)^3}{(p-1)^3}, k, \frac{p^{k-1}(p^k-1)^2-p^{u-1}(p^u-1)^2}{(p-1)^2}\right].$$

The number of codewords with Hamming weight $\frac{p^{k-1}(p^k-1)^2}{(p-1)^2}$ is $p^{k-u}-1$, and the number of codewords with Hamming weight $\frac{p^{k-1}(p^k-1)^2-p^{u-1}(p^u-1)^2}{(p-1)^2}$ is p^k-p^{k-u}.

Proof Clearly, the result holds for the case $k=3$ and $u=2$. Suppose that the result holds for the case $k-1$ and $2\le u\le k-2$. Then for the case k and $2\le u\le k-1$, the matrix $(1-v^2)G^{\beta}_{k,u}$ takes the form

$$(1-v^2)G^{\beta}_{k,u}=\begin{bmatrix}(1-v^2)G^{\beta}_{k}\backslash & \mathbf{0}\\ & (1-v^2)G^{\beta}_{u}\end{bmatrix},$$

where G^{β}_{k} is defined above. Therefore, we have that each nonzero codeword of $(1-v^2)G^{\beta}_{k,u}$ has Hamming weight $\frac{p^{k-1}(p^k-1)^2}{(p-1)^2}$ or $\frac{p^{k-1}(p^k-1)^2-p^{u-1}(p^u-1)^2}{(p-1)^2}$, and the dimension of $M^{\beta}_{k,u}$ is k. By the computation, there are $p^{k-u}-1$ codewords of Hamming weight $\frac{p^{k-1}(p^k-1)^2}{(p-1)^2}$ and p^k-p^{k-u} codewords of Hamming weight $\frac{p^{k-1}(p^k-1)^2-p^{u-1}(p^u-1)^2}{(p-1)^2}$. □

At the end of this section, we give an example of the torsion code $M^{\beta}_{3,2}$ to illustrate the main work.

Example 1 Consider the type β MacDonald codes over the ring $\mathbb{F}_3+v\mathbb{F}_3+v^2\mathbb{F}_3$ with $v^3=v$. In this case, we have $G^{\alpha}_1=[0\ 1\ 2\ v\ 2v\ 1+v\ 2+2v\ 2+v\ 1+2v\ v^2\ 1+v^2\ 2+v^2\ v+v^2\ 2v+v^2\ 1+v+v^2\ 2+2v+v^2\ 2+v+v^2\ 1+2v+v^2\ 2v^2\ 1+2v^2\ 2+2v^2\ v+2v^2\ 2v+2v^2\ 1+v+2v^2\ 2+2v+2v^2\ 2+v+2v^2\ 1+2v+2v^2]$,

$$G^{\beta}_2=\begin{bmatrix}1 & 0 & v & 1+v & 2+v & 2+v^2 & v+v^2 & 2v+v^2\\ G^{\alpha}_1 & 1 & \delta_1 & \lambda_1 & \sigma_1 & \mu_1 & \nu_1 & \omega_1\end{bmatrix},$$

where

$$\begin{aligned}\delta_1&=[1\ 2\ 1+v\ 2+2v\ 2+v\ 1+2v\ 1+v+2v^2\ 2+2v+v^2\ 2+v^2],\\ \lambda_1&=[1\ 2\ v\ 2v\ 2+v\ 1+2v\ 2+v+v^2\ 1+2v+2v^2\ 2v+v^2],\\ \sigma_1&=[1\ 2\ v\ 2v\ 1+v\ 2+2v\ 1+v^2\ 2+2v^2\ v+v^2],\\ \mu_1&=[1\ 2\ v],\ \nu_1=[1\ 2\ 2+v],\ \omega_1=[1\ 2\ 1+v]\end{aligned}$$

and

$$G^{\beta}_3=\begin{bmatrix}1 & 0 & v & 1+v & 2+v & 2+v^2 & v+v^2 & 2v+v^2\\ G^{\alpha}_2 & G^{\beta}_2 & \delta_2 & \lambda_2 & \sigma_2 & \mu_2 & \nu_2 & \omega_2\end{bmatrix},$$

