New code equivalence based on relative generalized Hamming weights [*]

Zihui Liu [†]

Department of Mathematics, Beijing Institute of Technology, Beijing 100081, China

Xin-Wen Wu

School of Information and Communication Technology, Griffith University

Gold Coast, QLD 4222, Australia

Wende Chen

Institute of Systems Science, Academy of Mathematics and Systems Science,

Chinese Academy of Sciences, Beijing 100080, China

Yuan Luo

Department of Computer Sciences and Engineering, Shanghai Jiao Tong University,

Shanghai 200240, China

Abstract. Code equivalence is a basic concept in coding theory. The well-known theorem by MacWilliams gives a sufficient condition for code equivalence. Recently the MacWilliams theorem has been generalized, by Fan, Liu and Puig, making use of the generalized Hamming weights (GHWs). In this paper, we will present a further generalization of the MacWilliams theorem. Our result extends both the MacWilliams theorem and the result by Fan, Liu and Puig. We will first define "relative subcodes" of a linear code, based on the relative generalized Hamming weights (RGHWs) which is a generalization of the GHWs; and then establish a method based on finite projective geometry to characterize relative subcodes. Using this method, we will prove our main result.

Key words. Code equivalence; relative generalized Hamming weight; relative projective subspaces; relative subcodes; value assignment

[*] This work was supported by the Special Training Program of BIT. The work of Y. Luo was supported in part by the National Natural Science Foundation of China (Grants No. 60972033 and 60832001), and the National Basic Research Program of China (Grant No. 2007CB310900).

[†] To whom correspondence should be addressed. Email: lzhui@bit.edu.cn

1 Introduction

Code equivalence is a basic concept in coding theory. The well-known theorem by MacWilliams [9, 10] has established a sufficient condition for code equivalence. The theorem shows that any isomorphism between two linear codes preserving the Hamming weight is an equivalence of the codes, where "isomorphism" is a one-to-one correspondence preserving linearity between two vector spaces (here linear codes are viewed as vector spaces).

Two codes which are equivalent have many common properties; for instance, they have the same weight distribution and the same support weight distribution of subcodes. In particular, equivalent codes have the same generalized Hamming weights (GHWs) [14] and the same relative generalized Hamming weights (RGHWs) [8]. In addition, there is an obvious one-to-one correspondence between the sets of the minimal codewords of equivalent codes; and thus equivalent codes can be used to construct the same secret sharing scheme [6].

Code equivalence and the MacWilliams theorem have been extensively studied. Bogart et al. [1] and Ward et al. [13] have given different proofs to the MacWilliams theorem. Wood [15, 16] has generalized the MacWilliams theorem to the Frobenius rings, and characterized the Frobenius rings by using code equivalence. Making use of the GHWs, Fan, Liu and Puig [4] have established a new code equivalence. Their result shows that any isomorphism ϕ between two k-dimensional linear codes C and C', which preserves the support weights of all t-dimensional subcodes for some t (where $0 < t < k$), is an equivalence of C and C'. As the Hamming weight of a codeword is a special case of the support weight of a t-dimensional subcode, this result obviously has generalized the MacWilliams theorem.

In the present paper, making uses of the RGHWs, we will further generalize the MacWilliams theorem. Our result extends both the MacWilliams theorem and the result in [4]. The rest of the paper is organized as follows. In Section 2, preliminary definitions and notations will be given. In Section 3, a tool for proving our main result will be established, which is based on finite projective geometry. The main result is presented in Section 4. In Section 5, the proof of the main result will be given. The concluding remarks will be given in Section 6.

2 Preliminaries

Two linear codes C and C', with the same length n over a finite field $GF(q)$, are called *equivalent*, if there exists a one-to-one correspondence, $\phi : C \to C'$, defined as

$$\phi(x_1, \cdots, x_n) = (v_1 x_{\pi(1)}, \cdots, v_n x_{\pi(n)}), \quad \forall\ (x_1, \cdots, x_n) \in C, \tag{1}$$

where π is an arbitrary permutation of $\{1, 2, \cdots, n\}$, and $v_1, \cdots, v_n$ are arbitrary fixed nonzero elements of $GF(q)$. A one-to-one correspondence defined by (1) is called a *monomial transformation.*

Obviously, a monomial transformation $\phi : C \to C'$ is an isomorphism (i.e., one-to-one correspondence preserving linearity between two vector spaces) that preserves the Hamming weight of each codeword of C. On the other hand, the well-known theorem by MacWilliams [9, 10] shows that, any isomorphism $\phi : C \to C'$ preserving the Hamming weight of each codeword of C is a monomial transformation; and thus C and C' are equivalent.

Assume that C is an $[n, k]$ linear code over $GF(q)$. For any subcode D of C, the *support* $\chi(D)$ of D is defined as the set of positions where not all the codewords of D have zero coordinates.

Definition 1. The *support weight* (also called *effective length*) $w(D)$ of D is defined as the size of $\chi(D)$, that is, $w(D) = |\chi(D)|$.

Definition 2. [14] The *generalized Hamming weights* (GHWs) of C are a group of parameters $(d_1, d_2, \cdots, d_k)$, where

$$d_r = \min\{w(D) : D \text{ is an } [n, r] \text{ subcode of } C\}, \quad 1 \leq r \leq k.$$

In particular, d_1 is the minimum distance of C, and d_k is the effective length of C.

Based on the GHW, Fan, Liu and Puig [4] have generalized the MacWilliams theorem by using the support weights of subcodes. The result in [4] says that for two k-dimensional linear codes C and C', and an integer t with $0 < t < k$, any isomorphism $\phi : C \to C'$ preserving the support weights of all t-dimensional subcodes is a monomial transformation. It is clear that the MacWilliams theorem is a special case of the result by Fan, Liu and Puig for $t = 1$.

