Rep. Fac. Sci. Kagoshima Univ. (Math., Phys. & Chem.),
No. 28, 11-14, 1995.

MacWilliams Theorem for Linear Codes with Group Actions

Tsuyoshi ATSUMI*

(Received September 21, 1995)

Abstract

We prove MacWilliams theorem for linear codes with finite group actions. When acting group is trivial, our result becomes the ordinary MacWilliams theorem.

Key words: group, linear code, dual code, weight enumerator, MacWilliams identity.

1 Introduction and Summary

Yoshida [3] has given a version of the MacWilliams theorem [2] for codes with group action. In this paper we establish another version of the MacWilliams theorem. Our result seems to be a special case of Yoshida's. But we can not prove this.

Let V be the vector space $\mathbf{F}_q^n$, where $\mathbf{F}_q$ is the field with q elements. From now on we assume that G is a finite permutation group on the coordinates of V and $|G|$ is prime to q. Then we can define a natural action of G on V as follows: If $\mathbf{v} = (v_1, \ldots, v_n)$ and $g \in G$, we let $\mathbf{v}g = (x_1, \ldots, x_n)$, where for $i = 1, \ldots, n$, $x_i = v_{ig^{-1}}$. In this way V becomes an FG-module. A G-code is an FG-submodule of V. As in [1], the operator θ is defined by

$$\theta = \frac{1}{|G|} \sum_{g \in G} g.$$

Here we note that $C_V(G) = V\theta$ and $\theta^t = \theta$ (see [1]).

Let $C_1, \ldots, C_t$ be the orbits of the coordinates of V under the action of G. Let m_i be the orbit length of C_i. Define $\overline{C}_i$ as the vector of V which has 1 as its entry for every

* Department of Mathematics, Faculty of Science, Kagoshima University, Kagoshima 890, Japan.

point of C_i and 0 elsewhere. (This definition of the $\overline{C}_i$'s is slightly different from that in the proof of Theorem 4.3 in [1]). Then each of $\overline{C}_1, \ldots \overline{C}_t$ is in $V\theta$ and every element $\mathbf{u}$ of $V\theta$ is of the form

$$\mathbf{u} = \sum_{i=1}^{t} x_i \overline{C}_i.$$

This basis $\{\overline{C}_1, \ldots, \overline{C}_t\}$ of $V\theta$ is a key to our proof. The G-weight of a vector $\mathbf{u} = \sum_{i=1}^{t} x_i \overline{C}_i \in V\theta$ denoted $wg(\mathbf{u})$ is defined as the number of non-zero x_i. So if G consists of the identity element, e, alone, then the G-weight $wg(\mathbf{u})$ of a vector $\mathbf{u}$ is the ordinary weight $|\mathbf{u}|$. For vectors $\mathbf{a} = \sum_{i=1}^{t} a_i \overline{C}_i$, $\mathbf{b} = \sum_{i=1}^{t} b_i \overline{C}_i$ of $V\theta$, an inner product $(\mathbf{a}, \mathbf{b})_G$ of $\mathbf{a}$ and $\mathbf{b}$ is defined by

$$(1) \qquad (\mathbf{a}, \mathbf{b})_G = a_1 b_1 + \cdots + a_t b_t.$$

Let D be a vector subspace of $V\theta$. $D_G^{\perp}$ is the dual of D in $V\theta$ with respect to the inner product (1). (Notice that if G consists of the identity element, e, alone, then $D_{\{e\}}^{\perp}$ is the ordinary dual $D^{\perp}$ of D in V.)

We describe a weight enumerator of a vector subspace D of $V\theta$. The weight enumerator $W_D(x, y)$ of D is defined by

$$W_D(x, y) = \sum_{\mathbf{u} \in D} x^{t - wg(\mathbf{u})} y^{wg(\mathbf{u})}.$$

Clearly if G is trivial, that is, $G = \{e\}$, then this weight enumerator becomes the ordinary weight enumerator. We shall prove the following:

Theorem 1 *If C is a G-code, then*

$$W_{C^{\perp}\theta}(x, y) = \frac{1}{|C\theta|} W_{C\theta}(x + (q-1)y, x - y).$$

If G is trivial, that is, $G = \{e\}$, then our Theorem is the ordinary MacWilliams theorem [2, p. 146].

For notation and terminology, we shall refer the following book and paper: [2] for coding theory; [3] for codes with group action.