where

$$\delta_2 = \begin{bmatrix} 0 & A & v & 2v & v^2 & 2v^2 & v+v^2 & 2v+2v^2 & 2v+v^2 & v+2v^2 \\ \delta_1 & G_1^{\alpha} & \delta_1 & \delta_1 & \delta_1 & \delta_1 & \delta_1 & \delta_1 & \delta_1 & \delta_1 \end{bmatrix},$$
$$A = [1\ 2\ 1+v\ 2+2v\ 2+v\ 1+2v\ 1+v+2v^2\ 2+2v+v^2\ 2+v^2].$$
$$\lambda_2 = \begin{bmatrix} 0 & B & 1+v & 2+2v & v+v^2 & 2v+2v^2 & C \\ \lambda_1 & G_1^{\alpha} & \lambda_1 & \lambda_1 & \lambda_1 & \lambda_1 & \lambda_1 \end{bmatrix},$$
$$B = [1\ 2\ v\ 2v\ 2+v\ 1+2v\ 2+v+v^2\ 1+2v+2v^2\ 2v+v^2],$$
$$C = [1+2v+v^2\ 2+v+2v^2\ 2+v^2\ 1+2v^2].$$
$$\sigma_2 = \begin{bmatrix} 0 & D & 2+v & 1+2v & 2v+v^2 & v+2v^2 & E \\ \sigma_1 & G_1^{\alpha} & \sigma_1 & \sigma_1 & \sigma_1 & \sigma_1 & \sigma_1 \end{bmatrix},$$
$$D = [1\ 2\ v\ 2v\ 1+v\ 2+2v\ 1+v^2\ 2+2v^2\ v+v^2],$$
$$E = [2+v^2\ 1+2v^2\ 1+v+v^2\ 2+2v+2v^2].$$
$$\mu_2 = \begin{bmatrix} 0 & F & 1+v & 2+2v & v+v^2 & 2+v & 1+2v & 2v+v^2 & H \\ \mu_1 & G_1^{\alpha} & \lambda_1 & \lambda_1 & \lambda_1 & \sigma_1 & \sigma_1 & \sigma_1 & \mu_1 \end{bmatrix},$$
$$F = [1\ 2\ v],\ H = [2+v^2\ 1+2v^2].$$
$$\nu_2 = \begin{bmatrix} 0 & I & v & 2v & 2v+v^2 & 1+v & 2+2v & 2+v^2 & v+v^2 & 2v+2v^2 \\ \nu_1 & G_1^{\alpha} & \delta_1 & \delta_1 & \delta_1 & \lambda_1 & \lambda_1 & \lambda_1 & \nu_1 & \nu_1 \end{bmatrix},$$
$$I = [1\ 2\ 2+v].$$

and

$$\omega_2 = \begin{bmatrix} 0 & J & v & 2v & v+v^2 & 2+v & 1+2v & 2+v^2 & 2v+v^2 & v+2v^2 \\ \omega_1 & G_1^{\alpha} & \delta_1 & \delta_1 & \delta_1 & \sigma_1 & \sigma_1 & \sigma_1 & \omega_1 & \omega_1 \end{bmatrix}.$$
$$J = [1\ 2\ 1+v].$$

Let $G_k^{\alpha'}$ be the matrix replacing $(1-v^2)$ by 1 in $(1-v^2)G_k^{\alpha}$, $G_k^{\beta'}$ be the matrix replacing $(1-v^2)$ by 1 in $(1-v^2)G_k^{\beta}$. In addition, δ_k', λ_k', σ_k', μ_k', ν_k' and ω_k' be the matrices replacing $(1-v^2)$ by 1 in $(1-v^2)\delta_k$, $(1-v^2)\lambda_k$, $(1-v^2)\sigma_k$, $(1-v^2)\mu_k$, $(1-v^2)\nu_k$ and $(1-v^2)\omega_k$, respectively. Then, we have