To further generalize the MacWilliams theorem, we will need the following definitions. Let J be a subset of I $= \{1, \ldots, n\}$. Define $C_{\mathrm{J}} = \{(c_1, \ldots, c_n) \in C : c_t = 0 \text{ for } t \notin \mathrm{J}\}$. Obviously, C_{J} is a subcode of C.

Definition 3.[8] Let C is a k-dimensional linear code, and C_1 is a given k_1-dimensional subcode of C. The *relative generalized Hamming weights* (RGHWs) of C with respect to C_1 are a group of parameters $(M_1,\, M_2,\, \cdots,\, M_{k-k_1})$, where

$$M_j = \min\{|\mathrm{J}| : \dim(C_{\mathrm{J}}) - \dim((C_1)_{\mathrm{J}}) = j\}, \quad 1 \leq j \leq k - k_1.$$

Obviously, the GHWs can be retrieved from RGHWs with $C_1 = \{0\}$.

Liu et al. [7] have given an alternative definition for the RGHWs as follows:

$$M_j = \min\{w(D) : D \text{ is a } j \text{ -dimensional subcode of } C \text{ and } D \cap C_1 = \{0\}\}, \qquad 1 \leq j \leq k - k_1. \tag{2}$$

Based on (2), we are now ready to define relative subcodes.

Definition 4. A *relative* (r, θ) *subcode* of the pair (C, C_1), called an (r, θ) subcode for short, is an r-dimensional subcode D of C satisfying $\dim(D \cap C_1) = \theta$.

By Definition 4, the j-th RGHW M_j is the minimum support weight of all $(j,0)$ subcodes.

3 Finite projective geometry method

Finite projective geometry has been extensively used to study linear codes [2, 3, 5, 7, 12]. In this section, a finite projective geometry method will be introduced. The method will be used to prove our main result.

Let L be a subset of $\{1,2,\cdots,k\}$, whose elements represent the k coordinate positions of the vectors in $GF(q)^k$. Define

$$\delta_{\mathrm{L}}(i)=\begin{cases}1, & i\in \mathrm{L},\\ 0, & i\in\{1,2,\cdots,k\}\backslash \mathrm{L}. \quad (\text{that is } i\in\{1,2,\cdots,k\} \text{ but } i\notin \ \mathrm{L})\end{cases}$$

Definition 5. Assume $\boldsymbol{v}\in GF(q)^k$ and $\boldsymbol{v}=(v_1,\cdots,v_i,\cdots,v_k)$. The *projection operator* $\mathrm{P}_{\mathrm{L}}: GF(q)^k\to GF(q)^k$ is defined as

$$\mathrm{P}_{\mathrm{L}}(\boldsymbol{v})=(\delta_{\mathrm{L}}(1)v_1,\cdots,\delta_{\mathrm{L}}(i)v_i,\cdots,\delta_{\mathrm{L}}(k)v_k).$$

The operator P_{L} is extended to a subspace $U\subset GF(q)^k$ by setting

$$\mathrm{P}_{\mathrm{L}}(U)=\{\mathrm{P}_{\mathrm{L}}(\boldsymbol{v}):\boldsymbol{v}\in U\}. \tag{3}$$

Obviously, $\mathrm{P}_{\mathrm{L}}(U)$ is also a subspace of $GF(q)^k$.

Let C be an $[n,k]$ linear code. Adding a zero coordinate C, we obtain an $[n+1,k]$ code

$$C^0=\{(\boldsymbol{c}\,|\,0):\boldsymbol{c}\in C\},$$

whose subcodes have the same support weight distribution as C. So, without loss of generality, we assume that C has no zero-position from scratch; i.e., $n=d_k$, where d_k is the last GHW of C. Or equivalently, any generator matrix of C has no zero-column.

Fix a generator matrix of C, say $\boldsymbol{G}$. Since $\boldsymbol{G}$ has no zero-column, the columns of $\boldsymbol{G}$ may be considered as points in the projective space $PG(k-1,q)$. We thus obtain a *projective multiset* (or a *value assignment* [3]) which is a map m from $PG(k-1,q)$ to the set of nonnegative integers, i.e.

$$m:\ PG(k-1,q)\to\mathbb{N}=\{0,1,\cdots\}.$$

For a point $p\in PG(k-1,q)$, we call $m(p)$ the *value* (or *multiplicity*) of p. This definition is extended to $S\subset PG(k-1,q)$ by setting

$$m(S)=\sum_{p\in S}m(p).$$

$m(S)$ is called the *value* of S.

Obviously, each generator matrix $\boldsymbol{G}$ determines a value assignment m which is dependent on both C and $\boldsymbol{G}$. Hence, we sometimes denote the value assignment m by $m_{C,\boldsymbol{G}}$ (When there is no confusion, we still use m for $m_{C,\boldsymbol{G}}$ in the paper).

If U is a projective subspace and $\mathrm{P}_{\mathrm{L}}(U) \neq \{0\}$, then $\dim \mathrm{P}_{\mathrm{L}}(U) \geq 0$ (see (3)). Define $\dim \mathrm{P}_{\mathrm{L}}(U) = -1$ when $\mathrm{P}_{\mathrm{L}}(U) = \{0\}$, i.e. when $\mathrm{P}_{\mathrm{L}}(U)$ contains no projective points.

Definition 6. A *relative* (ξ, η) *projective subspace* of $PG(k-1, q)$, denoted by P_ξ^η, is a ξ-dimensional subspace P such that $\dim \mathrm{P}_{\mathrm{L}}(P) = \eta$, where $\mathrm{L} = \{1,\, 2,\, \cdots,\, k_1\}$, and $0 \leq k_1 \leq k$.