2 Proof of Theorem

In order to prove Theorem we need the following proposition.

Proposition 1 *Let V be the vector space $\mathbf{F}_q^n$. Assume that G is a finite permutation group on the coordinates of V and $|G|$ is prime to q. If C is a G-code and*

$$\theta = \frac{1}{|G|} \sum_{g \in G} g,$$

then

$$(C\theta)^{\perp} = ker\,\theta + C^{\perp}\theta.$$

Proof See the proofs of Theorem 4.2 and Corollary 1 in [1]. □

We shall prove Theorem. If $\mathbf{x} = \sum_i x_i\overline{C}_i \in C\theta$ and $\mathbf{y} = \sum_i y_i\overline{C}_i \in C^{\perp}\theta$, by Proposition 1 we have

$$0 = (\mathbf{x}, \mathbf{y}) = \sum_i m_i x_i y_i = (\mathbf{x}, \mathbf{y}')_G,$$

where $\mathbf{y}' = \sum_i m_i y_i \overline{C}_i$. From this it follows that

$$(2) \qquad (C\theta)^{\perp}_G \supseteq (C^{\perp}\theta)M,$$

where

$$M = diag(\underbrace{m_1, \ldots, m_1}_{m_1 \text{ times}}, \underbrace{m_2, \ldots, m_2}_{m_2 \text{ times}}, \ldots, \underbrace{m_t, \ldots, m_t}_{m_t \text{ times}}).$$

We shall show that

$$(3) \qquad (C\theta)^{\perp}_G = (C^{\perp}\theta)M.$$

By Proposition 1, we have

$$(4) \qquad dim\, C^{\perp}\theta = dim\,(C\theta)^{\perp} - dim\, ker\,\theta.$$

From linear algebra theory,

$$
\begin{aligned}
&(5) \qquad & dim\, V &= dim\, V\theta + dim\, ker\,\theta, \\
&(6) \qquad & dim\, V &= dim\,(C\theta)^{\perp} + dim\, C\theta, \\
&(7) \qquad & dim\, V\theta &= dim\,(C\theta)^{\perp}_G + dim\, C\theta.
\end{aligned}
$$

From (4), (5), (6) and (7) we see that

$$(8) \qquad dim\,(C\theta)^{\perp}_G = dim\,(C^{\perp}\theta).$$

Since M is a non-singular matrix, we have

$$(9) \qquad dim\, C^{\perp}\theta = dim\,(C^{\perp}\theta)M.$$

From (2), (8) and (9) it follows that

$$(C\theta)^{\perp}_G = (C^{\perp}\theta)M.$$

Here notice that MacWilliams theorem [2, p. 146] for the ordinary weight enumerator of the code $C\theta$ in $V\theta$ holds in this case, too.

Now we shall finish the proof of Theorem. By MacWilliams theorem and (3), we obtain the following:

$$W_{(C^{\perp}\theta)M}(x,y) = \frac{1}{|C\theta|} W_{C\theta}(x+(q-1)y, x-y). \tag{10}$$

Since $W_{(C^{\perp}\theta)M}(x,y) = W_{C^{\perp}\theta}(x,y)$, it follows from (10) that

$$W_{C^{\perp}\theta}(x,y) = \frac{1}{|C\theta|} W_{C\theta}(x+(q-1)y, x-y).$$

□

Remark. Generalizing a result of Thompson, Hayden [1] has proved the following proposition.

Proposition 2 *Using the notation of Proposition 1, then with an appropriate orthonormal base for $V\theta$, (extending $\mathbf{F}_q$ if necessary) we have where $(C\theta)^{\perp}_{V\theta}$ is the dual in terms of this basis*

$$(C\theta)^{\perp}_{V\theta} = C^{\perp}\theta.$$

So our result (3) is a generalization of Proposition 2 in a sense.

References

[1] W. G. Bridges, M. Hall, Jr. and J. L. Hayden, Codes and Designs, J. Combin. Theory Ser. A **31**(1981),155–174.

[2] F. J. MacWilliams and N. J. A. Sloane, The Theory of The Error-Correcting Codes, North Holland, Amsterdam-New York-Oxford, 1977.

[3] T. Yoshida, MacWilliams Identities for Linear Codes with Group Action, Kumamoto J. Math.,**6**(1993), 23–45.