$$G_1^{\alpha'} = [0\ 1\ 2\ 0\ 0\ 1\ 2\ 2\ 1\ 0\ 1\ 2\ 0\ 0\ 1\ 2\ 2\ 1\ 0\ 1\ 2\ 0\ 0\ 1\ 2\ 2\ 1],$$
$$G_2^{\alpha'} = \begin{bmatrix} 0 & 1 & 2 & 0 & 0 & 1 & 2 & 2 & 1 & \cdots & 2 & 2 & 1 \\ G_1^{\alpha'} & G_1^{\alpha'} & G_1^{\alpha'} & G_1^{\alpha'} & G_1^{\alpha'} & G_1^{\alpha'} & G_1^{\alpha'} & G_1^{\alpha'} & G_1^{\alpha'} & \cdots & G_1^{\alpha'} & G_1^{\alpha'} & G_1^{\alpha'} \end{bmatrix},$$
$$G_2^{\beta'} = \begin{bmatrix} 1 & 0 & 0 & 1 & 2 & 2 & 0 & 0 \\ G_1^{\alpha'} & 1 & \delta_1' & \lambda_1' & \sigma_1' & \mu_1' & \nu_1' & \omega_1' \end{bmatrix},$$
$$\delta_2' = \begin{bmatrix} 0 & A & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \delta_1' & G_1^{\alpha'} & \delta_1' & \delta_1' & \delta_1' & \delta_1' & \delta_1' & \delta_1' & \delta_1' & \delta_1' \end{bmatrix},$$
$$A = [1\ 2\ 1\ 2\ 2\ 1\ 1\ 2\ 2].$$
$$\lambda_2' = \begin{bmatrix} 0 & B & 1 & 2 & 0 & 0 & 1 & 2 & 2 & 1 \\ \lambda_1' & G_1^{\alpha'} & \lambda_1' & \lambda_1' & \lambda_1' & \lambda_1' & \lambda_1' & \lambda_1' & \lambda_1' & \lambda_1' \end{bmatrix},$$
$$B = [1\ 2\ 0\ 0\ 2\ 1\ 2\ 1\ 0].$$
$$\sigma_2' = \begin{bmatrix} 0 & C & 2 & 1 & 0 & 0 & 2 & 1 & 1 & 2 \\ \sigma_1' & G_1^{\alpha'} & \sigma_1' & \sigma_1' & \sigma_1' & \sigma_1' & \sigma_1' & \sigma_1' & \sigma_1' & \sigma_1' \end{bmatrix},$$
$$C = [1\ 2\ 0\ 0\ 1\ 2\ 1\ 2\ 0].$$

$$\mu_2' = \begin{bmatrix} 0 & 1 & 2 & 0 & 1 & 2 & 0 & 2 & 1 & 0 & 2 & 1 \\ \mu_1' & G_1^{\alpha'} & G_1^{\alpha'} & G_1^{\alpha'} & \lambda_1' & \lambda_1' & \lambda_1' & \sigma_1' & \sigma_1' & \sigma_1' & \mu_1' & \mu_1' \end{bmatrix},$$

$$\nu_2' = \begin{bmatrix} 0 & 1 & 2 & 2 & 0 & 0 & 0 & 1 & 2 & 2 & 0 & 0 \\ \nu_1' & G_1^{\alpha'} & G_1^{\alpha'} & G_1^{\alpha'} & \delta_1' & \delta_1' & \delta_1' & \lambda_1' & \lambda_1' & \lambda_1' & \nu_1' & \nu_1' \end{bmatrix},$$

and

$$\omega_2' = \begin{bmatrix} 0 & 1 & 2 & 1 & 0 & 0 & 0 & 2 & 1 & 2 & 0 & 0 \\ \omega_1' & G_1^{\alpha'} & G_1^{\alpha'} & G_1^{\alpha'} & \delta_1' & \delta_1' & \delta_1' & \sigma_1' & \sigma_1' & \sigma_1' & \omega_1' & \omega_1' \end{bmatrix}.$$

Therefore, the generator matrix $G_{3,2}^{\beta'}$ of $M_{3,2}^{\beta}$ is

$$G_{3,2}^{\beta'} = \begin{bmatrix} 1 & 0 & 0 & 1 & 2 & 2 & 0 & 0 \\ G_2^{\alpha'} & G_2^{\beta'} & \delta_2' & \lambda_2' & \sigma_2' & \mu_2' & \nu_2' & \omega_2' \end{bmatrix}.$$

By the Magma computational algebra system (see Bosma et al. 1997), the torsion code $M_{3,2}^{\beta}$ is a 3-ary [2133, 3, 1473] linear code with Hamming weight distributions $A_H(0) = 1$, $A_H(1473) = 24$ and $A_H(1521) = 2$.

3 Secret sharing schemes from MacDonald codes over R

A secret sharing scheme is a method that a dealer distributes shares of a secret to participants such that only qualified subsets of participants can recover the secret from their shares. Let $\mathcal{P} = \{P_1, P_2, \ldots, P_{n-1}\}$ be a set of participants. We use s to denote a secret. If a set $A \subseteq \mathcal{P}$ can recover the secret s, then A is called a qualified set. Otherwise, it is called a unqualified set. A secret sharing scheme is called *perfect* if all the unqualified sets cannot get any information about the secret s in the information theoretic sense. Throughout this paper, we consider only perfect secret sharing schemes. If the shares are of the same size as that of the secret s, the secret sharing scheme is called *ideal*. A *minimal qualified set* B is that if $B \subseteq \mathcal{P}$ is a qualified set and for all $C \subset B$ with C is an unqualified set. The *access structure* of a secret sharing scheme is defined to be the set of all qualified sets.