According to the definition above, $P_{k-k_1-1}^{-1}$ represents a $(k-k_1-1)$-dimensional subspace P such that $\dim \mathrm{P}_{\mathrm{L}}(P) = -1$, that is, a $(k-k_1-1)$-dimensional subspace of $PG(k-1, q)$ consists of all those points whose first k_1 coordinates are all 0.

Some other examples for P_ξ^η are as follows. P_0^{-1} represents a point in the subspace $P_{k-k_1-1}^{-1}$, whereas P_0^0 represents a point in the set $PG(k-1,q) \backslash P_{k-k_1-1}^{-1} = \{p : p \in PG(k-1,q) \text{ but } p \notin P_{k-k_1-1}^{-1}\}$.

In the proof of our main result, we will denote by $\begin{bmatrix} s \\ t \end{bmatrix}_q$ a q-ary *Gaussian binomial coefficient* [11], that is,

$$\begin{bmatrix} s \\ t \end{bmatrix}_q = \begin{cases} 1, & t = 0, \\ \dfrac{(q^s-1)(q^{s-1}-1)\ldots(q^{s-t+1}-1)}{(q^t-1)(q^{t-1}-1)\ldots(q-1)}, & t \neq 0. \end{cases}$$

4 The main result

Theorem. Assume that two k-dimensional linear codes C and C' have the same effective length. Let $\phi : C \to C' = \phi(C)$ be a vector space homomorphism, and let $C_1' = \phi(C_1)$ be the image of C_1 under ϕ for a fixed k_1-dimensional subcode $C_1 \subset C$. If there exists some r_0 satisfying $k_1 \leq r_0 \leq k-2$ such that for any $(r_0, k_1 - 1)$ subcode D of (C, C_1), $\phi(D)$ is an (r_0, k_1-1) subcode of (C', C_1') and $w(\phi(D)) = w(D)$, then C and C' are equivalent.

Remark 1. Consider a special case of the theorem, that is, $C_1 = \{0\}$. In this case, any relative subcode D of C specified in the theorem is actually a traditional r_0-dimensional subcode of C. This is exactly the result presented in [4]. Therefore, our result has extended the result in [4], and thus generalized the well-known MacWilliams theorem.

Remark 2. In fact, the homomorphism ϕ satisfying the conditions of the theorem is an isomorphism (see Section 5). Hence, if $\boldsymbol{G}$ is a generator matrix of C whose first k_1 rows generate the subcode C_1, then $\phi(\boldsymbol{G})$ is a generator matrix of C', and $C_1' = \phi(C_1)$ is generated by the first k_1 rows of $\phi(\boldsymbol{G})$, where $\phi(\boldsymbol{G})$ is the matrix whose i-th row is

$\phi(\boldsymbol{g_i})$, while $\boldsymbol{g_i}$ is the i-th row of $\boldsymbol{G}$. If D is an (r, k_1-1) subcode of (C, C_1), then $\phi(D)$ is an (r, k_1-1) subcode of (C', C_1').

In the theorem above, the assumption that C and C' have the same effective length is necessary. In fact, if $w(\phi(D)) = w(D)$ holds for any r_0-dimensional subcode D of C for some r_0 satisfying $1 \leq r_0 \leq k-1$, then C and C' have the same effective length [4]. However, the assumption that $w(\phi(D)) = w(D)$ for any (r_0, k_1-1) subcode D for some r_0 satisfying $k_1 \leq r_0 \leq k-2$, as in the theorem, is not sufficient to show that C and C' have the same effective length. An example is given below.

Example 1. Let C and C' be the binary codes with generator matrix

$$\begin{pmatrix} 1\,0\,1\,1\,1\,0\,0\,1\,1\,1\,0\,1\,1\,0 \\ 0\,1\,0\,0\,1\,1\,1\,0\,1\,1\,1\,1\,0\,1 \\ 0\,0\,0\,1\,0\,0\,1\,1\,0\,1\,1\,1\,0\,0 \\ 0\,0\,1\,0\,0\,1\,0\,1\,1\,0\,1\,1\,0\,0 \end{pmatrix}$$

and

$$\begin{pmatrix} 1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,1\,0\,1\,1\,0\,1\,1\,0\,1\,1\,0\,1\,1\,0\,1 \\ 0\,0\,0\,1\,1\,0\,1\,1\,0\,1\,1\,0\,1\,1\,0\,1\,1 \end{pmatrix},$$

respectively, and let $\phi : C \to C'$ be a linear extension of the row-to-row correspondence of these two matrixes. Then ϕ is an isomorphism. Let C_1 and $C_1' = \phi(C_1)$ be the subcodes of C and C' generated by the first two rows of their generator matrixes, respectively. Then it is not difficult to check that $w(\phi(D)) = w(D)$ for all the $(2, 1)$ subcodes D of (C, C_1), but C and C' have different effective lengths.

Remark 3. When $r_0 = k_1 - 1$ or $r_0 = k-1$, the theorem is not true. See the following two examples.

Example 2. Consider the case $r_0 = k_1 - 1$. Let C and C' be four-dimensional binary codes with generator matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

and

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix},$$

respectively, and let $\phi : C \to C'$ be a linear extension of the row-to-row correspondence of these two matrixes. Assume that C_1 is a two-dimensional subcode generated by the first two rows of the generator matrix of C, and that $C_1' = \phi(C_1)$. Then $w(\phi(D)) = w(D)$ for all $(1,1)$ subcodes D, but C and C' are not equivalent.

