Cryptogr. Commun. (2017) 9:545–562
DOI 10.1007/s12095-016-0198-1

Complete weight enumerators of two classes of linear codes

Xianfang Wang[1] · Jian Gao[2] · Fang-Wei Fu[1]

Received: 23 December 2015 / Accepted: 28 June 2016 / Published online: 7 July 2016

Abstract In this paper, we give the complete weight enumerators of two classes of linear codes over the finite field $\mathbb{F}_p$, where p is a prime. These linear codes are the torsion codes of MacDonald codes over the finite non-chain ring $\mathbb{F}_p + v\mathbb{F}_p$, where $v^2 = v$. We also employ these linear codes to construct systematic authentication codes with new parameters.

Keywords Complete weight enumerators · Linear codes · A finite non-chain ring · Authentication codes

Mathematics Subject Classification (2010) 94B05 · 11T71 · 94A62

1 Introduction

Let $\mathbb{F}_q$ be a finite field with q elements. An $[n, k, d]$ linear code $\mathcal{C}$ over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$ with minimal (Hamming) distance d. Let $\mathbf{c} = (c_1, c_2, \cdots, c_n)$ be a codeword of $\mathcal{C}$. The support of $\mathbf{c}$ is defined as $\mathrm{supp}(\mathbf{c}) = \{i : c_i \neq 0\}$. Then the (Hamming)

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

Xianfang Wang
xianfw@mail.nankai.edu.cn

Fang-Wei Fu
fwfu@nankai.edu.cn

[1] Chern Institute of Mathematics and LPMC, Nankai University, Tianjin, 30007, People's Republic of China

[2] School of Science, Shandong University of Technology, Zibo, 255091, People's Republic of China

weight $w(\mathbf{c})$ of $\mathbf{c}$ is $w(\mathbf{c}) = |\mathrm{supp}(\mathbf{c})|$. Let A_i denote the number of codewords with Hamming weight i in $\mathcal{C}$. The weight enumerator of $\mathcal{C}$ is defined by

$$A_0 + A_1 z + A_2 z^2 + \cdots + A_n z^n.$$

The definition of the complete weight enumerator of linear codes is given in [18, 19]. We recall the definition as that in [15]. Let the elements of $\mathbb{F}_q$ be $\omega_0 = 0, \ \omega_1, \ \omega_2, \cdots, \omega_{q-1}$. The composition of a vector $\mathbf{v} = (v_0, v_1, \cdots, v_{n-1}) \in \mathbb{F}_q^n$ is defined to be $\mathrm{comp}(\mathbf{v}) = (t_0, t_1, \cdots, t_{q-1})$, where each $t_i = t_i(\mathbf{v})$ is the number of components v_j $(0 \le j \le n-1)$ of $\mathbf{v}$ that are equal to ω_i. Clearly, $\sum_{i=0}^{q-1} t_i = n$. Let $A(t_0, t_1, \cdots, t_{q-1})$ be the number of codewords $\mathbf{c} \in \mathcal{C}$ with $\mathrm{comp}(c) = (t_0, t_1, \cdots, t_{q-1})$. Then the complete weight enumerator of $\mathcal{C}$ is the polynomial

$$\begin{aligned} W_{\mathcal{C}}(z_0, z_1, \cdots, z_{q-1}) &= \sum_{\mathbf{c}\in\mathcal{C}} z_0^{t_0(\mathbf{c})} z_1^{t_1(\mathbf{c})} \cdots z_{q-1}^{t_{q-1}(\mathbf{c})} \\ &= \sum_{(t_0,t_1,\cdots,t_{q-1})\in B_n} A(t_0, t_1, \cdots, t_{q-1}) z_0^{t_0} z_1^{t_1} \cdots z_{q-1}^{t_{q-1}}, \end{aligned}$$

where $B_n = \left\{(t_0, t_1, \cdots, t_{q-1}) : 0 \le t_i \le n, \sum_{i=0}^{q-1} t_i = n\right\}$. If we let $z_0 = 1, \ z_1 = z_2 = \cdots z_{q-1} = z$, then the complete weight enumerator of $\mathcal{C}$ is the weight enumerator of $\mathcal{C}$. For binary linear codes, the complete weight enumerators are just the Hamming weight enumerators.

The complete weight enumerators are applied to study the monomial and quadratic bent functions [11]. It was pointed out that the complete weight enumerators can be used to calculate the deception probabilities of certain authentication codes in [8, 9]. Blake and Kith [3, 12] researched the complete weight enumerators of Reed-Solomon codes. The complete weight enumerators of the generalized Kerdock code and related linear codes over Galois rings are given by Kuzmin and Nechaev [13, 14]. Recently, the complete weight enumerators of linear codes or cyclic codes over finite fields were studied in [2, 10, 15–17, 24–28]. The weight enumerators of the torsion codes of MacDonald codes over the finite non-chain ring $\mathbb{F}_p + v\mathbb{F}_p$, where p is a prime, have been given in [23], it was used to study the access structure of secret sharing. To the best of our knowledge, the complete weight enumerators of these torsion codes have not been studied.

In this paper, we will investigate the complete weight enumerators of the torsion codes of MacDonald codes over the finite non-chain ring $\mathbb{F}_p + v\mathbb{F}_p$. We will recall the definitions of MacDonald codes and its torsion codes in Section 2. In Section 3, we will give the complete weight enumerators of these torsion codes. Some applications of these complete weight enumerators in authentication codes will be considered in Section 4.

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

Let R be the ring $\mathbb{F}_p + v\mathbb{F}_p$, where p is a prime and $v^2 = v$. Clearly, R is isomorphic to the quotient ring $\mathbb{F}_p[v]/\langle v^2 - v\rangle$. R is a commutative ring with identity and characteristic p. For any element $r \in R$, there are unique $a, b \in \mathbb{F}_p$ such that $r = a + bv$. Further, R is principal and has two maximal ideals $\langle v\rangle$ and $\langle 1 - v\rangle$. It means that R is not a local ring, which implies that R is a finite non-chain ring.

In this section, we will recall the definitions of MacDonald codes over R and their torsion codes. The MacDonald code is a punctured code of the simplex code. The MacDonald code over $\mathbb{F}_2$ was first introduced by MacDonald [20]. The formal definition of the MacDonald code and its torsion code will be given below. MacDonald codes from simplex codes of type α over the ring $\mathbb{F}_2 + v\mathbb{F}_2$ with $v^2 = v$ could be found in [7]. In [5], MacDonald codes from simplex codes of type α over the ring $\mathbb{F}_3 + v\mathbb{F}_3$ with $v^2 = 1$ were given. Simplex codes of type β over the ring $\mathbb{F}_3 + v\mathbb{F}_3$ with $v^2 = 1$ were studied in [6]. Recently, the weight enumerators of the torsion codes of MacDonald codes from simplex codes of type α and type β over the ring R were given in [23].

In the following, we give the definition of the torsion code first. A linear code $\mathcal{C}$ over R of length n is an R-submodule of R^n. For any linear code $\mathcal{C}$ over R , we have $\mathcal{C} = (1-v)H^+ \oplus vH^-$, where $H^+ = \{s : \exists t \in \mathbb{F}_p^n \; such \; that \; (1-v)s + vt \in \mathcal{C}\}$ and $H^- = \{t : \exists s \in \mathbb{F}_p^n \; such \; that \; (1-v)s + vt \in \mathcal{C}\}$. Clearly, H^+ and H^- are both linear codes of length n over $\mathbb{F}_p$. We define H^+ and H^- as the torsion codes of $\mathcal{C}$.

2.1 MacDonald codes of type α

A type α simplex code S_k^α is a linear code over R. Its generator matrix $\mathbf{G}_k^\alpha$ is constructed inductively. Let $\mathbf{G}_k^\alpha$ be a $k \times p^{2k}$ matrix over R, where

$$\boldsymbol{G}_k^\alpha = \left[\begin{array}{c:c:c:c} 0 \;\cdots\; 0 & 1 \;\cdots\; 1 & \cdots & (p-1)+v(p-1) \;\cdots\; (p-1)+v(p-1) \\ \hdashline \boldsymbol{G}_{k-1}^\alpha & \boldsymbol{G}_{k-1}^\alpha & \cdots & \boldsymbol{G}_{k-1}^\alpha \end{array}\right]$$

and

$$\boldsymbol{G}_1^\alpha = [0\ 1\ \cdots\ p-1\ v\ \cdots\ v(p-1)\ \cdots\ (p-1)+v\ \cdots\ (p-1)+v(p-1)].$$

Lemma 1 [23] *The torsion codes H^+ and H^- of S_k^α are permutation equivalent to each other.*

The MacDonald code of type α over the ring R can be constructed from the generator matrix $\boldsymbol{G}_k^\alpha$ of the simplex code S_k^α. For $1 \le u \le k-1$, let $\boldsymbol{G}_{k,u}^\alpha$ be the matrix obtained from $\boldsymbol{G}_k^\alpha$ by deleting columns corresponding to the columns of $\boldsymbol{G}_u^\alpha$, i.e.

$$\boldsymbol{G}_{k,u}^\alpha = \left[\boldsymbol{G}_k^\alpha \setminus \frac{\boldsymbol{0}}{\boldsymbol{G}_u^\alpha}\right] \tag{1}$$

where $[\boldsymbol{A} \setminus \boldsymbol{B}]$ denotes the matrix obtained from the matrix $\boldsymbol{A}$ by deleting the matrix $\boldsymbol{B}$, and the size of $\boldsymbol{0}$ is $(k-u) \times p^{2u}$.

Definition 1 The code $\mathcal{C}_{k,u}^\alpha$ generated by $\boldsymbol{G}_{k,u}^\alpha$ is called a type α MacDonald code.

We can see that the code $\mathcal{C}_{k,u}^\alpha$ is a linear code over the ring R of length $p^{2k} - p^{2u}$. Let $\mathcal{C}_{k,u,T}^\alpha$ be the torsion code of $\mathcal{C}_{k,u}^\alpha$. That is the generator matrix of $\mathcal{C}_{k,u,T}^\alpha$ is obtained by replacing $(1-v)$ by 1 in the matrix $(1-v)\boldsymbol{G}_{k,u}^\alpha$. Similarly, we can get another torsion code of $\mathcal{C}_{k,u}^\alpha$ by replacing v by 1 in $v\boldsymbol{G}_{k,u}^\alpha$. But, by Lemma 1, we know that the two torsion codes are equivalent to each other. Therefore we only need to consider the former case, i.e. we only study $\mathcal{C}_{k,u,T}^\alpha$, which is a $[p^{2k} - p^{2u}, k]$ code [23].

2.2 MacDonald codes of type β

The 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 $\boldsymbol{G}_k^\alpha$.