In Massey (1993), the author gave a method of constructing secret sharing schemes by linear codes over finite field $\mathbb{F}_q$. We employ the same method in this section. Let C ba an $[n, k]_q$ linear code over $\mathbb{F}_q$, and $G = [g_0, g_1, \ldots, g_{n-1}]$ be the generator matrix of C. Let $C^{\perp}$ be the dual code of C, and $H = [h_0, h_1, \ldots, h_{n-1}]$ be the generator matrix of $C^{\perp}$.

In the secret sharing scheme based on C, the secret s is an element of $\mathbb{F}_q$, and $n-1$ parties $P_1, P_2, \ldots, P_{n-1}$ and a dealer are involved. To compute shares with respect to a secret s, the dealer chooses randomly a vector $u = (u_0, u_1, \ldots, u_{n-k-1})$ such that $s = uh_0$. The dealer then treats u as an information vector and computes the corresponding codeword

$$t = (t_0, t_1, \ldots, t_{n-1}) = uH.$$

He then gives t_i to party P_i as share for each $i \geq 1$.

Note that $t_0 = uh_0 = s$. Clearly, a set of shares $\{t_{i_1}, t_{i_2}, \ldots, t_{i_m}\}$, $1 \leq i_1 < \cdots < i_m \leq n-1$ and $1 \leq m \leq n-1$, determines the secret if and only if h_0 is a linear combination of $h_{i_1}, h_{i_2} \ldots, h_{i_m}$. Generally, we have the following result.

Lemma 3 (Massey 1993) *Let G be a generator matrix of an $[n, k]_q$ linear code C. In the secret sharing scheme based on C, a set of shares $\{t_{i_1}, t_{i_2}, \ldots, t_{i_m}\}$, $1 \leq i_1 < \cdots < i_m \leq n-1$ and $1 \leq m \leq n-1$, determines the secret if and only if there is a codeword*

$(1, 0, \ldots, 0, c_{i_1}, 0, \ldots, 0, c_{i_m}, 0, \ldots, 0)$ in the dual code $C^\perp$, where $c_{i_j} \neq 0$ for at least one j.

To describe the secret sharing scheme of a linear code, we also need to introduce the covering problem of linear codes.

The *support* of a vector $c = (c_0, c_1, \ldots, c_{n-1})$ is defined as the set $\{0 \leq i \leq n-1 \mid c_i \neq 0\}$. We say that a vector c_1 covers a vector c_2 if the support of c_1 contains that of c_2 as a proper subsets. If a nonzero codeword c covers only its scalar multiples, but no other nonzero codewords, then it is called a *minimal codeword*. The *covering problem* of a linear code C is to determine its all minimal codewords. This is a very hard problem in general, but can be solved for certain types of linear codes. From Lemma 3, we can see that there is a one-to-one correspondence between the set of minimal qualified sets and the set of minimal codewords with 1 as its first component in the dual code $C^\perp$.

The access structure of the secret sharing scheme based on a linear code is very complex in general, but can be determined in certain special cases.

Lemma 4 (Ding and Yuan 2003) *Let C be an $[n, k]_q$ linear code and $G = [g_0, g_1, \ldots, g_{n-1}]$ be its generator matrix. If each nonzero codeword of C is a minimal codeword, then in the secret sharing scheme based on $C^\perp$, there are altogether q^{k-1} minimal qualified sets. In addition, we have the following:*

1. *If g_i is a multiple of g_0, $1 \leq i \leq n-1$, then participant P_i must be in every minimal qualified set.*
2. *If g_i is not a multiple of g_0, $1 \leq i \leq n-1$, then participant P_i must be in $(q-1)q^{k-2}$ out of q^{k-1} minimal qualified set.*

When the conditions of Lemma 3 are satisfied, the secret sharing scheme based on the dual code $C^\perp$ is interesting. In the following, we give a lemma to construct a linear code whose nonzero codewords are all minimal.

Lemma 5 (Ashikhmin and Barg 1998) *In an $[n, k]_q$ linear code C, let $w_{\min}$ and $w_{\max}$ be the minimum and maximum nonzero weights, respectively. If $\frac{w_{\min}}{w_{\max}} > \frac{q-1}{q}$, then all the codewords of C are minimal.*

Let $G^\alpha_{k,u}$ and $G^\beta_{k,u}$ be the generator matrices of the torsion codes $M^\alpha_{k,u}$ and $M^\beta_{k,u}$, respectively. In the following, we will prove that all the codewords of the torsion codes $M^\alpha_{k,u}$ and $M^\beta_{k,u}$ are minimal.