Example 3. Consider the case $r_0 = k-1$. Let C and C' be four-dimensional binary codes with generator matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

and

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix},$$

respectively. Let C_1 denote the two-dimensional subcode generated by the first two rows of the generator matrix of C, and let $C_1' = \phi(C_1)$. Then it is easy to verify that $w(\phi(D)) = w(D)$ for all $(3,1)$ subcodes D. However, C and C' are not equivalent.

5 Proof of the main result

In this section, we first give a number of lemmas. Using these lemmas, we then prove the theorem presented in the previous section.

5.1 Some lemmas

We assume that $\phi : C \to C'$ is an isomorphism throughout this subsection, and that $\boldsymbol{G}$ is a fixed generator matrix of C with the first k_1 rows generating the subcode C_1. Denote the image of C_1 by $C_1' = \phi(C_1)$. Let $m_{C,\boldsymbol{G}}$ and $m'_{C',\phi(\boldsymbol{G})}$ be the corresponding value assignments (denote them by m and m', respectively, for short).

Lemma 1 will give a one-to-one correspondence between the set of relative subcodes and the set of relative projective subspaces. In this way we characterize the support weights of relative subcodes by using the values of relative projective subspaces.

Lemma 1. Assume that C and C' have effective lengths n and n'. Let ϕ, C_1, C_1', $\boldsymbol{G}$, m and m' be defined as above.

(R1). ϕ is a natural one-to-one correspondence between the $(r, k_1 - 1)$ subcodes of (C, C_1) and the $(r, k_1 - 1)$ subcodes of (C', C_1').

(R2). There is a one-to-one correspondence between the $(r, k_1 - 1)$ subcodes D of (C, C_1) and the projective subspaces P^0_{k-r-1}, such that if D corresponds to P^0_{k-r-1}, then $n - w(D) = m(PG(k-1,q)) - w(D) = m(P^0_{k-r-1})$ and $n' - w(\phi(D)) = m'(PG(k-1,q)) - w(\phi(D)) = m'(P^0_{k-r-1})$.

Proof. (R1) is proven in Remark 2. We now prove (R2). According to Definition 4, we may assume that a generator matrix of an $(r, k_1 - 1)$ subcode D is $\boldsymbol{A}_{r\times k}\boldsymbol{G}$, where

$$\boldsymbol{A}_{r\times k} = \begin{pmatrix} \boldsymbol{A}_{(k_1-1)\times k_1} & \boldsymbol{0}_{(k_1-1)\times(k-k_1)} \\ \boldsymbol{A}_{(r-k_1+1)\times k_1} & \boldsymbol{A}_{(r-k_1+1)\times(k-k_1)} \end{pmatrix}$$

and $\mathrm{rank}(\boldsymbol{A}_{(k_1-1)\times k_1}) = k_1 - 1$, $\mathrm{rank}(\boldsymbol{A}_{(r-k_1+1)\times(k-k_1)}) = r - k_1 + 1$. Then a generator matrix of $\phi(D)$ is $\boldsymbol{A}_{r\times k}\phi(\boldsymbol{G})$. Let U represent the vector space orthogonal to the vector space spanned by the rows of $\boldsymbol{A}_{r\times k}$. Then $\dim(U) = k - r$. Since $\mathrm{P}_{\mathrm{L}}(U)$ for $\mathrm{L} = \{1, 2, \cdots, k_1\}$ is orthogonal to the vector space spanned by the first $k_1 - 1$ rows of $\boldsymbol{A}_{r\times k}$, we have $\dim \mathrm{P}_{\mathrm{L}}(U) \leq 1$. If $\dim \mathrm{P}_{\mathrm{L}}(U) = 0$, then a generator matrix of U is

$$\begin{pmatrix} \boldsymbol{0}_{(k-r)\times k_1} & \boldsymbol{U}_{(k-r)\times(k-k_1)} \end{pmatrix}.$$

Thus, $\boldsymbol{A}_{(r-k_1+1)\times(k-k_1)}\boldsymbol{U}^T_{(k-r)\times(k-k_1)} = \boldsymbol{0}$, where $\boldsymbol{U}^T_{(k-r)\times(k-k_1)}$ denotes the transpose of the matrix $\boldsymbol{U}_{(k-r)\times(k-k_1)}$. Therefore, $\mathrm{rank}(\boldsymbol{A}_{(r-k_1+1)\times(k-k_1)})+\mathrm{rank}(\boldsymbol{U}^T_{(k-r)\times(k-k_1)}) \leq k - k_1$. This is a contradiction to the fact that $\mathrm{rank}(\boldsymbol{A}_{(r-k_1+1)\times(k-k_1)}) + \mathrm{rank}(\boldsymbol{U}^T_{(k-r)\times(k-k_1)}) = (r - k_1 + 1) + (k - r) = k - k_1 + 1$. Thus, $\dim \mathrm{P}_{\mathrm{L}}(U) = 1$. U is exactly P^0_{k-r-1}, corresponding to the $(r, k_1 - 1)$ subcode D. □

The following Lemmas 2 and 3 give some useful properties of the values of relative projective subspaces; and Lemma 4 presents the relationship between m and m'.

Lemma 2. Assume $m(PG(k-1, q)) = m'(PG(k-1, q))$ and $m(P^{k_1-1}_{i_0}) = m'(P^{k_1-1}_{i_0})$ for any $P^{k_1-1}_{i_0}$ for some i_0 satisfying $k_1 \leq i_0 \leq k-2$. Then, $m(P^{k_1-1}_{i}) = m'(P^{k_1-1}_{i})$ for any $P^{k_1-1}_{i}$, where $k_1 - 1 \leq i \leq k - 1$.