Let λ_k be a matrix of size $k \times \frac{p^{2k}-p^k}{p-1}$ over the ring R. Let $\lambda_1 = [1\ 2\ \cdots\ p-1\ v]$ and

$$\lambda_2 = \left[\begin{array}{c|c|c|c|c|c|c|c|c|c} 0 & 1 & 2 & \cdots & p-1 & v & 1+(p-1)v & 2+(p-2)v & \cdots & p-1+v \\ \hline \lambda_1 & \boldsymbol{G}_1^\alpha & \boldsymbol{G}_1^\alpha & \cdots & \boldsymbol{G}_1^\alpha & \boldsymbol{G}_1^\alpha & \lambda_1 & \lambda_1 & \cdots & \lambda_1 \end{array}\right].$$

Then λ_k is constructed inductively as follows

$$\lambda_k = \left[\begin{array}{c|c|c|c|c|c|c|c|c} 0 & 1 & \cdots & p-1 & v & 1+(p-1)v & 2+(p-2)v & \cdots & p-1+v \\ \hline \lambda_{k-1} & \boldsymbol{G}_{k-1}^\alpha & \cdots & \boldsymbol{G}_{k-1}^\alpha & \boldsymbol{G}_{k-1}^\alpha & \lambda_{k-1} & \lambda_{k-1} & \cdots & \lambda_{k-1} \end{array}\right].$$

Let δ_k be a matrix of size $k \times \frac{p^{2k}-p^k}{p-1}$ over the ring R. Let $\delta_1 = [1\ 2 \cdots p-1\ p-1+v]$ and

$$\delta_2 = \left[\begin{array}{c|c|c|c|c|c|c|c|c|c} 0 & 1 & 2 & \cdots & p-1 & p-1+v & v & 2v & \cdots & (p-1)v \\ \hline \delta_1 & \boldsymbol{G}_1^\alpha & \boldsymbol{G}_1^\alpha & \cdots & \boldsymbol{G}_1^\alpha & \boldsymbol{G}_1^\alpha & \delta_1 & \delta_1 & \cdots & \delta_1 \end{array}\right].$$

Then δ_k is constructed inductively as follows

$$\delta_k = \left[\begin{array}{c|c|c|c|c|c|c|c|c|c} 0 & 1 & 2 & \cdots & p-1 & p-1+v & v & 2v & \cdots & (p-1)v \\ \hline \delta_{k-1} & \boldsymbol{G}_{k-1}^\alpha & \boldsymbol{G}_{k-1}^\alpha & \cdots & \boldsymbol{G}_{k-1}^\alpha & \boldsymbol{G}_{k-1}^\alpha & \delta_{k-1} & \delta_{k-1} & \cdots & \delta_{k-1} \end{array}\right].$$

Let $\boldsymbol{G}_k^\beta$ be the generator matrix of S_k^β. The size of $\boldsymbol{G}_k^\beta$ is $k \times \left(\frac{p^k-1}{p-1}\right)^2$. Let $\boldsymbol{G}_1^\beta = [1]$ and

$$\boldsymbol{G}_2^\beta = \left[\begin{array}{c|c|cccccc|ccc} 1 & 0 & v & v & \cdots & v & v & p-1+v & \cdots & p-1+v & p-1+v \\ \hline \boldsymbol{G}_1^\alpha & 1 & 1 & 2 & \cdots & p-1 & p-1+v & 1 & \cdots & p-1 & v \end{array}\right].$$

Then $\boldsymbol{G}_k^\beta$ is constructed inductively as follows

$$\boldsymbol{G}_k^\beta = \left[\begin{array}{c|c|c|c} 1 & 0 & v & p-1+v \\ \hline \boldsymbol{G}_{k-1}^\alpha & \boldsymbol{G}_{k-1}^\beta & \delta_{k-1} & \lambda_{k-1} \end{array}\right].$$

Therefore we have the following result similar to Lemma 1.

Lemma 2 [23] *The torsion codes H^+, H^- of S_k^β are permutation equivalent to each other.*

We can construct type β MacDonald codes similar to the construction of type α MacDonald codes in Definition 1. For $2 \le u \le k-1$, let $\boldsymbol{G}_{k,u}^\beta$ be the matrix obtained from $\boldsymbol{G}_k^\beta$ by deleting columns corresponding to the columns of $\boldsymbol{G}_u^\beta$, i.e.

$$\boldsymbol{G}_{k,u}^\beta = \left[\boldsymbol{G}_k^\beta \setminus \frac{\boldsymbol{0}}{\boldsymbol{G}_u^\beta}\right] \tag{2}$$

where $[\boldsymbol{A} \setminus \boldsymbol{B}]$ denotes the matrix obtained from the matrix $\boldsymbol{A}$ by deleting the matrix $\boldsymbol{B}$, and the size of $\boldsymbol{0}$ is $(k-u) \times \left(\frac{p^u-1}{p-1}\right)^2$.

Definition 2 The code $\mathcal{C}^{\beta}_{k,u}$ generated by $G^{\beta}_{k,u}$ is called a type β MacDonald code.

Let $\mathcal{C}^{\beta}_{k,u,T}$ be the torsion code of $\mathcal{C}^{\beta}_{k,u}$. That is the generator matrix of $\mathcal{C}^{\beta}_{k,u,T}$ is obtained by replacing v by 1 in the matrix $v\boldsymbol{G}^{\beta}_{k,u}$. Similarly, we can get another torsion code of $\mathcal{C}^{\beta}_{k,u}$ by replacing $1-v$ by 1 in $(1-v)\boldsymbol{G}^{\beta}_{k,u}$. But, from Lemma 2, we know that the two torsion codes are equivalent to each other. So we only consider the former case, i.e., $\mathcal{C}^{\beta}_{k,u,T}$, whose dimension is k [23].

3 The complete weight enumerators of torsion codes of MacDonald codes

For the convenience, we introduce some notations which will be used throughout the paper. For a matrix $\boldsymbol{G}$, let $N_{\boldsymbol{G}}$ be the number of columns of $\boldsymbol{G}$. Specially, $N_{\boldsymbol{G}^{\alpha}_0}=1$, $N_{\boldsymbol{G}^{\beta}_0}=N_{\lambda_0}=N_{\delta_0}=0$. Let $(\boldsymbol{G})_j$ denote the jth row of the matrix $\boldsymbol{G}$, the composition of $(\boldsymbol{G})_j$ be denoted by $\mathrm{comp}((\boldsymbol{G})_j)$. Let η_j and γ_j $(j\geq 1)$be the integers $\frac{p^{j-1}-1}{p-1}$ and $\frac{p^{2j-2}-p^{j-1}}{p-1}$ respectively, where p is a prime. For any $\omega_i\in\mathbb{F}_p^*$, define the permutation map $\tau_i:\mathbb{F}_p\to\mathbb{F}_p$, with $\tau_i(a)=\omega_i\cdot a \pmod p$. Similarly, for any $\omega_i\in\mathbb{F}_p$, define the permutation map $\tau_i':\mathbb{F}_p\to\mathbb{F}_p$, with $\tau_i'(a)=\omega_i+a \pmod p$. For a vector $\mathbf{v}=(v_1,v_2,\cdots,v_n)\in\mathbb{F}_p^n$, $\mathrm{comp}(\mathbf{v})=(t_0,t_1,\cdots,t_{p-1})$, define $\tau_i'(\mathbf{v})=(\tau_i'(v_1),\tau_i'(v_2),\cdots,\tau_i'(v_n))$, $\tau_i(\mathbf{v})=(\tau_i(v_1),\tau_i(v_2),\cdots,\tau_i(v_n)$. It is clear that $\mathrm{comp}(\mathbf{v})=\mathrm{comp}(\tau_i'(\mathbf{v}))$ $(resp.\ \mathrm{comp}(\mathbf{v})=\mathrm{comp}(\tau_i(\mathbf{v})))$ if $t_0=t_1=\cdots=t_{p-1}$ $(resp.\ t_1=t_2=\cdots=t_{p-1})$.

3.1 The complete weight enumerator of $\mathcal{C}^{\alpha}_{k,u,T}$

Let $\boldsymbol{G}^{\alpha}_{k,T}$ be the matrix that is obtained by replacing $(1-v)$ by 1 in the matrix $(1-v)\boldsymbol{G}^{\alpha}_{k}$. Similarly, let $\boldsymbol{G}^{\alpha}_{k,u,T}$ be the generator matrix of $\mathcal{C}^{\alpha}_{k,u,T}$, that is, $\boldsymbol{G}^{\alpha}_{k,u,T}$ is obtained by replacing $(1-v)$ by 1 in the matrix $(1-v)\boldsymbol{G}^{\alpha}_{k,u}$. Let $\mathbf{g}^{\alpha}_i$ $(1\leq i\leq k)$ be the ith row of $\boldsymbol{G}^{\alpha}_{k,u,T}$. We give the composition of each row of $\boldsymbol{G}^{\alpha}_{k,T}$, $(\boldsymbol{G}^{\alpha}_{k,T})_i$, and $\mathbf{g}^{\alpha}_i$ in the following results.

Proposition 1 $comp((\boldsymbol{G}^{\alpha}_{k,T})_j)=z_0^{p^{2k-1}}z_1^{p^{2k-1}}\cdots z_{p-1}^{p^{2k-1}}$, $1\leq j\leq k$.

Proof The composition of the first row of $\boldsymbol{G}^{\alpha}_{k,T}$ is $z_0^{pN_{G^{\alpha}_{k-1}}}z_1^{pN_{G^{\alpha}_{k-1}}}\cdots z_{p-1}^{pN_{G^{\alpha}_{k-1}}}$. The composition of the jth row of $\boldsymbol{G}^{\alpha}_{k,T}$ equals to $(\mathrm{comp}((G^{\alpha}_{k-j+1,T})_1))^{p^{2j-2}}$. Then, we have $\mathrm{comp}((\boldsymbol{G}^{\alpha}_{k,T})_j)=z_0^{p^{2j-1}N_{G^{\alpha}_{k-j}}}z_1^{p^{2j-1}N_{G^{\alpha}_{k-j}}}\cdots z_{p-1}^{p^{2j-1}N_{G^{\alpha}_{k-j}}}$, $1\leq j\leq k$. The result is obtained as $N_{G^{\alpha}_{k-j}}=p^{2k-2j}$. □

Proposition 2 *For* $1\leq u\leq k-1$,

$$comp(\mathbf{g}^{\alpha}_j)=\begin{cases} z_0^{p^{2k-1}-p^{2u}}z_1^{p^{2k-1}}\cdots z_{p-1}^{p^{2k-1}} & if\ 1\leq j\leq k-u,\\ z_0^{p^{2k-1}-p^{2u-1}}z_1^{p^{2k-1}-p^{2u-1}}\cdots z_{p-1}^{p^{2k-1}-p^{2u-1}} & if\ k-u+1\leq j\leq k.\end{cases} \tag{3}$$

Proof For $1 \le j \le k-u$, $\mathrm{comp}(\mathbf{g}_j^\alpha) = \mathrm{comp}((\boldsymbol{G}_{k,T}^\alpha)_j) \cdot z_0^{-N_{G_u^\alpha}} = \mathrm{comp}((\boldsymbol{G}_{k,T}^\alpha)_j) \cdot z_0^{-p^{2u}}$. For $k-u+1 \le j \le k$, $\mathrm{comp}(\mathbf{g}_j^\alpha) = \mathrm{comp}((\boldsymbol{G}_{k,T}^\alpha)_j) \cdot [\mathrm{comp}((\boldsymbol{G}_{u,T}^\alpha)_{j-k+u})]^{-1}$. Then, the Eq. (3) holds immediately from Proposition 1. □

Now, we consider the composition of the vector which is a linear combination of any two rows of $\boldsymbol{G}_{k,u,T}^\alpha$.

Lemma 3 *For any* $\omega_1,\ \omega_2 \in \mathbb{F}_p^*$, *and* $1 \le i < j \le k$, *we have* $comp(\omega_1 \cdot \boldsymbol{g}_i^\alpha) = comp(\boldsymbol{g}_i^\alpha)$ *and* $comp(\omega_1 \cdot \boldsymbol{g}_i^\alpha + \omega_2 \cdot \boldsymbol{g}_j^\alpha) = comp(\boldsymbol{g}_j^\alpha)$.