Proposition 1 *In the secret sharing scheme based on ${M^\alpha_{k,u}}^\perp$, there are $p^{3k} - p^{3u} - 1$ participants and p^{k-1} minimal qualified sets. If the ith column of $G^\alpha_{k,u}$ is a multiple of the 0th column of $G^\alpha_{k,u}$, then participant P_i is in every minimal qualified set. Otherwise, each participant P_i is involved in exactly $(p-1)p^{k-2}$ out of p^{k-1} minimal qualified sets.*

Proof Let $w_{\min}$ and $w_{\max}$ be the minimum and maximum nonzero weights in the torsion code $M^\alpha_{k,u}$. From Theorem 1, we know that $w_{\min} = (p-1)(p^{3k-1} - p^{3u-1})$ and $w_{\max} = (p-1)p^{3k-1}$. Therefore, we have

$$\frac{w_{\min}}{w_{\max}} = \frac{(p-1)(p^{3k-1} - p^{3u-1})}{(p-1)p^{3k-1}} = 1 - \frac{1}{p^{3(k-u)}} > \frac{p-1}{p},$$

where $1 \leq u \leq k-1$. By Lemma 5, we have that all the codewords of $M^\alpha_{k,u}$ are minimal. Then, the conclusion comes from Lemma 4. □

Proposition 2 *In the secret sharing scheme based on* $M_{k,u}^{\beta\ \perp}$, *there are* $\frac{(p^k-1)^3-(p^u-1)^3}{(p-1)^3}-1$ *participants and* p^{k-1} *minimal qualified sets. If the* i*th column of* $G_{k,u}^{\beta}$ *is a multiple of the* 0*th column of* $G_{k,u}^{\beta}$, *then participant* P_i *is in every minimal qualified set. Otherwise each participant* P_i *is involved in exactly* $(p-1)p^{k-2}$ *out of* p^{k-1} *minimal qualified sets.*

Proof Let $w_{\min}$ and $w_{\max}$ be the minimum and maximum nonzero weights in the torsion code $M_{k,u}^{\beta}$. From Theorem 2, we know that

$$w_{\min}=\frac{p^{k-1}(p^k-1)^2-p^{u-1}(p^u-1)^2}{(p-1)^2} \quad \text{and} \quad w_{\max}=\frac{p^{k-1}(p^k-1)^2}{(p-1)^2}.$$

Therefore, we have

$$\frac{w_{\min}}{w_{\max}}=\frac{p^{k-1}(p^k-1)^2-p^{u-1}(p^u-1)^2}{p^{k-1}(p^k-1)^2}=1-\frac{(p^u-1)^2}{p^{(k-u)}(p^k-1)^2}>\frac{p-1}{p},$$

where $2\le u\le k-1$. By Lemma 5, we have that all the codewords of $M_{k,u}^{\beta}$ are minimal. Then, the conclusion comes from Lemma 4. □

Example 2 By Example 1, we have that the Hamming weight distributions of torsion code $M_{3,2}^{\beta}$ are $A_H(0)=1$, $A_H(1473)=24$ and $A_H(1521)=2$. In the following, we construct secret sharing schemes based on $M_{3,2}^{\beta\perp}$. We have 2132 participants and 9 minimal qualified sets. We can consider participants P_i, where $i\in Q=\{3, 5, 9, 12, 13, 18, 21, 22, 81, 84, 85, 90, 93, 94, 99, 102, 103, 108, 111, 112, 117, 120, 121, 126, 129, 130, 243, 246, 247, 252, 255, 256, 261, 264, 265, 324, 327, 328, 333, 336, 337, 342, 345, 346, 351, 354, 355, 360, 363, 364, 369, 372, 373, 486, 489, 490, 495, 498, 499, 504, 507, 508, 567, 570, 571, 576, 579, 580, 585, 588, 589, 594, 597, 598, 603, 606, 607, 612, 615, 616, 1055, 1056, 1061, 1116, 1119, 1120, 1125, 1128, 1129, 1134, 1137, 1138, 1143, 1146, 1147, 1152, 1155, 1156, 1161, 1164, 1165, 1278, 1281, 1282, 1287, 1290, 1291, 1296, 1299, 1300, 1325, 1326, 1331, 1334, 1335, 1340, 1379, 1380, 1385, 1440, 1443, 1444, 1449, 1452, 1453, 1458, 1461 1462, 1467, 1470, 1471, 1476, 1479, 1480, 1485, 1487, 1489, 1602, 1605, 1606, 1611, 1614, 1615, 1620, 1623, 1624, 1649, 1650, 1655, 1658, 1659, 1664, 1703, 1758, 1761, 1762, 1767, 1770, 1771, 1776, 1779, 1780, 1805, 1806, 1811, 1832, 1833, 1838\}$.
Since these columns of $G_{3,2}^{\beta}$ are multiples of the 0th column of $G_{3,2}^{\beta}$, then these participants $P_i, i\in Q$ must be in every minimal qualified set. Other participants P_j must be in exactly 6 out of 9 minimal qualified sets, where $0<j\notin Q$.