Proof. For any fixed $P^{k_1-1}_{i_0-1}$, the number of the $P^{k_1-1}_{i_0}$ satisfying $PG(k-1, q) \supset P^{k_1-1}_{i_0} \supset P^{k_1-1}_{i_0-1}$ is equal to $\begin{bmatrix} k - i_0 \\ 1 \end{bmatrix}_q$ (see [11, pp. 698]). Thus,

$$\begin{aligned} &\left(\begin{bmatrix} k - i_0 \\ 1 \end{bmatrix}_q - 1\right) m(P^{k_1-1}_{i_0-1}) \\ = &\sum_{P^{k_1-1}_{i_0} \supset P^{k_1-1}_{i_0-1}} m(P^{k_1-1}_{i_0}) - m(PG(k-1, q)) \\ = &\sum_{P^{k_1-1}_{i_0} \supset P^{k_1-1}_{i_0-1}} m'(P^{k_1-1}_{i_0}) - m'(PG(k-1, q)) \\ = &\left(\begin{bmatrix} k - i_0 \\ 1 \end{bmatrix}_q - 1\right) m'(P^{k_1-1}_{i_0-1}). \end{aligned}$$

From $k_1 \leq i_0 \leq k - 2$, it follows that $\begin{bmatrix} k - i_0 \\ 1 \end{bmatrix}_q - 1 \neq 0$. Therefore,

$$m(P^{k_1-1}_{i_0-1}) = m'(P^{k_1-1}_{i_0-1}), \qquad \forall\ P^{k_1-1}_{i_0-1}. \tag{4}$$

Similarly, for any fixed $P^{k_1-1}_{i_0-2}$, we have

$$\begin{aligned}
&\left(\begin{bmatrix} k-i_0+1 \\ 1 \end{bmatrix}_q - 1\right) m(P^{k_1-1}_{i_0-2}) \\
&= \sum_{P^{k_1-1}_{i_0-1} \supset P^{k_1-1}_{i_0-2}} m(P^{k_1-1}_{i_0-1}) - m(PG(k-1,q)) \\
&= \sum_{P^{k_1-1}_{i_0-1} \supset P^{k_1-1}_{i_0-2}} m'(P^{k_1-1}_{i_0-1}) - m'(PG(k-1,q)), \qquad (\text{ by } (4)) \\
&= \left(\begin{bmatrix} k-i_0+1 \\ 1 \end{bmatrix}_q - 1\right) m'(P^{k_1-1}_{i_0-2}).
\end{aligned}$$

Therefore,

$$m(P^{k_1-1}_{i_0-2}) = m'(P^{k_1-1}_{i_0-2}), \qquad \forall\, P^{k_1-1}_{i_0-2}.$$

We prove the following in the similar way

$$m(P^{k_1-1}_{k_1}) = m'(P^{k_1-1}_{k_1}), \quad \forall\, P^{k_1-1}_{k_1}, \quad \text{and } m(P^{k_1-1}_{k_1-1}) = m'(P^{k_1-1}_{k_1-1}), \quad \forall\, P^{k_1-1}_{k_1-1}. \tag{5}$$

Now for any $P^{k_1-1}_i$, $k_1-1 \le i \le k-1$, there is a $P^{k_1-1}_{k_1-1}$ such that $P^{k_1-1}_{k_1-1} \subset P^{k_1-1}_i$, and the number of the $P^{k_1-1}_{k_1}$ satisfying $P^{k_1-1}_{k_1-1} \subset P^{k_1-1}_{k_1} \subset P^{k_1-1}_i$ is $\begin{bmatrix} i-k_1+1 \\ 1 \end{bmatrix}_q$. Thus, we have

$$\begin{aligned}
&m(P^{k_1-1}_i) \\
&= \sum_{P^{k_1-1}_{k_1-1} \subset P^{k_1-1}_{k_1} \subset P^{k_1-1}_i} m(P^{k_1-1}_{k_1}) - \left(\begin{bmatrix} i-k_1+1 \\ 1 \end{bmatrix}_q - 1\right) m(P^{k_1-1}_{k_1-1}) \\
&= \sum_{P^{k_1-1}_{k_1-1} \subset P^{k_1-1}_{k_1} \subset P^{k_1-1}_i} m'(P^{k_1-1}_{k_1}) - \left(\begin{bmatrix} i-k_1+1 \\ 1 \end{bmatrix}_q - 1\right) m'(P^{k_1-1}_{k_1-1}), \quad (\text{ by } (5)) \\
&= m'(P^{k_1-1}_i).
\end{aligned}$$

□

Lemma 3. Assume $m(PG(k-1,q)) = m'(PG(k-1,q))$ and $m(P^0_s) = m'(P^0_s)$ for any P^0_s and some s satisfying $1 \le s \le k-k_1-1$. Then, $m(P^t_{s+t}) = m'(P^t_{s+t})$ for any P^t_{s+t}, where $-1 \le t \le k_1-1$.

Proof. The number of the P^{-1}_{s-1} contained in the $P^{-1}_{k-k_1-1}$ is

$$X = \begin{bmatrix} k-k_1 \\ s \end{bmatrix}_q, \tag{6}$$

and the number of the P^{-1}_{s-1}, $p_0 \in P^{-1}_{s-1} \subset P^{-1}_{k-k_1-1}$, for a fixed point $p_0 \in P^{-1}_{k-k_1-1}$, is

$$Y = \begin{bmatrix} k-k_1-1 \\ s-1 \end{bmatrix}_q$$

(see [11, pp. 698]). Thus,

$$\sum_{P_{s-1}^{-1}\subset P_{k-k_1-1}^{-1}} m(P_{s-1}^{-1}) = Ym(P_{k-k_1-1}^{-1}), \quad \text{and}$$
$$\sum_{P_{s-1}^{-1}\subset P_{k-k_1-1}^{-1}} m'(P_{s-1}^{-1}) = Ym'(P_{k-k_1-1}^{-1}). \tag{7}$$