Proof By Proposition 2, we know that every element of $\mathbb{F}_p^*$ appears the same time in $\mathbf{g}_j^\alpha$, where $1 \le j \le k$. Moreover, τ_1 is a permutation, so the frequency of every nonzero element in $\tau_1(\mathbf{g}_i^\alpha)$ is the same as that in $\mathbf{g}_i^\alpha$, and hence $\mathrm{comp}(\omega_1 \cdot \mathbf{g}_i^\alpha) = \mathrm{comp}(\mathbf{g}_i^\alpha)$. The i-th row of $\boldsymbol{G}_{k,T}^\alpha$ is

$$(\boldsymbol{G}_{k,T}^\alpha)_i = \underbrace{[(\boldsymbol{G}_{k-i+1,T}^\alpha)_1, (\boldsymbol{G}_{k-i+1,T}^\alpha)_1, \cdots, (\boldsymbol{G}_{k-i+1,T}^\alpha)_1]}_{p^{2i-2}}.$$

For $0 \le l \le p-1$, let

$$\boldsymbol{M}_l = \left[\begin{array}{c:c:c:c} l \quad \cdots \quad l & \cdots & l \quad \cdots \quad l \\ \hline (\boldsymbol{G}_{k-j+1,T}^\alpha)_1 & \cdots & (\boldsymbol{G}_{k-j+1,T}^\alpha)_1 \end{array}\right]_{2\times p^{2k-2i}},$$

the number of the block $(\boldsymbol{G}_{k-j+1,T}^\alpha)_1$ in $\boldsymbol{M}_l$ is $p^{2j-2i-2}$. Let

$$\boldsymbol{M} = \left[\boldsymbol{M}_0\,\boldsymbol{M}_1\,\cdots\,\boldsymbol{M}_{p-1}\ \underbrace{\boldsymbol{M}_0\,\boldsymbol{M}_0\,\cdots\,\boldsymbol{M}_0}_{p-1}\ \underbrace{\boldsymbol{M}_1\,\boldsymbol{M}_1\,\cdots\,\boldsymbol{M}_1}_{p-1}\ \cdots\ \underbrace{\boldsymbol{M}_{p-1}\,\boldsymbol{M}_{p-1}\,\cdots\,\boldsymbol{M}_{p-1}}_{p-1}\right]_{2\times p^{2k-2i+2}}.$$

We need to consider the following three cases.

Case 1: $1 \le i \le k-u$ and $2 \le j \le k-u$. Let

$$\hat{\boldsymbol{M}}_0 = \left[\begin{array}{c:c:c:c} 0 \quad \cdots \quad 0 & 0 \quad \cdots \quad 0 & \cdots & 0 \quad \cdots \quad 0 \\ \hline (\boldsymbol{G}_{k-j+1,T}^\alpha)_1 & (\boldsymbol{G}_{k-j+1,T}^\alpha)_1 & \cdots & (\boldsymbol{G}_{k-j+1,T}^\alpha)_1 \end{array}\right],$$

the size of the $\hat{\boldsymbol{M}}_0$ is $2\times(p^{2k-2i}-p^{2u})$ and the number of the block $(\boldsymbol{G}_{k-j+1,T}^\alpha)_1$ in $\hat{\boldsymbol{M}}_0$ is $p^{2j-2i-2}-1$. Let

$$\hat{\boldsymbol{M}} = \left[\hat{\boldsymbol{M}}_0\,\boldsymbol{M}_1\,\cdots\,\boldsymbol{M}_{p-1}\ \underbrace{\boldsymbol{M}_0\,\boldsymbol{M}_0\,\cdots\,\boldsymbol{M}_0}_{p-1}\ \underbrace{\boldsymbol{M}_1\,\boldsymbol{M}_1\,\cdots\,\boldsymbol{M}_1}_{p-1}\ \cdots\ \underbrace{\boldsymbol{M}_{p-1}\,\boldsymbol{M}_{p-1}\,\cdots\,\boldsymbol{M}_{p-1}}_{p-1}\right].$$

the size of $\hat{\boldsymbol{M}}$ is $2 \times (p^{2k-2i+2} - p^{2u})$. Then, we have

$$\begin{bmatrix} \mathbf{g}_i^\alpha \\ \mathbf{g}_j^\alpha \end{bmatrix} = \left[\hat{\boldsymbol{M}} \underbrace{\boldsymbol{M}\,\boldsymbol{M} \cdots \boldsymbol{M}}_{p^{2i-2}-1} \right]_{2\times(p^{2k}-p^{2u})}.$$

Case 2: $1 \le i \le k-u$ and $k-u+1 \le j \le k$. We need to change the structure of $\hat{\boldsymbol{M}}_0$. Let

$$\hat{\boldsymbol{M}}_0 = \left[\begin{array}{c:c:c} 0 \quad \cdots \quad 0 & \cdots & 0 \quad \cdots \quad 0 \\ (\boldsymbol{G}^\alpha_{k-j+1,T})_1 & \cdots & (\boldsymbol{G}^\alpha_{k-j+1,T})_1 \end{array} \right]_{2\times(p^{2k-2i}-p^{2u})},$$

the number of the block $(\boldsymbol{G}^\alpha_{k-j+1,T})_1$ in $\hat{\boldsymbol{M}}_0$ is $p^{2j-2i-2} - p^{2u-2k+2j-2}$. Then the structures of $\hat{\boldsymbol{M}}$ and $\begin{bmatrix} \mathbf{g}_i^\alpha \\ \mathbf{g}_j^\alpha \end{bmatrix}$ are the same as that in Case 1.

Case 3: $k-u+1 \le i < j \le k$. In this case, we have

$$\begin{bmatrix} \mathbf{g}_i^\alpha \\ \mathbf{g}_j^\alpha \end{bmatrix} = [\boldsymbol{M}\,\boldsymbol{M}\,\boldsymbol{M} \cdots \boldsymbol{M}]_{2\times(p^{2k}-p^{2u})},$$

the number of the block $\boldsymbol{M}$ appears $p^{2i-2} - p^{2u-2k+2i-2}$ times.

Every element in $\mathbb{F}_p$ appears the same number of times in $(\boldsymbol{G}^\alpha_{k-j+1,T})_1$, and τ, τ' are permutation maps. So, for any $\omega_1, \omega_2 \in \mathbb{F}_p^*$, we have

$$\begin{aligned} \mathrm{comp}(\tau'_{\tau_{\omega_1}(l)}(\tau_{\omega_2}((\boldsymbol{G}^\alpha_{k-j+1,T})_1))) &= \mathrm{comp}(\tau'_{\omega}(\tau_{\omega_2}((\boldsymbol{G}^\alpha_{k-j+1,T})_1))) \\ &= \mathrm{comp}(\tau_{\omega_2}((\boldsymbol{G}^\alpha_{k-j+1,T})_1)) \\ &= \mathrm{comp}((\boldsymbol{G}^\alpha_{k-j+1,T})_1), \end{aligned}$$

where $\omega = \omega_1 \cdot l (\mathrm{mod}\ p)$, $0 \le l \le p-1$. Hence, $\mathrm{comp}(\omega_1 \cdot (\boldsymbol{M}_l)_1 + \omega_2 \cdot (\boldsymbol{M}_l)_2) = \mathrm{comp}((\boldsymbol{M}_l)_2)$, for any $0 \le l \le p-1$. Moreover, for the $\hat{\boldsymbol{M}}_0$ in the above Case 1 and Case 2, we have $\mathrm{comp}(\omega_1 \cdot (\hat{\boldsymbol{M}}_0)_1 + \omega_2 \cdot (\hat{\boldsymbol{M}}_0)_2) = \mathrm{comp}(\omega_2 \cdot (\hat{\boldsymbol{M}}_0)_2) = \mathrm{comp}((\hat{\boldsymbol{M}}_0)_2)$. Until now, we have proved that $\mathrm{comp}(\omega_1 \cdot (\boldsymbol{M})_1 + \omega_2 \cdot (\boldsymbol{M})_2) = \mathrm{comp}((\boldsymbol{M})_2)$ and $\mathrm{comp}(\omega_1 \cdot (\hat{\boldsymbol{M}})_1 + \omega_2 \cdot (\hat{\boldsymbol{M}})_2) = \mathrm{comp}((\hat{\boldsymbol{M}})_2)$. Then, from the structure of $\begin{bmatrix} \mathbf{g}_i^\alpha \\ \mathbf{g}_j^\alpha \end{bmatrix}$ in the aforementioned three cases, we have $\mathrm{comp}(\omega_1 \cdot \mathbf{g}_i^\alpha + \omega_2 \cdot \mathbf{g}_j^\alpha) = \mathrm{comp}(\mathbf{g}_j^\alpha)$. □

We give the complete weight enumerator of $\mathcal{C}^\alpha_{k,u,T}$, $1 \le u \le k-1$, in the following result.

Theorem 1 *Let $1 \le u \le k-1$. The complete weight enumerator of the torsion code $\mathcal{C}^\alpha_{k,u,T}$ is given by*

$$\begin{aligned} W_{\mathcal{C}^\alpha_{k,u,T}}(z_0, z_1, \cdots, z_{p-1}) = {} & z_0^{p^{2k}-p^{2u}} + (p^{k-u}-1) z_0^{p^{2k-1}-p^{2u}} z_1^{p^{2k-1}} z_2^{p^{2k-1}} \cdots z_{p-1}^{p^{2k-1}} \\ & + (p^k - p^{k-u}) z_0^{p^{2k-1}-p^{2u-1}} z_1^{p^{2k-1}-p^{2u-1}} z_2^{p^{2k-1}-p^{2u-1}} \\ & \cdots z_{p-1}^{p^{2k-1}-p^{2u-1}}. \end{aligned}$$

Proof For any $\boldsymbol{u} = (u_1, u_2, \cdots, u_k) \in \mathbb{F}_p^k$, let $i_{\boldsymbol{u}} = max\{i : u_i \ne 0,\ 1 \le i \le k\}$. From Lemma 3, we have $\mathrm{comp}(\boldsymbol{u} \cdot \boldsymbol{G}^\alpha_{k,u,T}) = \mathrm{comp}(\mathbf{g}^\alpha_{i_{\boldsymbol{u}}})$. So, the number of codewords whose

composition equals to comp($\mathbf{g}_i^{\alpha}$) is $p^{i-1}(p-1)$. Then, according to Proposition 2, we get the complete weight enumerator of $\boldsymbol{G}_{k,u,T}^{\alpha}$ as follows

$$\begin{aligned} W_{\mathcal{C}_{k,u,T}^{\alpha}}(z_0, z_1, \cdots, z_{p-1}) &= z_0^{p^{2k}-p^{2u}} + \sum_{i=1}^{k-u} p^{i-1}(p-1)\mathrm{comp}(\mathbf{g}_1^{\alpha}) \\ &\quad + \sum_{i=k-u+1}^{k} p^{i-1}(p-1)\mathrm{comp}(\mathbf{g}_{k-u+1}^{\alpha}) \\ &= z_0^{p^{2k}-p^{2u}} + (p^{k-u}-1)z_0^{p^{2k-1}-p^{2u}} z_1^{p^{2k-1}} z_2^{p^{2k-1}} \cdots z_{p-1}^{p^{2k-1}} \\ &\quad + (p^k - p^{k-u}) z_0^{t_0} z_1^{t_0} z_2^{t_0} \cdots z_{p-1}^{t_0}, \end{aligned}$$

where $t_0 = p^{2k-1} - p^{2u-1}$. □

Let $z_0 = 1, z_1 = z_2 = \cdots z_{p-1} = z$. Then we get the Hamming weight distribution of $\mathcal{C}_{k,u,T}^{\alpha}$, which is consistent with that in [23].