4 Association schemes from MacDonald codes over R

In Luo et al. (2018), the authors obtained a class of linear codes with two weights over $\mathbb{F}_q$. They also employed these linear codes to construct association schemes. Similarly, we can use MacDonald codes of type α over R to construct association schemes. Let X be a finite set with the cardinality of X greater than 2. Denote by $X\times X$ the Cartesian product of X. For a positive integer d, consider a set $L=\{L_0, L_1, \ldots, L_d\}$, where $L_i, i=0, 1, \ldots, d$, is a subset of $X\times X$.

Definition 3 (Luo et al. 2018) Let X be a finite set with the cardinality of X greater than 2, $L_0=\{(a,a)|\ a\in X\}$, $L_i=\{(a,b)|\ a,b\in X\}$, $i=1,2,\ldots,d$. Let $X\times X$ is a disjoint

union of $L_0, L_1, \ldots, L_d$. For each integer $i, j, k \in \{0, 1, \ldots, d\}$, there exists an integer $j \in \{0, 1, \ldots, d\}$ such that $L_j = L_i^t$, where $L_i^t = \{(a, b)|\ (b, a) \in L_i\}$. And each pair $(a, b) \in L_k$, the cardinality of set $\{c \in X|\ (a, c) \in L_i, (c, b) \in L_j\}$ is equal to a constant integer p_{ij}^k. Then, the pair (X, L) is called a d-class association scheme.

Let $X = \mathbb{F}_p^n$. For any $\mathbf{x}, \mathbf{y} \in X$, denote the Hamming distance of $\mathbf{x}$ and $\mathbf{y}$ by $d(\mathbf{x}, \mathbf{y})$, where $d(\mathbf{x}, \mathbf{y}) = \#\{i \mid 1 \le i \le n, x_i \ne y_i\}$. Let $L_i = \{(\mathbf{x}, \mathbf{y}) \in \mathbb{F}_p^n \times \mathbb{F}_p^n |\ d(\mathbf{x}, \mathbf{y}) = i\}$, $L = \{L_0, L_1, \ldots, L_d\}$. Then, $(\mathbb{F}_p^n, L)$ is an n-class association scheme known as the Hamming association scheme.

In Luo et al. (2018), the authors give a necessary and sufficient condition for constructing a 2-class association scheme from a linear code with parameters $[n, 2]$.

Lemma 6 (Luo et al. 2018) *Assume that C is an $[n, 2]$ linear code over $\mathbb{F}_q$ with nonzero weights w_1 and w_2. Let c_1, c_2 be two codewords of C such that c_1, c_2 are linear independent and $w(c_1) = w(c_2) = w_1$. For any $a, b \in \mathbb{F}_q^*$, if $w(ac_1 + bc_2) = w_2$, then the restriction to C of the Hamming association scheme is a 2-class association scheme if and only if $w_2 \ne w_1 + 1$.*

In the following, we give an proposition to show that 2-class association schemes can be constructed by MacDonald codes over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$.