For any given $P_{s-1}^{-1} \subset P_{k-k_1-1}^{-1}$, the number of the s-dimensional projective subspaces in $PG(k-1,q)$ containing the P_{s-1}^{-1} is

$$\begin{bmatrix} k-s \\ 1 \end{bmatrix}_q,$$

and the number of the P_s^{-1}, $P_{s-1}^{-1} \subset P_s^{-1} \subset P_{k-k_1-1}^{-1}$, is

$$\begin{bmatrix} k-k_1-s \\ 1 \end{bmatrix}_q.$$

Therefore, the number of the P_s^0, $P_s^0 \supset P_{s-1}^{-1}$, is

$$Z = \begin{bmatrix} k-s \\ 1 \end{bmatrix}_q - \begin{bmatrix} k-k_1-s \\ 1 \end{bmatrix}_q.$$

For any given $P_{s-1}^{-1} \subset P_{k-k_1-1}^{-1}$, we have

$$\begin{aligned}\sum_{P_s^0\supset P_{s-1}^{-1}} m(P_s^0) &= Zm(P_{s-1}^{-1}) + m(PG(k-1,q)\backslash P_{k-k_1-1}^{-1}) \\ &= Zm(P_{s-1}^{-1}) + m(PG(k-1,q)) - m(P_{k-k_1-1}^{-1}).\end{aligned} \tag{8}$$

Similarly, we have

$$\sum_{P_s^0\supset P_{s-1}^{-1}} m'(P_s^0) = Zm'(P_{s-1}^{-1}) + m'(PG(k-1,q)) - m'(P_{k-k_1-1}^{-1}). \tag{9}$$

From (8), (9), the assumption that $m(P_s^0) = m'(P_s^0)$ for any P_s^0, and $m(PG(k-1,q) = m'(PG(k-1,q))$, we have

$$Zm(P_{s-1}^{-1}) - m(P_{k-k_1-1}^{-1}) = Zm'(P_{s-1}^{-1}) - m'(P_{k-k_1-1}^{-1}). \tag{10}$$

Note that (10) is correct for any $P_{s-1}^{-1} \subset P_{k-k_1-1}^{-1}$. Summing up both sides of (10) over all the possible P_{s-1}^{-1}, $P_{s-1}^{-1} \subset P_{k-k_1-1}^{-1}$,

$$\begin{aligned}&\sum_{P_{s-1}^{-1}\subset P_{k-k_1-1}^{-1}} (Zm(P_{s-1}^{-1}) - m(P_{k-k_1-1}^{-1})) \\ &= Z\sum_{P_{s-1}^{-1}\subset P_{k-k_1-1}^{-1}} m(P_{s-1}^{-1}) - \sum_{P_{s-1}^{-1}\subset P_{k-k_1-1}^{-1}} m(P_{k-k_1-1}^{-1}) \\ &= ZYm(P_{k-k_1-1}^{-1}) - Xm(P_{k-k_1-1}^{-1}), \qquad (\text{ by (6) and (7) }) \\ &= (ZY-X)m(P_{k-k_1-1}^{-1}),\end{aligned}$$

and

$$\sum_{P_{s-1}^{-1}\subset P_{k-k_1-1}^{-1}} (Zm'(P_{s-1}^{-1}) - m'(P_{k-k_1-1}^{-1})) = (ZY-X)m'(P_{k-k_1-1}^{-1}).$$

Therefore, from (10),

$$(ZY-X)m(P_{k-k_1-1}^{-1}) = (ZY-X)m'(P_{k-k_1-1}^{-1}). \tag{11}$$

If $ZY-X = (\frac{q^{k-k_1-s}(q^{k_1}-1)}{q-1} - \frac{q^{k-k_1}-1}{q^s-1})Y = 0$, then

$$\frac{q^{k-k_1-s}(q^{k_1}-1)}{q-1} = \frac{q^{k-k_1}-1}{q^s-1}. \tag{12}$$

Note that q^{k-k_1-s} is always a positive power of a certain prime p_1 under the assumption $k-k_1-s>0$. Then it follows from (12) that $p_1|q^{k-k_1}-1$, which is a contradiction, since $q^{k-k_1}\geq q$. Thus, $ZY-X\neq 0$. Then, from (11) we have

$$m(P_{k-k_1-1}^{-1}) = m'(P_{k-k_1-1}^{-1}). \tag{13}$$

With (10) and (13), it is easy to verify that

$$m(P_{s-1}^{-1}) = m'(P_{s-1}^{-1}) \qquad \text{for any } P_{s-1}^{-1}\subset P_{k-k_1-1}^{-1}. \tag{14}$$

Now, for any given P_{s+t}^t, $0\leq t\leq k_1-1$, there is a P_{s-1}^{-1} satisfying $P_{s-1}^{-1}\subset P_{s+t}^t$. Moreover, the number of the P_s^0, $P_{s-1}^{-1}\subset P_s^0\subset P_{s+t}^t$, is $\begin{bmatrix} t+1 \\ 1 \end{bmatrix}_q$. Thus, by (14), we have

$$\begin{aligned} m(P_{s+t}^t) &= \sum_{P_{s-1}^{-1}\subset P_s^0\subset P_{s+t}^t} m(P_s^0) - \Big(\begin{bmatrix} t+1 \\ 1 \end{bmatrix}_q - 1\Big)m(P_{s-1}^{-1}) \\ &= \sum_{P_{s-1}^{-1}\subset P_s^0\subset P_{s+t}^t} m'(P_s^0) - \Big(\begin{bmatrix} t+1 \\ 1 \end{bmatrix}_q - 1\Big)m'(P_{s-1}^{-1}) \\ &= m'(P_{s+t}^t). \end{aligned}$$

□

Lemma 4. Assume $m(PG(k-1,q)) = m'(PG(k-1,q))$, and $m(P_s^0) = m'(P_s^0)$ for any P_s^0 for some s satisfying $1\leq s\leq k-k_1-1$. Then, $m(p) = m'(p)$ for any point $p\in PG(k-1,q)$.