Example 1 Let $p = 3,\ k = 3,\ u = 1$. Then from Theorem 1, we have the complete weight enumerator of $\mathcal{C}_{3,1,T}^{\alpha}$ as follows

$$W_{\mathcal{C}_{3,1,T}^{\alpha}} = z_0^{720} + 8z_0^{234}z_1^{243}z_2^{243} + 18z_0^{240}z_1^{240}z_2^{240}.$$

For $u = 2$, the complete weight enumerator of $\mathcal{C}_{3,2,T}^{\alpha}$ is

$$W_{\mathcal{C}_{3,2,T}^{\alpha}} = z_0^{648} + 2z_0^{162}z_1^{243}z_2^{243} + 24z_0^{216}z_1^{216}z_2^{216}.$$

Both of the two results are consistent with numerical computation by the Magma Computational Algebra System [4].

3.2 The complete weight enumerators of $\mathcal{C}_{k,u,T}^{\beta}$

Let $\hat{\boldsymbol{G}}_{k,T}^{\alpha}$ be the matrix that is obtained by replacing v by 1 in the matrix $v\boldsymbol{G}_k^{\alpha}$. Similarly, let $\boldsymbol{G}_{k,u,T}^{\beta}$ be the generator matrix of $\mathcal{C}_{k,u,T}^{\beta}$, that is, $\boldsymbol{G}_{k,u,T}^{\beta}$ is obtained by replacing v by 1 in the matrix $v\boldsymbol{G}_{k,u}^{\beta}$. Let $\boldsymbol{G}_{k,T}^{\beta}(resp.\ \lambda_{k,T}, \delta_{k,T})$ denote the matrix which is obtained by replacing v by 1 in the matrix $v\boldsymbol{G}_k^{\beta}(v\lambda_k, v\delta_k)$. Let $\mathbf{g}_i^{\beta}$ $(1 \le i \le k)$ be the ith row of $\boldsymbol{G}_{k,u,T}^{\beta}$. For these matrices, we give the composition of their rows first.

Proposition 3 *For $k \ge 1$, we have*

$$\begin{aligned} comp((\hat{\boldsymbol{G}}_{k,T}^{\alpha})_1) &= z_0^{p^{2k-1}} z_1^{p^{2k-1}} \cdots z_{p-1}^{p^{2k-1}}, \\ comp((\lambda_{k,T})_1) &= z_0^{\frac{p^{2k-1}-p^k}{p-1}} z_1^{2p^{2k-2}} z_2^{p^{2k-2}} \cdots z_{p-1}^{p^{2k-2}}, \\ comp((\delta_{k,T})_1) &= z_0^{\frac{p^{2k-1}-p^{k-1}}{p-1}} \cdots z_{p-1}^{\frac{p^{2k-1}-p^{k-1}}{p-1}}, \\ comp((\boldsymbol{G}_{k,T}^{\beta})_1) &= z_0^{N_{\boldsymbol{G}_{k-1}^{\beta}} + N_{\lambda_{k-1}}} z_1^{\frac{p^{2k-1}-p^{k-1}}{p-1}}. \end{aligned}$$

For $1 \le j \le k$, *we have*

$$\begin{aligned}
comp((\hat{\boldsymbol{G}}^{\alpha}_{k,T})_j) = &\quad (comp(\hat{\boldsymbol{G}}^{\alpha}_{k-j+1,T})_1)^{p^{2j-2}},\\
comp((\boldsymbol{G}^{\beta}_{k,T})_j) = &\quad comp((\boldsymbol{G}^{\alpha}_{k-j+1,T})_1)^{N_{\boldsymbol{G}^{\beta}_{j-1}}} \cdot comp((\delta_{k-j+1,T})_1)^{\eta_j}\\
&\cdot comp((\lambda_{k-j+1,T})_1)^{\eta_j} \cdot comp((\boldsymbol{G}^{\beta}_{k-j+1,T})_1),\\
comp((\lambda_{k,T})_j) = &\ (comp(\lambda_{k-j+1,T})_1)^{p^{j-1}} \cdot (comp(\hat{\boldsymbol{G}}^{\alpha}_{k-j+1,T})_1)^{N_{\lambda_{j-1}}},\\
comp((\delta_{k,T})_j) = &\ (comp(\delta_{k-j+1,T})_1)^{p^{j-1}} \cdot (comp(\hat{\boldsymbol{G}}^{\alpha}_{k-j+1,T})_1)^{N_{\delta_{j-1}}}.
\end{aligned}$$

Proof Here, we only give the calculation of the composition of $(\boldsymbol{G}^{\beta}_{k,T})_j$, as the others are easy to verify. Here, we only give the calculation of the composition of $(\boldsymbol{G}^{\beta}_{k,T})_j$, as the others are easy to verify.

$$\begin{aligned}
&\mathrm{comp}((\boldsymbol{G}^{\beta}_{k,T})_j) = \mathrm{comp}((\hat{\boldsymbol{G}}^{\alpha}_{k-1,T})_{j-1}) \cdot \mathrm{comp}((\delta_{k-1,T})_{j-1}) \cdot \mathrm{comp}((\lambda_{k-1,T})_{j-1}) \cdot \mathrm{comp}((\boldsymbol{G}^{\beta}_{k-1,T})_{j-1})\\
=\ &\mathrm{comp}((\hat{\boldsymbol{G}}^{\alpha}_{k-1,T})_{j-1}) \cdot \mathrm{comp}((\delta_{k-1,T})_{j-1}) \cdot \mathrm{comp}((\lambda_{k-1,T})_{j-1})\\
&\cdot \mathrm{comp}((\hat{\boldsymbol{G}}^{\alpha}_{k-2,T})_{j-2}) \cdot \mathrm{comp}((\delta_{k-2,T})_{j-2}) \cdot \mathrm{comp}((\lambda_{k-2,T})_{j-2}) \cdot \mathrm{comp}((\boldsymbol{G}^{\beta}_{k-2,T})_{j-2})\\
&\vdots\\
=\ &\prod_{i=1}^{j-1} \mathrm{comp}((\hat{\boldsymbol{G}}^{\alpha}_{k-j+i,T})_i) \cdot \prod_{i=1}^{j-1} \mathrm{comp}((\delta_{k-j+i,T})_i) \cdot \prod_{i=1}^{j-1} \mathrm{comp}((\lambda_{k-j+i,T})_i) \cdot \mathrm{comp}((\boldsymbol{G}^{\beta}_{k-j+1,T})_1)\\
=\ &\mathrm{comp}((\hat{\boldsymbol{G}}^{\alpha}_{k-j+1,T})_1)^{\sum_{t=0}^{j-2} p^{2t}} \cdot \mathrm{comp}((\delta_{k-j+1,T})_1)^{\sum_{t=0}^{j-2} p^t} \cdot \mathrm{comp}((\hat{\boldsymbol{G}}^{\alpha}_{k-j+1,T})_1)^{\sum_{l=2}^{j-1}\sum_{t=l-1}^{2l-3} p^t}\\
&\cdot \mathrm{comp}((\lambda_{k-j+1,T})_1)^{\sum_{t=0}^{j-2} p^t} \cdot \mathrm{comp}((\hat{\boldsymbol{G}}^{\alpha}_{k-j+1,T})_1)^{\sum_{l=2}^{j-1}\sum_{t=l-1}^{2l-3} p^t} \cdot \mathrm{comp}((\boldsymbol{G}^{\beta}_{k-j+1,T})_1).\\
=\ &\mathrm{comp}((\hat{\boldsymbol{G}}^{\alpha}_{k-j+1,T})_1)^{\sum_{t=0}^{j-2} p^{2t} + 2\sum_{l=2}^{j-1}\sum_{t=l-1}^{2l-3} p^t} \cdot \mathrm{comp}((\delta_{k-j+1,T})_1)^{\eta_j}\\
&\cdot \mathrm{comp}((\lambda_{k-j+1,T})_1)^{\eta_j} \cdot \mathrm{comp}((\boldsymbol{G}^{\beta}_{k-j+1,T})_1).\\
=\ &\mathrm{comp}((\hat{\boldsymbol{G}}^{\alpha}_{k-j+1,T})_1)^{N_{\boldsymbol{G}^{\beta}_{j-1}}} \cdot \mathrm{comp}((\delta_{k-j+1,T})_1)^{\eta_j} \cdot \mathrm{comp}((\lambda_{k-j+1,T})_1)^{\eta_j} \cdot \mathrm{comp}((\boldsymbol{G}^{\beta}_{k-j+1,T})_1).
\end{aligned}$$

In the last equality we use the equation $\sum_{t=0}^{j-2} p^{2t} + 2\sum_{l=2}^{j-1}\sum_{t=l-1}^{2l-3} p^t = N_{\boldsymbol{G}^{\beta}_{j-1}}$. □

We give the composition of $\mathbf{g}^{\beta}_j$, $1 \le j \le k$, in the following result.

Proposition 4 *For* $k \ge 1$, $1 \le u \le k-1$,

$$comp(\boldsymbol{g}^{\beta}_1) = z_0^{N_{G^{\beta}_{k-1}} - N_{G^{\beta}_u} + N_{\lambda_{k-1}}} z_1^{N_{G^{\alpha}_{k-1}} + N_{\delta_{k-1}}}.$$

If $2 \le j \le k-u$,

$$\begin{aligned}
comp(\boldsymbol{g}^{\beta}_j) = &\ z_0^{\eta_{k+1}\eta_k - N_{\boldsymbol{G}^{\beta}_u}} z_1^{p^{k-j}(\eta_{k+j-1} + \eta_j\eta_k + p^{k-j}(\eta_j+1))}\\
&z_2^{\eta_k(\eta_k - \eta_{k-j+1}) + p^{2k-2j}\eta_{2j-1}} \cdots z_{p-1}^{\eta_k(\eta_k - \eta_{k-j+1}) + p^{2k-2j}\eta_{2j-1}},
\end{aligned}$$

and if $k-u+1 \le j \le k$,

$$\begin{aligned} comp(\mathbf{g}_j^{\beta}) \;=\; & z_0^{\eta_{k+1}\eta_k-\eta_{u+1}\eta_u} z_1^{p^{k-j}(\eta_{k+j-1}+\eta_j\eta_k-\eta_{2u+j-k-1}-\eta_{j-k+u}\eta_u+p^{k-j}(\eta_j-\eta_{j-k+u}))} \\ & z_2^{\eta_k(\eta_k-\eta_{k-j+1})-\eta_u(\eta_u-\eta_{k-j+1})+p^{2k-2j}(\eta_{2j-1}-\eta_{2j-2k+2u-1})} \cdots \\ & z_{p-1}^{\eta_k(\eta_k-\eta_{k-j+1})-\eta_u(\eta_u-\eta_{k-j+1})+p^{2k-2j}(\eta_{2j-1}-\eta_{2j-2k+2u-1})}. \end{aligned}$$