Proposition 3 *Let $M_{2,1}^\alpha$ be a torsion code of MacDonald codes of type α over the ring $\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p$ with $v^3 = v$. Let c_1, c_2 be two codewords of $M_{2,1}^\alpha$ such that c_1, c_2 are linear independent and $w(c_1) = w(c_2) = w_1$. For any $a, b \in \mathbb{F}_p^*$, if $w(ac_1 + bc_2) = w_2$, then the restriction to $M_{2,1}^\alpha$ of the Hamming association scheme is a 2-class association scheme.*

Proof By Theorem 1, we have that $M_{2,1}^\alpha$ is an $[p^6 - p^3, 2, (p-1)(p^5 - p^2)]$ linear code over $\mathbb{F}_q$ with nonzero weights $w_1 = (p-1)(p^5 - p^2)$ and $w_2 = (p-1)p^5$. Clearly, $w_1 + 1 \ne w_2$ for p is an odd prime. Then, the conclusion comes from Lemma 6. □

Example 3 Consider the torsion code $M_{2,1}^\alpha$ of MacDonald codes of type α over the ring $\mathbb{F}_3 + v\mathbb{F}_3 + v^2\mathbb{F}_3$ with $v^3 = v$. The generator matrix $G_{2,1}^{\alpha'}$ of $M_{2,1}^\alpha$ is given by

$$G_{2,1}^{\alpha'} = \begin{bmatrix} 1 & 2 & 0 & 0 & 1 & 2 & 2 & 1 & A & A \\ G_1^{\alpha'} & G_1^{\alpha'} & G_1^{\alpha'} & G_1^{\alpha'} & G_1^{\alpha'} & G_1^{\alpha'} & G_1^{\alpha'} & G_1^{\alpha'} & G_1^{\alpha'} & G_1^{\alpha'} \end{bmatrix},$$

where $A = [0\ 1\ 2\ 0\ 0\ 1\ 2\ 2\ 1]$. By the Magma computational algebra system (Bosma et al. 1997), the torsion code $M_{2,1}^\alpha$ is a 3-ary [702, 2, 468] code with Hamming weight distributions $A_H(0) = 1$, $A_H(468) = 6$ and $A_H(486) = 2$.

Let $c_0 = $ (0, 1, 2, 0, 0, 1, 2, 2, 1, 0, 1, 2, 0, 0, 1,

2, 2, 1, 0, 1, 2, 0, 0, 1, 2, 2, 1 and $c_1 = ($1, 2, 0, 1, 1, 2, 0, 0, 2, 1, 2, 0, 1, 1, 2, 0, 0, 2, 1, 2, 0, 1, 1, 2, 0, 0, 2, 2, 0, 1, 2, 2, 0, 1, 1, 0, 2, 0, 1, 2, 2, 0, 1, y1, 0, 2, 0, 1, 2, 2, 0, 1, 1, 0, 0, 1, 2, 0, 0, 1, 2, 2, 1, 0, 1, 2, 0, 0, 1, 2, 2, 1, 0, 1, 2, 0, 0, 1, 2, 2, 1, 0, 1, 2, 0, 0, 1, 2, 2, 1, 0, 1, 2, 0, 0, 1, 2, 2, 1, 1, 2, 0, 1, 1, 2, 0, 0, 2, 1, 2, 0, 1, 1, 2, 0, 0, 2, 1, 2, 0, 1, 1, 2, 0, 0, 2, 2, 0, 1, 2, 2, 0, 1, 1, 0, 2, 0, 1, 2, 2, 0, 1, 1, 0, 2, 0, 1, 2, 2, 0, 1, 1, 0, 1, 2, 0, 1, 1, 2, 0, 0, 2, 1, 2, 0, 1, 1, 2, 0, 0, 2, 1, 2, 0, 1, 1, 2, 0, 0, 2, 2, 0, 1, 2, 2, 0, 1, 1, 0, 2, 0, 1, 2, 2, 0, 1, 1, 0, 2, 0, 1, 2, 2, 0, 1, 1, 0, 0, 1, 2, 0, 0, 1, 2, 2, 1, 0, 1, 2, 0, 0, 1, 2, 2, 1, 0, 1, 2, 0, 0, 1, 2, 2, 1, 1, 2, 0, 1, 1, 2, 0, 0, 2, 1, 2, 0, 1, 1, 2, 0, 0, 2, 1, 2, 0, 1, 1, 2, 0, 0, 2, 2, 0, 1, 2, 2, 0, 1, 1, 0, 2, 0, 1, 2, 2, 0, 1, 1, 0, 2, 0, 1, 2, 2, 0, 1, 1, 0, 0, 1, 2, 0, 0, 1, 2, 2, 1, 0, 1, 2, 0, 0, 1, 2, 2, 1, 0, 1, 2, 0, 0, 1, 2, 2, 1, 0, 1, 2, 0, 0, 1, 2, 2, 1, 0, 1, 2, 0, 0, 1, 2, 2, 1, 0, 1, 2, 0, 0, 1, 2, 2, 1, 1, 2, 0, 1, 1, 2, 0, 0, 2, 1, 2, 0, 1, 1, 2, 0, 0, 2, 1, 2, 0, 1, 1, 2, 0, 0, 2, 2, 0, 1, 2, 2, 0, 1, 1, 0, 2, 0, 1, 2, 2, 0, 1, 1, 0, 2, 0, 1, 2, 2, 0, 1, 1, 0, 1, 2, 0, 1, 1, 2, 0, 0, 2, 1, 2, 0, 1, 1, 2, 0, 0, 2, 1, 2, 0, 1, 1, 2, 0, 0, 2, 2, 0, 1, 2, 2, 0, 1, 1, 0, 2, 0, 1, 2, 2, 0, 1, 1, 0, 2, 0, 1, 2, 2, 0, 1, 1, 0). We find that both codewords c_0 and c_1 are linear independent and $w(c_0) = w(c_1) = 468$, $2w(c_0) + w(c_1) = 486$. Consequently, the restriction to $M^{\alpha}_{2,1}$ of the Hamming scheme is a 2-class association scheme.