Proof. It follows from Lemma 3 that

$$m(P_{s+t}^t) = m'(P_{s+t}^t), \text{ for any } P_{s+t}^t \text{ and any } t,\ -1\leq t\leq k_1-1. \tag{15}$$

In particular, $m(P_{s+k_1-1}^{k_1-1}) = m'(P_{s+k_1-1}^{k_1-1})$. Then, it follows from Lemma 2 that

$$m(P_i^{k_1-1}) = m'(P_i^{k_1-1}), \text{ for any } P_i^{k_1-1} \text{ and any } i,\ k_1-1\leq i\leq k-1. \tag{16}$$

For any fixed $P^{k_1-2}_{s+k_1-3}$, there exists a $P^{k_1-1}_{s+k_1-1}$ such that $P^{k_1-2}_{s+k_1-3} \subset P^{k_1-1}_{s+k_1-1}$. Note that the number of the $P^{k_1-1}_{s+k_1-2}$ satisfying $P^{k_1-2}_{s+k_1-3} \subset P^{k_1-1}_{s+k_1-2} \subset P^{k_1-1}_{s+k_1-1}$ is q, and the number of the $P^{k_1-2}_{s+k_1-2}$ satisfying $P^{k_1-2}_{s+k_1-3} \subset P^{k_1-2}_{s+k_1-2} \subset P^{k_1-1}_{s+k_1-1}$ is one. So,

$$\begin{aligned}
&qm(P^{k_1-2}_{s+k_1-3}) \\
&= \sum_{P^{k_1-2}_{s+k_1-3} \subset P^{k_1-1}_{s+k_1-2} \subset P^{k_1-1}_{s+k_1-1}} m(P^{k_1-1}_{s+k_1-2}) \ + \ m(P^{k_1-2}_{s+k_1-2}) \ - \ m(P^{k_1-1}_{s+k_1-1}) \\
&= \sum_{P^{k_1-2}_{s+k_1-3} \subset P^{k_1-1}_{s+k_1-2} \subset P^{k_1-1}_{s+k_1-1}} m'(P^{k_1-1}_{s+k_1-2}) \ + \ m'(P^{k_1-2}_{s+k_1-2}) \ - \ m'(P^{k_1-1}_{s+k_1-1}), \ (\text{ by } (15), (16)) \\
&= qm'(P^{k_1-2}_{s+k_1-3}).
\end{aligned}$$

Thus, we have

$$m(P^{k_1-2}_{s+k_1-3}) = m'(P^{k_1-2}_{s+k_1-3}), \quad \forall \ P^{k_1-2}_{s+k_1-3}. \tag{17}$$

For any fixed $P^{k_1-3}_{s+k_1-4}$, there is a $P^{k_1-1}_{s+k_1-2}$ such that $P^{k_1-3}_{s+k_1-4} \subset P^{k_1-1}_{s+k_1-2}$. The number of the $P^{k_1-2}_{s+k_1-3}$, $P^{k_1-3}_{s+k_1-4} \subset P^{k_1-2}_{s+k_1-3} \subset P^{k_1-1}_{s+k_1-2}$, is $q+1$. Therefore,

$$\begin{aligned}
qm(P^{k_1-3}_{s+k_1-4}) &= \sum_{P^{k_1-3}_{s+k_1-4} \subset P^{k_1-2}_{s+k_1-3} \subset P^{k_1-1}_{s+k_1-2}} m(P^{k_1-2}_{s+k_1-3}) - m(P^{k_1-1}_{s+k_1-2}) \\
&= \sum_{P^{k_1-3}_{s+k_1-4} \subset P^{k_1-2}_{s+k_1-3} \subset P^{k_1-1}_{s+k_1-2}} m'(P^{k_1-2}_{s+k_1-3}) - m'(P^{k_1-1}_{s+k_1-2}), \quad (\text{ by } (16), (17)) \\
&= qm'(P^{k_1-3}_{s+k_1-4}).
\end{aligned}$$

It follows that

$$m(P^{k_1-3}_{s+k_1-4}) = m'(P^{k_1-3}_{s+k_1-4}), \quad \forall \ P^{k_1-3}_{s+k_1-4}. \tag{18}$$

Similarly, using (17) and (18), we get

$$m(P^{k_1-4}_{s+k_1-5}) = m'(P^{k_1-4}_{s+k_1-5}), \quad \forall \ P^{k_1-4}_{s+k_1-5}.$$

Then through deduction, we have

$$m(P^0_{s-1}) = m'(P^0_{s-1}), \quad \forall \ P^0_{s-1}. \tag{19}$$

For any fixed P^0_{s-2}, there exists a P^0_s such that $P^0_{s-2} \subset P^0_s$. Thus,

$$\begin{aligned}
qm(P^0_{s-2}) &= \sum_{P^0_{s-2} \subset P^0_{s-1} \subset P^0_s} m(P^0_{s-1}) - m(P^0_s) \\
&= \sum_{P^0_{s-2} \subset P^0_{s-1} \subset P^0_s} m'(P^0_{s-1}) - m'(P^0_s), \quad (\text{ by } (19)) \\
&= qm'(P^0_{s-2}).
\end{aligned}$$