Proof The composition of $\mathbf{g}_1^{\beta}$ can be calculated directly from the structure of $\boldsymbol{G}_{k,u,T}^{\beta}$. For $2 \le j \le k-u$,

$$\begin{aligned} & \mathrm{comp}(\mathbf{g}_j^{\beta}) = \mathrm{comp}((\boldsymbol{G}_{k,T}^{\beta})_j) \cdot z_0^{-N_{\boldsymbol{G}_u^{\beta}}} \\ = \;& \mathrm{comp}((\hat{\boldsymbol{G}}_{k-j+1,T}^{\alpha})_1)^{N_{\boldsymbol{G}_{j-1}^{\beta}}} \cdot \mathrm{comp}((\delta_{k-j+1,T})_1)^{\eta_j} \cdot \mathrm{comp}((\lambda_{k-j+1,T})_1)^{\eta_j} \cdot \mathrm{comp}((\boldsymbol{G}_{k-j+1,T}^{\beta})_1) \cdot z_0^{-N_{\boldsymbol{G}_u^{\beta}}} \\ = \;& \left(z_0^{pN_{\boldsymbol{G}_{k-j,T}^{\alpha}}} z_1^{pN_{\boldsymbol{G}_{k-j,T}^{\alpha}}} \cdots z_{p-1}^{pN_{\boldsymbol{G}_{k-j,T}^{\alpha}}} \right)^{N_{\boldsymbol{G}_{j-1}^{\beta}}} \cdot \left(z_0^{N_{\delta_{k-j}}+N_{\boldsymbol{G}_{k-j}^{\alpha}}} z_1^{N_{\delta_{k-j}}+N_{\boldsymbol{G}_{k-j}^{\alpha}}} \cdots z_{p-1}^{N_{\delta_{k-j}}+N_{\boldsymbol{G}_{k-j}^{\alpha}}} \right)^{\eta_j} \\ & \cdot \left(z_0^{pN_{\lambda_{k-j}}} z_1^{2N_{\boldsymbol{G}_{k-j}^{\alpha}}} z_2^{N_{\boldsymbol{G}_{k-j}^{\alpha}}} \cdots z_{p-1}^{N_{\boldsymbol{G}_{k-j}^{\alpha}}} \right)^{\eta_j} \cdot \left(z_0^{N_{\boldsymbol{G}_{k-j}^{\beta}}+N_{\lambda_{k-j}}} z_1^{N_{\boldsymbol{G}_{k-j}^{\alpha}}+N_{\delta_{k-j}}} \right) \cdot z_0^{-N_{\boldsymbol{G}_u^{\beta}}} \\ = \;& z_0^{\eta_{k+1}\eta_k-N_{\boldsymbol{G}_u^{\beta}}} z_1^{p^{k-j}(\eta_{k+j-1}+\eta_j\eta_k+p^{k-j}(\eta_j+1))} z_2^{\eta_k(\eta_k-\eta_{k-j+1})+p^{2k-2j}\eta_{2j-1}} \\ & \cdots z_{p-1}^{\eta_k(\eta_k-\eta_{k-j+1})+p^{2k-2j}\eta_{2j-1}}. \end{aligned}$$

If $k-u+1 \le j \le k$, we can calculate the composition of $\mathbf{g}_j^{\beta}$ in the same way, and we have

$$\begin{aligned} \mathrm{comp}(\mathbf{g}_j^{\beta}) \;=\; & \mathrm{comp}((\boldsymbol{G}_{k,T}^{\beta})_j) \cdot \left(\mathrm{comp}((G_{u,T}^{\beta})_{j-k+u}) \right)^{-1} \\ =\; & \mathrm{comp}((\hat{\boldsymbol{G}}_{k-j+1,T}^{\alpha})_1)^{N_{\boldsymbol{G}_{j-1}^{\beta}}} \cdot \mathrm{comp}((\delta_{k-j+1,T})_1)^{\eta_j} \cdot \mathrm{comp}((\lambda_{k-j+1,T})_1)^{\eta_j} \\ & \cdot \mathrm{comp}((\boldsymbol{G}_{k-j+1,T}^{\beta})_1) \cdot \left(\mathrm{comp}((G_{u,T}^{\beta})_{j-k+u}) \right)^{-1} \\ & \vdots \\ =\; & z_0^{\eta_{k+1}\eta_k-\eta_{u+1}\eta_u} z_1^{p^{k-j}(\eta_{k+j-1}+\eta_j\eta_k-\eta_{2u+j-k-1}-\eta_{j-k+u}\eta_u+p^{k-j}(\eta_j-\eta_{j-k+u}))} \\ & z_2^{\eta_k(\eta_k-\eta_{k-j+1})-\eta_u(\eta_u-\eta_{k-j+1})+p^{2k-2j}(\eta_{2j-1}-\eta_{2j-2k+2u-1})} \cdots \\ & z_{p-1}^{\eta_k(\eta_k-\eta_{k-j+1})-\eta_u(\eta_u-\eta_{k-j+1})+p^{2k-2j}(\eta_{2j-1}-\eta_{2j-2k+2u-1})}. \end{aligned}$$

□

For $0 \le i, j \le p-1$ and $\boldsymbol{v} \in \mathbb{F}_p^n$, suppose that the composition of $\boldsymbol{v}$ is $z_0^{t_0} z_1^{t_1} \cdots z_{p-1}^{t_{p-1}}$. We define the map $f_{(i \leftrightarrow j)}$ by $f_{(i \leftrightarrow j)}(\mathrm{comp}(\boldsymbol{v})) = z_0^{t_0} z_1^{t_1} \cdots z_{i-1}^{t_{i-1}} z_i^{t_j} z_{i+1}^{t_{i+1}} \cdots z_{j-1}^{t_{j-1}} z_j^{t_i} z_{j+1}^{t_{j+1}} \cdots z_{p-1}^{t_{p-1}}$. The map $f_{(i \leftrightarrow j)}$ exchanges the power of z_i and the power of z_j in the composition of $\boldsymbol{v}$. Before we give the complete enumerator of $\boldsymbol{G}_{k,u,T}^{\beta}$, we need the following results.

We first study the composition of $\omega_1 \cdot \mathbf{v}$, where $\omega_1 \in \mathbb{F}_p^*$, $\mathbf{v}$ is a row vector of $\hat{\boldsymbol{G}}_{k,T}^{\alpha}(resp.\ \lambda_{k,T},\ \delta_{k,T}, \boldsymbol{G}_{k,T}^{\beta})$.

Lemma 4 *For any $1 \le i \le k$ and $\omega_1 \in \mathbb{F}_p^*$, we have*

$$\begin{aligned} comp(\omega_1(\hat{\boldsymbol{G}}_{k,T}^{\alpha})_i) &= comp((\hat{\boldsymbol{G}}_{k,T}^{\alpha})_i), \\ comp(\omega_1(\delta_{k,T})_i)) &= comp((\delta_{k,T})_i), \\ comp(\omega_1(\lambda_{k,T})_i)) &= f_{(1\leftrightarrow\omega_1)}(comp((\lambda_{k,T})_i)), \\ comp(\omega_1(\boldsymbol{G}_{k,T}^{\beta})_i) &= f_{(1\leftrightarrow\omega_1)}(comp((\boldsymbol{G}_{k,T}^{\beta})_i)). \end{aligned}$$

Proof It is easy to verify that every element of $\mathbb{F}_p$ appears the same number of times in $(\hat{\boldsymbol{G}}_{k,T}^{\alpha})_i$ and $(\delta_{k-1,T})_i$. Since τ_1 is a permutation on $\mathbb{F}_p^*$, then we have $\mathrm{comp}(\omega_1(\hat{\boldsymbol{G}}_{k,T}^{\alpha})_i) = \mathrm{comp}((\hat{\boldsymbol{G}}_{k,T}^{\alpha})_i)$ and $\mathrm{comp}(\omega_1(\delta_{k-1,T})_i)) = \mathrm{comp}((\delta_{k-1,T})_i)$.

We prove the other two equalities by induction. Clearly, for $k = 1$ and $i = 1$, $\mathrm{comp}(\omega_1(\lambda_{1,T})_1) = f_{(1\leftrightarrow\omega_1)}(\mathrm{comp}((\lambda_{1,T})_1))$ holds. Suppose that $\mathrm{comp}(\omega_1(\lambda_{k-1,T})_i) = f_{(1\leftrightarrow\omega_1)}(\mathrm{comp}((\lambda_{k-1,T})_i))$ for $1 \le i \le k-1$. Then, for $1 \le i \le k$, we have

$$\begin{aligned} \mathrm{comp}(\omega_1(\lambda_{k,T})_i) &= \left(\mathrm{comp}(\omega_1(\lambda_{k-1,T})_{i-1})\right)^p \cdot \left(\mathrm{comp}(\omega_1(\hat{\boldsymbol{G}}_{k-1,T}^{\alpha})_{i-1})\right)^p \\ &= \left(f_{(1\leftrightarrow\omega_1)}(\mathrm{comp}((\lambda_{k-1,T})_{i-1}))\right)^p \cdot \left(\mathrm{comp}((\hat{\boldsymbol{G}}_{k-1,T}^{\alpha})_{i-1})\right)^p \\ &= f_{(1\leftrightarrow\omega_1)}\left((\mathrm{comp}((\lambda_{k-1,T})_{i-1}))^p \cdot \mathrm{comp}((\hat{\boldsymbol{G}}_{k-1,T}^{\alpha})_{i-1})^p\right) \\ &= f_{(1\leftrightarrow\omega_1)}((\mathrm{comp}((\lambda_{k,T})_i))). \end{aligned}$$

Similarly, we can also prove the last equality by induction. For $k = i = 1$, the result is obvious. Suppose that $\mathrm{comp}(\omega_1(\boldsymbol{G}_{k-1,T}^{\beta})_i) = f_{(1\leftrightarrow\omega_1)}(\mathrm{comp}((\boldsymbol{G}_{k-1,T}^{\beta})_i))$ for $1 \le i \le k-1$. Then, for $1 \le i \le k$, we have

$$\begin{aligned} &\mathrm{comp}(\omega_1(\boldsymbol{G}_{k,T}^{\beta})_i) = \left(\mathrm{comp}(\omega_1(\hat{\boldsymbol{G}}_{k-1,T}^{\alpha})_{i-1})\right) \cdot \left(\mathrm{comp}(\omega_1(\boldsymbol{G}_{k-1,T}^{\beta})_{i-1})\right) \cdot \left(\mathrm{comp}(\omega_1(\delta_{k-1,T})_{i-1})\right) \\ &\quad \cdot \left(\mathrm{comp}(\omega_1(\lambda_{k-1,T})_{i-1})\right) \\ &= \left(\mathrm{comp}((\hat{\boldsymbol{G}}_{k-1,T}^{\alpha})_{i-1})\right) \cdot \left(f_{(1\leftrightarrow\omega_1)}(\mathrm{comp}((\boldsymbol{G}_{k-1,T}^{\beta})_{i-1}))\right) \cdot \left(\mathrm{comp}((\delta_{k-1,T})_{i-1})\right) \\ &\quad \cdot \left(f_{(1\leftrightarrow\omega_1)}(\mathrm{comp}((\lambda_{k-1,T})_{i-1}))\right) \\ &= f_{(1\leftrightarrow\omega_1)}\left(\mathrm{comp}((\hat{\boldsymbol{G}}_{k-1,T}^{\alpha})_{i-1}) \cdot \mathrm{comp}((\boldsymbol{G}_{k-1,T}^{\beta})_{i-1}) \cdot \mathrm{comp}((\delta_{k-1,T})_{i-1}) \cdot \mathrm{comp}((\lambda_{k-1,T})_{i-1})\right). \\ &= f_{(1\leftrightarrow\omega_1)}\left(\mathrm{comp}((\boldsymbol{G}_{k,T}^{\beta})_i)\right). \end{aligned}$$

□

Now, we investigate the composition of the vector which is a linear combination of any two rows in $\hat{\boldsymbol{G}}_{k,T}^{\alpha}(resp.\ \lambda_{k,T},\ \delta_{k,T}, \boldsymbol{G}_{k,T}^{\beta})$.