5 Conclusion

In this paper, we studied MacDonald codes over the finite non-chain ring $\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p$, where p is an odd prime and $v^3 = v$. Some applications of MacDonald codes were also investigated in this paper. For $p = 2$, the ring $\mathbb{F}_2 + v\mathbb{F}_2 + v^2\mathbb{F}_2$ has different structural properties from the ring $\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p$ with p an odd prime (see Shi et al. 2013). It is interesting to consider MacDonald codes and their applications over this ring. Further, the ring $\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p$ is the special case of the ring $\mathbb{F}_p[v]/\langle v^m - v\rangle$ with $m = 3$. Based on the complexity of the generator matrix of MacDonald codes, considering MacDonald codes and their applications over the general finite non-chain ring $\mathbb{F}_p[v]/\langle v^m - v\rangle$ may be an interesting and challenging work.

Acknowledgements This research is supported by the National Natural Science Foundation of China (Grant Nos. 11701336, 11626144 and 11671235), and the Scientific Research Fund of Hunan Provincial Key Laboratory of Mathematical Modeling and Analysis in Engineering (No. 2018MMAEZD04).

References

Ashikhmin A, Barg A (1998) Minimal vectors in linear codes. IEEE Trans Inf Theory 44(5):2010–2017

Bosma W, Cannon J, Playoust C (1997) The Magma algebra system I: the user language. J Symb Comput 24(3):235–265

Colbourn, C, Gupta, M (2003) On quaternary MacDonald codes. In: Proceeding of IEEE international conference on information technology: coding and computing. Las Vegas, pp 212–215

Delsarte P (1973) An algebraic approach to the association schemes of coding theory. J Philips Res Rep Suppl 10:97

Dertli A, Cengellenmis Y (2011) MacDonald codes over the ring $\mathbb{F}_2 + v\mathbb{F}_2$. Int J Algebra 5(20):985–991

Ding C, Yuan J (2003) Covering and secret sharing with linear codes. Discrete mathematics and theoretical computer science. Springer, LNCS 2731, Berlin, Heidelberg, pp 11–25

Gao J (2015) Some results on linear codes over $\mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p$. J Appl Math Comput 47(1–2):473–485

Luo G, Cao X, Xu G, Xu S (2018) A new class of optimal linear codes with flexible parameters. Discrete Appl Math 237:126–131

MacDonald J (1960) Design methods for maximum minimum distance errorcorrecting codes. IBM J Res Dev 4:43–57

Massey JL (1993) Minimal codewords and secret sharing. In: Proceedings of the 6th Joint Swedish-Russian workshop on information theory, Netherlands, Veldhoven, pp 276–279

Patel A (1975) Maximal q-ary linear codes with large minimum distance. IEEE Trans Inf Theory 21:106–110

Shi M, Guan Y, Solé P (2017a) Two new families of two-weight codes. IEEE Trans Inf Theory 63(10):6240–6246

Shi M, Solé P, Wu B (2013) Cyclic codes and weight enumerators of linear codes over $\mathbb{F}_2 + v\mathbb{F}_2 + v^2\mathbb{F}_2$. Appl Comput Math 12(2):247–255

Shi M, Xu L, Yang G (2017b) A note on one weight and two weight projective $\mathbb{Z}_4$-codes. IEEE Trans Inf Theory 63(1):177–182

Wang X, Gao J, Fu F-W (2016) Secret sharing schemes from linear codes over $\mathbb{F}_p + v\mathbb{F}_p$. Int J Found Comput Sci 27(5):595–605