It follows that

$$m(P^0_{s-2}) = m'(P^0_{s-2}), \quad \forall \ P^0_{s-2}. \tag{20}$$

Similarly, by using (19) and (20), we obtain

$$m(P^0_{s-3}) = m'(P^0_{s-3}), \quad \forall \ P^0_{s-3}.$$

Through deduction, we have

$$m(P^0_1) = m'(P^0_1), \quad \forall\ P^0_1, \quad \text{and} \quad m(P^0_0) = m'(P^0_0), \quad \forall\ P^0_0. \tag{21}$$

Note that P^0_0 is a point of the set $PG(k-1,q)\backslash P^{-1}_{k-k_1-1}$, and P^0_1 is a projective line containing q points of the set $PG(k-1,q)\backslash P^{-1}_{k-k_1-1}$ and one point of the subspace $P^{-1}_{k-k_1-1}$. Then, by (21), $m(p) = m'(p)$, for any point $p \in PG(k-1,q)$. □

5.2 Proof of the theorem

Now we are ready to prove the main result.

Proof of the theorem. To prove the theorem, we first show that $\phi : C \to C'$ is an isomorphism, and then show that the isomorphism ϕ is a monomial transformation.

To show that $\phi : C \to C'$ is an isomorphism, by the assumption that $C' = \phi(C)$, it is sufficient to prove that ϕ is a monomorphism. If ϕ is not a monomorphism, there exists a $\boldsymbol{c} \in C\backslash\{0\}$ such that $\phi(\boldsymbol{c}) = 0$. Then, there is an (r_0, k_1-1) subcode D such that $\boldsymbol{c} \in D$. Therefore, $\dim(\phi(D)) \leq r_0 - 1$; and thus $\phi(D)$ is not a relative (r_0, k_1-1) subcode of (C', C'_1). This is a contradiction. Therefore, ϕ is an isomorphism.

To show that the isomorphism ϕ is a monomial transformation, it is sufficient to prove that $m(p) = m'(p)$, $\forall p \in PG(k-1,q)$, according to (1). Since C and C' have the same effective length, and $w(\phi(D)) = w(D)$, for all (r_0, k_1-1) subcodes D, by Lemma 1 we have

$$\begin{aligned}
&m(PG(k-1,q)) = m'(PG(k-1,q)), \text{ and}\\
&m(P^0_{k-r_0-1}) = m'(P^0_{k-r_0-1}), \quad \forall P^0_{k-r_0-1} \subset PG(k-1,q).
\end{aligned}$$

Then, the conclusion follows from Lemma 4. □

6 Conclusions

Based on the relative generalized Hamming weights, for a linear code C, we have first defined relative (r, θ) subcodes of the pair (C, C_1), where C_1 is any subcode of C. We then established a tool to characterize relative subcodes, by using finite project geometry. Making use of this tool, we have proved that any isomorphism between two linear codes C and C' of the same effective length, which preserves the support weights of a kind of relative subcodes, is an equivalence of the codes. In a special case of our result, that is, $C_1 = \{0\}$, the relative subcodes of (C, C_1) are actually traditional subcodes of C. Therefore, we have extended the result in [4]; and thus we have further generalized the well-known MacWilliams theorem.

Acknowledgements

We would like to express our sincere thanks to the anonymous referees and the editors for their comments, which have helped to improve the paper.

References

[1] K. Bogart, D. Goldberg, and J. Gordon, An elementary proof of the MacWilliams theorem on equivalence of codes, Inform. and Control 37(1978) 19-22.

[2] I. G. Bouyukliev, Classification of Griesmer codes and dual transform, Discr. Math. 309(2009) 4049-4068.

[3] W. D. Chen and T. Kløve, The weight hierarchies of q-ary codes of dimension 4, IEEE Trans. Inform. Theory 42(1996) 2265-2272.

[4] Y. Fan, H. W. Liu, and L. Puig, Generalized Hamming weights and equivalences of codes, Science in China (Series A) 46(2003) 690-695.

[5] A. Kohnert, (l, s)-extension of linear codes, Discr. Math. 309(2009) 412-417.

[6] Z. H. Li, T. Xue and H. Lai, Secret sharing schemes from binary linear codes, Inform. Sci. (online) doi: 10.1016/ j.ins.2010.07.029 (2010).

[7] Z. H. Liu, W. D. Chen and Y. Luo, The relative generalized Hamming weight of linear q -ary codes and their subcodes, Des. Codes Cryptogr. 48(2008) 111-123.

[8] Y. Luo, C. Mitrpant, A. J. Han Vinck and K. F. Chen, Some new characters on the wire-tap channel of type II, IEEE Trans. Inform. Theory 51(2005) 1222-1229.

[9] F. J. MacWilliams, Error-correcting codes for multiple-level transmission, Bell System Tech. J. 40(1961) 281-308.

[10] F. J. MacWilliams, Combinatorial properties of elementary abelian groups, Ph.D. thesis, Radcliffe College, Cambridge, Mass., 1962.

[11] N. J. A. Sloane and F. J. MacWilliams, The theory of error-correcting codes, North-Holland, 1977.

[12] M. A. Tsfasman and S. Vladuts, Geometric approach to higher weights, IEEE Trans. Inform. Theory 41(1995) 1564-1588.

[13] H. N. Ward and J. A. Wood, Characters and the equivalence of codes, J. Combin. Theory Ser.A 73(1996) 348-352.

[14] V. K. Wei, Generalized Hamming weight for linear codes, IEEE Trans. Inform. Theory 37(1991) 1412-1418.

[15] J. A. Wood, Duality for modules over finite rings and applications to coding theory, Amer. J. Math. 121(1999) 555-575.

[16] J. A. Wood, Code equivalence characterizes finite frobenius rings, Proceedings of the American Mathematical Society 136(2008) 699-706.