Lemma 5 *For any $1 \le i < j \le k$, and $\omega_1, \omega_2 \in \mathbb{F}_p^*$, we have*

$$comp(\omega_1(\hat{\boldsymbol{G}}_{k,T}^{\alpha})_i + \omega_2(\hat{\boldsymbol{G}}_{k,T}^{\alpha})_j) = comp((\hat{\boldsymbol{G}}_{k,T}^{\alpha})_j), \tag{4}$$

$$comp(\omega_1(\delta_{k,T})_i + \omega_2(\delta_{k,T})_j) = comp((\delta_{k,T})_j), \tag{5}$$

$$comp(\omega_1(\lambda_{k,T})_i + \omega_2(\lambda_{k,T})_j) = f_{(1\leftrightarrow\omega_2)}(comp((\lambda_{k,T})_j)), \tag{6}$$

$$comp(\omega_1(\boldsymbol{G}^{\beta}_{k,T})_i + \omega_2(\boldsymbol{G}^{\beta}_{k,T})_j) = f_{(1\leftrightarrow\omega_2)}(comp((\boldsymbol{G}^{\beta}_{k,T})_j)). \tag{7}$$

Proof The Eq. (4) can be proved by the method used in Lemma 3, since $\hat{\boldsymbol{G}}^{\alpha}_{k,T}$ has the similar structure as $\boldsymbol{G}^{\alpha}_{k,T}$. Actually, by Lemma 1, they are equivalent to each other. Hence, the Eq. (4) immediately follows from Lemma 3. Next, we will prove the rest three equations by induction. For $k = 2, i = 1, j = 2$, it is easy to see that the Eq. (5), (6) and (7) are correct. Assuming that the Eq. (5) is suitable for $1 \le i < j \le k-1$. Then, if $1 \le i < j \le k$, the composition of $\omega_1(\delta_{k,T})_i + \omega_2(\delta_{k,T})_j$ is

$$\begin{aligned}
\mathrm{comp}(\omega_1(\delta_{k,T})_i + \omega_2(\delta_{k,T})_j) &= (\mathrm{comp}(\omega_1(\delta_{k-1,T})_{i-1} + \omega_2(\delta_{k-1,T})_{j-1}))^p \\
&\quad \cdot(\mathrm{comp}(\omega_1(\hat{\boldsymbol{G}}^{\alpha}_{k-1,T})_{i-1} + \omega_2(\hat{\boldsymbol{G}}^{\alpha}_{k-1,T})_{j-1}))^p \\
&= (\mathrm{comp}(\delta_{k-1,T})_{j-1})^p \cdot (\mathrm{comp}(\boldsymbol{G}_{k-1,T^{\alpha}})_{j-1})^p \\
&= \mathrm{comp}((\delta_{k,T})_j).
\end{aligned}$$

Up to now, we have proved the Eq. (5). Similarly, assuming that the Eq. (6) is correct for $1 \le i < j \le k-1$. Then, for $1 \le i < j \le k$, we have

$$\begin{aligned}
\mathrm{comp}(\omega_1(\lambda_{k,T})_i + \omega_2(\lambda_{k,T})_j) &= (\mathrm{comp}(\omega_1(\lambda_{k-1,T})_{i-1} + \omega_2(\lambda_{k-1,T})_{j-1}))^p \\
&\quad \cdot(\mathrm{comp}(\omega_1(\hat{\boldsymbol{G}}^{\alpha}_{k-1,T})_{i-1} + \omega_2(\hat{\boldsymbol{G}}^{\alpha}_{k-1,T})_{j-1}))^p \\
&= (f_{(1\leftrightarrow\omega_2)}(\mathrm{comp}(\lambda_{k-1,T})_{j-1}))^p \cdot (\mathrm{comp}(\boldsymbol{G}_{k-1,T^{\alpha}})_{j-1})^p \\
&= f_{(1\leftrightarrow\omega_2)}\left((\mathrm{comp}(\lambda_{k-1,T})_{j-1})^p \cdot (\mathrm{comp}(\boldsymbol{G}_{k-1,T^{\alpha}})_{j-1})^p\right) \\
&= f_{(1\leftrightarrow\omega_2)}(\mathrm{comp}((\lambda_{k,T})_j)).
\end{aligned}$$

So, the Eq. (6) is correct. Lastly, for Eq. (7), assuming that it is correct when $1 \le i < j \le k-1$, then, if $1 \le i < j \le k$, we have

$$\begin{aligned}
&\mathrm{comp}(\omega_1(\boldsymbol{G}^{\beta}_{k,T})_i + \omega_2(\boldsymbol{G}^{\beta}_{k,T})_j) = \mathrm{comp}(\omega_1(\hat{\boldsymbol{G}}^{\alpha}_{k-1,T})_{i-1} + \omega_2(\hat{\boldsymbol{G}}^{\alpha}_{k-1,T})_{j-1}) \cdot \mathrm{comp}(\omega_1(\boldsymbol{G}^{\beta}_{k-1,T})_{i-1} \\
&+ \omega_2(\boldsymbol{G}^{\beta}_{k-1,T})_{j-1}) \cdot \mathrm{comp}(\omega_1(\delta_{k-1,T})_{i-1} + \omega_2(\delta_{k-1,T})_{j-1}) \cdot \mathrm{comp}(\omega_1(\lambda_{k-1,T})_{i-1} + \omega_2(\lambda_{k-1,T})_{j-1}) \\
&= \mathrm{comp}((\hat{\boldsymbol{G}}^{\alpha}_{k-1,T})_{j-1}) \cdot \left(f_{(1\leftrightarrow\omega_2)}(\mathrm{comp}((\boldsymbol{G}^{\beta}_{k-1,T})_{j-1}))\right) \cdot \mathrm{comp}((\delta_{k-1,T})_{j-1}) \\
&\quad \cdot \left(f_{(1\leftrightarrow\omega_2)}(\mathrm{comp}((\lambda_{k-1,T})_{j-1}))\right) \\
&= f_{(1\leftrightarrow\omega_2)}(\mathrm{comp}((\hat{\boldsymbol{G}}^{\alpha}_{k-1,T})_{j-1}) \cdot \mathrm{comp}((\boldsymbol{G}^{\beta}_{k-1,T})_{j-1}) \cdot \mathrm{comp}((\delta_{k-1,T})_{j-1}) \cdot \mathrm{comp}((\lambda_{k-1,T})_{j-1})) \\
&= f_{(1\leftrightarrow\omega_2)}(\mathrm{comp}((\boldsymbol{G}^{\beta}_{k,T})_j)).
\end{aligned}$$

□

Based on the above results, we can give the composition of the linear combination of $\mathbf{g}^{\beta}_i$ and $\mathbf{g}^{\beta}_j$.

Lemma 6 *For any* $1 \le i < j \le k$ *and* $\omega_1, \omega_2 \in \mathbb{F}^*_p$, *we have* $comp(\omega_1 \cdot \boldsymbol{g}^{\beta}_i) = f_{(1\leftrightarrow\omega_1)}(comp(\boldsymbol{g}^{\beta}_i))$ *and* $comp(\omega_1\boldsymbol{g}^{\beta}_i + \omega_2\boldsymbol{g}^{\beta}_j) = f_{(1\leftrightarrow\omega_2)}(comp(\boldsymbol{g}^{\beta}_j))$.

Proof When $i = 1$, it is straightforward to show that $\mathrm{comp}(\omega_1 \cdot \mathbf{g}_1^{\beta}) = f_{(1\leftrightarrow\omega_1)}(\mathrm{comp}(\mathbf{g}_1^{\beta}))$. If $2 \le i \le k-u$, by Lemma 4, then we have

$$\begin{aligned}
\mathrm{comp}(\omega_1 \cdot \mathbf{g}_i^{\beta}) &= \mathrm{comp}(\omega_1(\hat{\boldsymbol{G}}^{\alpha}_{k-1,T})_{i-1}) \cdot \mathrm{comp}(\omega_1(\boldsymbol{G}^{\beta}_{k-1,u,T})_{i-1}) \\
&\quad \cdot \mathrm{comp}(\omega_1(\delta_{k-1,T})_{j-1}) \cdot \mathrm{comp}(\omega_1(\lambda_{k-1,T})_{j-1}) \\
&= \mathrm{comp}((\hat{\boldsymbol{G}}^{\alpha}_{k-1,T})_{i-1} \cdot f_{(1\leftrightarrow\omega_1)}(\mathrm{comp}((\boldsymbol{G}^{\beta}_{k-1,T})_{i-1})) \cdot z_0^{-N_{\boldsymbol{G}_u^{\beta}}} \\
&\quad \cdot \mathrm{comp}((\delta_{k-1,T})_{j-1}) \cdot f_{(1\leftrightarrow\omega_1)}(\mathrm{comp}((\lambda_{k-1,T})_{j-1})) \\
&= f_{(1\leftrightarrow\omega_1)}(\mathrm{comp}((\boldsymbol{G}^{\beta}_{k,T})_i) \cdot z_0^{-N_{\boldsymbol{G}_u^{\beta}}}) \\
&= f_{(1\leftrightarrow\omega_1)}(\mathrm{comp}(\mathbf{g}_i^{\beta})).
\end{aligned}$$

Similarly, if $k-u+1 \le i \le k$, then we have

$$\begin{aligned}
&\mathrm{comp}(\omega_1 \cdot \mathbf{g}_i^{\beta}) = \mathrm{comp}(\omega_1(\hat{\boldsymbol{G}}^{\alpha}_{k-1,T})_{i-1}) \cdot \mathrm{comp}(\omega_1(\boldsymbol{G}^{\beta}_{k-1,u,T})_{i-1}) \\
&\cdot \mathrm{comp}(\omega_1(\delta_{k-1,T})_{j-1}) \cdot \mathrm{comp}(\omega_1(\lambda_{k-1,T})_{j-1}) \\
=\ & \mathrm{comp}((\hat{\boldsymbol{G}}^{\alpha}_{k-1,T})_{i-1} \cdot f_{(1\leftrightarrow\omega_1)}\left(\mathrm{comp}((\boldsymbol{G}^{\beta}_{k-1,T})_{i-1}) \cdot \left(\mathrm{comp}((\boldsymbol{G}^{\beta}_{u,T})_{i-k+u})\right)^{-1}\right) \\
&\cdot \mathrm{comp}((\delta_{k-1,T})_{j-1}) \cdot f_{(1\leftrightarrow\omega_1)}(\mathrm{comp}((\lambda_{k-1,T})_{j-1})) \\
=\ & f_{(1\leftrightarrow\omega_1)}\left(\mathrm{comp}((\boldsymbol{G}^{\beta}_{k,T})_i) \cdot \left(\mathrm{comp}((\boldsymbol{G}^{\beta}_{u,T})_{i-k+u})\right)^{-1}\right) \\
=\ & f_{(1\leftrightarrow\omega_1)}(\mathrm{comp}(\mathbf{g}_i^{\beta})).
\end{aligned}$$

Until now, we have proved the first part of the Lemma. For the second part, there are three cases to be considered.

Case 1: $1 \le i \le k-u$, $2 \le j \le k-u$. In this case, we have

$$\begin{aligned}
\mathrm{comp}(\omega_1\mathbf{g}_i^{\beta} + \omega_2\mathbf{g}_j^{\beta}) &= \mathrm{comp}(\omega_1(\boldsymbol{G}^{\beta}_{k,T})_i + \omega_2(\boldsymbol{G}^{\beta}_{k,T})_j) \cdot z_0^{-N_{\boldsymbol{G}_u^{\beta}}} \\
&= f_{(1\leftrightarrow\omega_2)}\left((\boldsymbol{G}^{\beta}_{k,T})_j\right) \cdot z_0^{-N_{\boldsymbol{G}_u^{\beta}}} \\
&= f_{(1\leftrightarrow\omega_2)}\left((\boldsymbol{G}^{\beta}_{k,T})_j \cdot z_0^{-N_{\boldsymbol{G}_u^{\beta}}}\right) \\
&= f_{(1\leftrightarrow\omega_2)}\left((\boldsymbol{G}^{\beta}_{k,u,T})_j\right) = f_{(1\leftrightarrow\omega_2)}(\mathrm{comp}(\mathbf{g}_j^{\beta})).
\end{aligned}$$

Case 2: $1 \le i \le k-u,\ k-u+1 \le j \le k$. In this case,

$$\begin{aligned}
\mathrm{comp}(\omega_1\mathbf{g}_i^{\beta} + \omega_2\mathbf{g}_j^{\beta}) &= \mathrm{comp}(\omega_1(\boldsymbol{G}^{\beta}_{k,T})_i + \omega_2(\boldsymbol{G}^{\beta}_{k,T})_j) \cdot \left(\mathrm{comp}(\omega_2(\boldsymbol{G}^{\beta}_{u,T})_{j-k+u})\right)^{-1} \\
&= f_{(1\leftrightarrow\omega_2)}\left((\boldsymbol{G}^{\beta}_{k,T})_j\right) \cdot \left(f_{(1\leftrightarrow\omega_2)}\left(\mathrm{comp}(\boldsymbol{G}^{\beta}_{u,T})_{j-k+u}\right)\right)^{-1} \\
&= f_{(1\leftrightarrow\omega_2)}\left((\boldsymbol{G}^{\beta}_{k,T})_j \cdot \left(\mathrm{comp}(\boldsymbol{G}^{\beta}_{u,T})_{j-k+u}\right)^{-1}\right) \\
&= f_{(1\leftrightarrow\omega_2)}\left((\boldsymbol{G}^{\beta}_{k,u,T})_j\right) = f_{(1\leftrightarrow\omega_2)}(\mathrm{comp}(\mathbf{g}_j^{\beta})).
\end{aligned}$$

Case 3: $k-u+1 \le i < j \le k$. In this case,

$$\begin{aligned}
\mathrm{comp}(\omega_1 \mathbf{g}_i^{\beta} + \omega_2 \mathbf{g}_j^{\beta}) &= \mathrm{comp}(\omega_1 (\boldsymbol{G}_{k,T}^{\beta})_i + \omega_2 (\boldsymbol{G}_{k,T}^{\beta})_j) \\
&\quad \cdot \left(\mathrm{comp}\left(\omega_1 (\boldsymbol{G}_{u,T}^{\beta})_{i-k+u} + \omega_2 (\boldsymbol{G}_{u,T}^{\beta})_{j-k+u} \right) \right)^{-1} \\
&= f_{(1 \leftrightarrow \omega_2)} \left((\boldsymbol{G}_{k,T}^{\beta})_j \right) \cdot \left(f_{(1 \leftrightarrow \omega_2)} \left(\mathrm{comp}(\boldsymbol{G}_{u,T}^{\beta})_{j-k+u} \right) \right)^{-1} \\
&= f_{(1 \leftrightarrow \omega_2)} \left((\boldsymbol{G}_{k,T}^{\beta})_j \cdot \left(\mathrm{comp}(\boldsymbol{G}_{u,T}^{\beta})_{j-k+u} \right)^{-1} \right) \\
&= f_{(1 \leftrightarrow \omega_2)} \left((\boldsymbol{G}_{k,u,T}^{\beta})_j \right) = f_{(1 \leftrightarrow \omega_2)} (\mathrm{comp}(\mathbf{g}_j^{\beta})).
\end{aligned}$$

The proof is completed.

□

Now, we can give the complete weight enumerator of $\mathcal{C}_{k,u,T}^{\beta}$.

Theorem 2 *Let $1 \le u \le k-1$. The complete weight enumerator of the torsion code $\mathcal{C}_{k,u,T}^{\beta}$ is given by*

$$W_{\mathcal{C}_{k,u,T}^{\beta}}(z_0, z_1, \cdots, z_{p-1}) = z_0^{N_{\boldsymbol{G}_{k,u}^{\beta}}} + \sum_{j=1}^{k} p^{j-1} \Gamma_j, \tag{8}$$

where $\Gamma_j = \sum_{i=1}^{p-1} f_{(1 \leftrightarrow i)}(comp(\mathbf{g}_j^{\beta}))$ and $comp(\mathbf{g}_j^{\beta})$ is the composition in Proposition 4.

Proof For any $\boldsymbol{u} = (u_1, u_2, \cdots, u_k) \in \mathbb{F}_p^k$, let $i_{\boldsymbol{u}} = max\{i : u_i \neq 0,\ 1 \le i \le k\}$. By Lemma 6, we have $\mathrm{comp}(\boldsymbol{u} \cdot \boldsymbol{G}_{k,u,T}^{\beta}) = f_{(1 \leftrightarrow u_{i_{\boldsymbol{u}}})} \mathrm{comp}(\mathbf{g}_{i_{\boldsymbol{u}}}^{\beta})$. So, the number of codewords whose composition equals to $f_{(1 \leftrightarrow \omega_i)}(\mathrm{comp}(\mathbf{g}_i^{\beta}))$ is p^{i-1}, where $1 \le \omega_i \le p-1, 1 \le i \le k$. Hence, the complete weight enumerator of $\mathcal{C}_{k,u,T}^{\beta}$ is

$$\begin{aligned}
W_{\mathcal{C}_{k,u,T}^{\beta}}(z_0, z_1, \cdots, z_{p-1}) &= z_0^{N_{\boldsymbol{G}_{k,u}^{\beta}}} + \mathrm{comp}(\mathbf{g}_1^{\beta}) + f_{(1 \leftrightarrow 2)}(\mathrm{comp}(\mathbf{g}_1^{\beta})) + \cdots \\
&\quad + f_{(1 \leftrightarrow p-1)}(\mathrm{comp}(\mathbf{g}_1^{\beta})) \\
&\quad + p \left(\mathrm{comp}(\mathbf{g}_2^{\beta}) + f_{(1 \leftrightarrow 2)}(\mathrm{comp}(\mathbf{g}_2^{\beta})) \right. \\
&\qquad \left. + \cdots + f_{(1 \leftrightarrow p-1)}(\mathrm{comp}(\mathbf{g}_2^{\beta})) \right) \\
&\quad + \cdots + p^{k-1} \left(\mathrm{comp}(\mathbf{g}_k^{\beta}) + f_{(1 \leftrightarrow 2)}(\mathrm{comp}(\mathbf{g}_k^{\beta})) \right. \\
&\qquad \left. + \cdots + f_{(1 \leftrightarrow p-1)}(\mathrm{comp}(\mathbf{g}_k^{\beta})) \right) \\
&= z_0^{N_{\boldsymbol{G}_{k,u}^{\beta}}} + \sum_{j=1}^{k} p^{j-1} \Gamma_j
\end{aligned}$$

where $\Gamma_j = \sum_{i=1}^{p-1} f_{(1\leftrightarrow i)}(\mathrm{comp}(\mathbf{g}_j^{\beta}))$. There are together pk compositions of all the p^k codewords. We can only give the complete weight enumerator of the code like Eq. (8), since the exact expansion of the $W_{\mathcal{C}_{k,u,T}^{\beta}}(z_0, z_1, \cdots, z_{p-1})$ is complex. □

Let $z_0 = 1, z_1 = \cdots = z_{p-1} = z$ in Eq. (8). Then we have $W_{\mathcal{C}_{k,u,T}^{\beta}}(z_0, z_1, \cdots, z_{p-1}) = W_{\mathcal{C}_{k,u,T}^{\beta}}(z) = 1+(p^{k-u}-1)z^{N_{\boldsymbol{G}_k^{\beta}}-\eta_{k+1}\eta_k}+(p^k-p^{k-u})z^{(N_{\boldsymbol{G}_k^{\beta}}-\eta_{k+1}\eta_k)-(N_{\boldsymbol{G}_u^{\beta}}-\eta_{u+1}\eta_u)}$, which is the Hamming weight distribution of $\mathcal{C}_{k,u,T}^{\beta}$. The result is consistent with that in [23].

Example 2 Let $p = 3, k = 3, u = 1$. By Theorem 2, we get the complete weight enumerator of $\mathcal{C}_{3,1,T}^{\beta}$ as follows

$$W_{\mathcal{C}_{3,1,T}^{\beta}}(z_0, z_1, z_2) = z_0^{168} + z_0^{51}z_1^{117} + z_0^{51}z_2^{117} + 3z_0^{51}z_1^{69}z_2^{48} + 3z_0^{51}z_1^{48}z_2^{69} + 9z_0^{52}z_1^{60}z_2^{56} + 9z_0^{52}z_1^{56}z_2^{60}.$$

For $u = 2$, by Theorem 2, we have the complete weight enumerator of $\mathcal{C}_{3,2,T}^{\beta}$ as follows

$$W_{\mathcal{C}_{3,2,T}^{\beta}}(z_0, z_1, z_2) = z_0^{153} + z_0^{36}z_1^{117} + z_0^{36}z_2^{117} + 3z_0^{48}z_1^{57}z_2^{48} + 3z_0^{48}z_1^{48}z_2^{57} + 9z_0^{48}z_1^{54}z_2^{51} + 9z_0^{48}z_1^{51}z_2^{54}.$$

These results are consistent with numerical computation by the Magma Computational Algebra System [4].

4 Authentication codes from $\mathcal{C}_{k,u,T}^{\alpha}$ and $\mathcal{C}_{k,u,T}^{\beta}$

A systematic authentication code is a four-tuple $(\mathcal{S}, \mathcal{T}, \mathcal{K}, \{E_k : k \in \mathcal{K}\})$, where $\mathcal{S}$ is the *source state space*, $\mathcal{T}$ is the *tag space*, $\mathcal{K}$ is the *key space* and $E_k : \mathcal{S} \to \mathcal{T}$ is called an *encoding rule*. We assume that the key space and source state space have a uniform probability distribution. We use P_I and P_S to denote the maximum success probabilities with respect to the *impersonation* and *substitution* attacks. The reader is referred to [8, 9, 21, 22] for more introductions to the authentication code. For the systematic authentication code, there are two lower bounds on P_I and P_S [21]: $P_I \geq \frac{1}{|\mathcal{T}|}$, and $P_S \geq \frac{1}{|\mathcal{T}|}$. In general, it is required that P_I and P_S are as small as possible. The systematic authentication code with $P_I = P_S = \frac{1}{|\mathcal{T}|}$ is called *optimal*. It is also desired that $|\mathcal{K}|$ must be as small as possible when the values P_I and P_S are fixed. In [9], a generic coding-theory construction of systematic authentication codes is presented as described below.

Let $\mathcal{C}$ be an $[n, k, d]$ linear code over $\mathbb{F}_p$. We use $\mathbf{c}_i = (c_{i,1}, c_{i,2}, \cdots, c_{i,n})$ to denote a codeword of $\mathcal{C}$, $1 \leq i \leq p^k$. Define a systematic authentication code as follows

$$(\mathcal{S}, \mathcal{T}, \mathcal{K}, \{E_k : k \in \mathcal{K}\}) = (\mathbb{Z}_{p^k}, \mathbb{F}_p, \mathbb{Z}_n \times \mathbb{F}_p, \{E_k : k \in \mathcal{K}\}), \tag{9}$$

where for any $k = (k_1, k_2) \in \mathcal{K}$ and $s \in \mathcal{S}$, $E_k(s) = c_{s,k_1} + k_2$.

Lemma 7 [9] *For the systematic authentication code of (9), we have*

$$P_I = \frac{1}{p} \text{ and } P_S = \max_{0 \neq \boldsymbol{c} \in \mathcal{C}} \max_{u \in \mathbb{F}_p} \frac{N(\boldsymbol{c}, u)}{n}$$

where $N(\mathbf{c}, u)$ denotes the number of times u occurs in the codeword $\mathbf{c}$. Futhermore, we have $|\mathcal{S}| = p^k$, $|\mathcal{T}| = p$ and $|\mathcal{K}| = np$.

We use $\overline{\mathcal{C}}^{\beta}_{k,u,T}$ to denote the code with generator matix $[\mathbf{g}_2^{\beta}, \mathbf{g}_3^{\beta}, \cdots, \mathbf{g}_k^{\beta}]^T$. Clearly, $\overline{\mathcal{C}}^{\beta}_{k,u,T}$ is a subcode of $\mathcal{C}^{\beta}_{k,u,T}$. Now, we consider the parameters of the authentication code constructed by the code $\mathcal{C}^{\alpha}_{k,u,T}$ and $\overline{\mathcal{C}}^{\beta}_{k,u,T}$ respectively. By Theorems 1 and 2 and Lemma 7, we have the following results immediately.

Theorem 3 *Let $\mathcal{C}$ be the code $\mathcal{C}^{\alpha}_{k,u,T}$, where $k \geq 2$, $1 \leq u \leq k-1$. Then for the authentication code of (9), we have*

$$P_I = \frac{1}{p} \ \text{and} \ P_S = \frac{1}{p} + \frac{1}{p^{2k-2u+1} - p}.$$

Furthermore, $|\mathcal{S}| = p^k$, $|\mathcal{T}| = p$ and $|\mathcal{K}| = p(p^{2k} - p^{2u})$.

Theorem 4 *Let $\mathcal{C}$ be the code $\overline{\mathcal{C}}^{\beta}_{k,u,T}$, where $k \geq 2$, $1 \leq u \leq k-1$. Then for the authentication code of (9), we have*

$$P_I = \frac{1}{p} \ \text{and}$$

$$P_S = \begin{cases} \frac{p^{2k-1}+3p^{2k-2}-3p^{k-1}-6p^{2k-3}+3p^{k-2}+2p^{2k-4}}{p^{2k}-2p^k-p^{2u}+2p^u} & if\ 1 \leq u \leq k-2, \\ \frac{1}{p} + \frac{p^{k-1}-2p^{k-2}+1}{p^{k+1}+p^k-2p} & if u = k-1. \end{cases}$$

Furthermore, $|\mathcal{S}| = p^{k-1}$, $|\mathcal{T}| = p$ and $|\mathcal{K}| = \frac{p(p^k-1)^2-p(p^u-1)^2}{(p-1)^2}$.

A systematic authentication code has five parameters. In many cases, it is impossible to compare two classes of authentication codes. It is difficult to say which is better when two authentication codes are not comparable. We will compare our codes in Theorems 3 and 4 with the code of Theorem 3 in [9]. Let p be an odd prime, $k = 2$ and $u = 1$. Then the code of Theorem 3 becomes

$$|\mathcal{S}| = p^2,\ |\mathcal{T}| = p,\ |\mathcal{K}| = p^5 - p^3,\ P_I = \frac{1}{p},\ P_S = \frac{1}{p} + \frac{1}{p^3 - p}.$$

If we take $m = 4$, then the code of Theorem 3 in [9] with the following parameters

$$|\mathcal{S}| = p^4,\ |\mathcal{T}| = p,\ |\mathcal{K}| = \frac{p(p^5-1)}{2},\ P_I = \frac{1}{p},\ P_S = \frac{1}{p} + \frac{p-1}{p(p^2+1)}.$$

Similarly, let $k = 2$, $u = 1$. Then the code of Theorem 4 becomes

$$|\mathcal{S}| = p,\ |\mathcal{T}| = p,\ |\mathcal{K}| = p^3 + 2p^2,\ P_I = \frac{1}{p},\ P_S = \frac{1}{p} + \frac{1}{p^2 + 2p}.$$

If we take $m = 3$, then the code of Theorem 3 in [9] with the following parameters

$$|\mathcal{S}| = p^3,\ |\mathcal{T}| = p,\ |\mathcal{K}| = \frac{p(p^3-1)}{2},\ P_I = \frac{1}{p},\ P_S = \frac{1}{p} + \frac{1}{p^{3/2} - 1}.$$

In these cases, we can see that both the key space and the P_S of our codes are smaller than that in [9]. Unfortunately, our source state space are also smaller than theirs'. However, for the device with very limited storage and power, for example, the wireless sensor network

and RFID tag, the source state space may be small. In this case, our authentication codes may be better than that in [9].

Note that the parameters of the authentication codes in Theorems 3 and 4 are new, and both of them are asymptotically optimal if p^k is large enough.

5 Conclusions

In this paper, we investigate the complete weight enumerators of the torsion codes of MacDonald codes over the finite non-chain ring $\mathbb{F}_p + v\mathbb{F}_p$. These torsion codes are linear codes over the finite field $\mathbb{F}_p$. We calculate the composition of the rows in the generator matrix first. Then, we analysis the composition of the linear combination of these rows. We give the complete weight enumerators without using exponential sums, since these torsion codes have good structures. We believe our method can be used to study other linear codes which have the similar good structures as the torsion codes in this paper. As an application, we employed these linear codes to construct authentication codes with new parameters.

Acknowledgments Part of this work was done when J. Gao was visiting the Chern Institute of Mathematics, Nankai University, Tianjin, China. J. Gao would like to thank the institution for the kind hospitality. This research is supported by the National Key Basic Research Program of China (973 Program Grant No. 2013CB834204), the National Natural Science Foundation of China (Nos. 61571243, 61171082 and 11526045), the Doctoral Research Foundation of Shandong University of Technology (No. 4041/415059) and the Innovation Research Program of Postgraduate Teaching of Shandong University of Technology (No. 4052/115017).

References

1. AL-Ashker, M., Isleem, I.: Simplex Linear Codes Over the Ring $f_2 + vf_2$. An-Najah Univ J. Res. (N. Sc.) **22**, 25–42 (2008)
2. Bae, S., Li, C., Yue, Q.: On the complete weight enumerator of some reducible cyclic codes. Discret. Math. **338**, 2275–2287 (2015)
3. Blake, I.F., Kith, K.: On the complete weight enumerator of Reed-Solomon codes. SIAM J. Discret. Math. **4**(2), 164–171 (1991)
4. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system I: The user language. J. Symb. Comp. **24**(3), 235–265 (1997)
5. Cengellenmis, Y., Al-Ashker, M.M.: MacDonald codes over the ring $\mathbb{F}_3 + v\mathbb{F}_3$. IUG Journal of Natural and Engineering Studies **20**(1), 103–112 (2012)
6. Cengellenmis, Y., Al-Ashker, M.M.: Simplex code of type beta over $\mathbb{F}_3 + v\mathbb{F}_3$. Proceedings of the Jangjeon Mathematical Society **14**(3), 277–284 (2011)
7. Dertli, A., Cengellenmis, Y.: MacDonald codes over the ring $\mathbb{F}_2 + v\mathbb{F}_2$. Int. J. Algebra. **5**(20), 985–991 (2011)
8. Ding, C., Wang, X.: A coding theory construction of new systematic authentication codes. Theor. Comput. Sci. **330**(1), 81–99 (2005)
9. Ding, C., Helleseth, T., Kløve, T., Wang, X.: A general construction of authentication codes. IEEE Trans. Inf. Theory **53**(6), 2229–2235 (2007)
10. Ding, C., Yin, J.: Algebraic constructions of constant composition codes. IEEE Trans. Inf. Theory **51**(4), 1585–1589 (2005)
11. Helleseth, T., Kholosha, A.: Monomial and quadratic bent functions over the finite fields of odd characteristic. IEEE Trans. Inf. Theory **52**(5), 2018–2032 (2006)
12. Kith, K.: Complete weight enumeration of Reed-Solomon codes. Masters Thesis, Department of Electrical and Computing Engineering, University of Waterloo, Waterloo, ON, Canada (1989)
13. Kuzmin, A.S., Nechaev, A.A.: Complete weight enumerators of generalized Kerdock code and linear recursive codes over Galois rings. In: Proceedings of the WCC99 Workshop on Coding and Cryptography, pp. 332-336, Paris, France, 11-14 January (1999)

14. Kuzmin, A.S., Nechaev, A.A.: Complete weight enumerators of generalized Kerdock code and related linear codes over Galois rings. Discret. Appl. Math. **111**, 117–137 (2001)
15. Li, C., Yue, Q., Fu, F.-W.: Complete weight enumerators of some cyclic codes. Des. Codes Cryptogr. preprint (2015)
16. Li, C., Bae, S., Ahn, J., Yang, S., Yao, Z.: Complete weight enumerators of linear codes and their applications. Des. Codes Cryptogr. preprint (2015)
17. Luo, J., Helleseth, T.: Constant composition codes as subcodes of cyclic codes. IEEE Trans. Inf. Theory **57**(11), 7482–7488 (2011)
18. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. North-Holland, Amsterdam (1977)
19. MacWilliams, F.J., Mallows, C.L., Sloane N.J.A.: Generalizations of Gleasons theorem on weight enumerators of self-dual codes. IEEE Trans. Inf. Theory **18**(6), 794–805 (1972)
20. MacDonald, J.E.: Design methods for maximum minimun-distance error-coorcting codes. IBM J. Res. Dev. **4**(1), 43–57 (1960)
21. Rees, R.S., Stinson, D.R.: Combinatorial Characterizations of Authentication Codes II. Des. Codes Cryptogr. **7**(3), 239-259 (1996)
22. Simmons, G.J.: Authentication Theory/Coding Theory. In: Advances in CryptologyCRYPTO84. Lecture Notes in Computer Science, vol. 196, pp. 411–431. Springer, Berlin (1984)
23. Wang, X., Gao, J., Fu, F.-W.: Secret sharing schemes from linear codes over $\mathbb{F}_p + v\mathbb{F}_p$. Int. J. Found. Comput. Sci to appear (2015)
24. Xiang, C., Liu, H.: The complete weight enumerator of a class of linear codes. arXiv:hep-th/1505.06502v2 (2015)
25. Yang, S., Yao, Z.: Complete weight enumerators of some linear codes. arXiv:1505.06326v2 (2015)
26. Yang, S., Yao, Z.: The complete weight enumerator of several cyclic codes. arXiv:1505.05575v2 (2015)
27. Yang, S., Yao, Z.: Complete weight enumerator of a family of linear Codes from Cyclotomy. arXiv:1507.05732v1 (2015)
28. Yang, S., Yao, Z.: Complete weight enumerators of a family of three-weight linear codes. Des. Codes Cryptogr (2016)