<table>
<thead>
<tr>
<th>項目</th>
<th>内容</th>
</tr>
</thead>
<tbody>
<tr>
<td>題目</td>
<td>A Note on Hayden's Theorem (GROUPS AND COMBINATORICS)</td>
</tr>
<tr>
<td>著者</td>
<td>Atsumi, Tsuyoshi</td>
</tr>
<tr>
<td>引用</td>
<td>数理解析研究所講究録 (1992), 794: 161-168</td>
</tr>
<tr>
<td>発行日</td>
<td>1992-06</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/2433/82729">http://hdl.handle.net/2433/82729</a></td>
</tr>
<tr>
<td>タイプ</td>
<td>Departmental Bulletin Paper</td>
</tr>
<tr>
<td>版本</td>
<td>publisher</td>
</tr>
<tr>
<td>発行機関</td>
<td>Kyoto University</td>
</tr>
</tbody>
</table>
A Note on Hayden’s Theorem

Tsuyoshi Atsumi

The Case a finite Group G acts on Code.

1. Definitions from Coding Theory

Yoshida [5] showed that there is a generalization of MacWilliams identity [3] to codes with group action. We use ideas from [1] to give an elementary proof to Yoshida’s identity in a special case.

Let $V$ be the vector space $F_q^n$, where $F_q$ 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 $v = (v_1, \ldots, v_n)$ and $g \in G$, we let $vg = (x_1, \ldots, x_n)$ 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 $\theta$ 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 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 $U = V\theta$ and every element $u$ of $U = V\theta$ is of the form

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

This basis $\{\overline{C}_1, \ldots, \overline{C}_t\}$ of $U$ is a key to our proof of Yoshida’s result. Yoshida weight of a vector $u = \sum_{i=1}^t x_i \overline{C}_i \in U$ denoted $wy(u)$ is defined as the number of non-zero $x_i$. So if $G$ consists of the identity element, $e$, alone, then Yoshida weight $wy(u)$ of a vector $u$ is the ordinary weight $|u|$. If $a = \sum_{i=1}^t a_i \overline{C}_i$ and $b = \sum_{i=1}^t b_i \overline{C}_i$; are any two vectors in $U$, then inner product $(a, b)_G$ of $a$ and $b$ is defined by

$$(a, b)_G = a_1 b_1 + \cdots + a_t b_t. \quad (1)$$  

Let $D$ be a vector subspace of $U = V\theta$. $D_G^\perp$ is the dual of $D$ in $U$ 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 $U = V\theta$. The weight enumerator $W_D(x, y)$ of $D$ is defined by

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

Clearly if $G$ is trivial, that is, $G = \{e\}$, then this weight enumerator becomes the ordinary weight enumerator. For notation and terminology, we will refer the following book and paper: [3] for coding theory; [5] for codes with group action.

2. G-Codes

We have the following theorem which is a special case of Yoshida’s result [5].

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

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

If $G$ is trivial, that is, $G = \{e\}$, then our theorem is the ordinary MacWilliams theorem [3. pp 146]

In order to prove Theorem 1 we need the following proposition.

**Proposition 1 (Hayden).** Let $V$ be the vector space $F_q^n$. 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

$$(C\theta)^\perp = \text{Ker } \theta + C^\perp \theta.$$  

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

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

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

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

$$(C\theta)^\perp \supseteq (C^\perp \theta)_M,$$  

where
\[ M = \text{diag}(a_1, \ldots, a_n) \quad i = 1, \ldots, n; \]
\[ a_i = m_j \quad \text{if} \quad i \in C_j. \]

Next we will show that
\[ (C\theta)^\perp_G \subseteq (C^\perp\theta)M. \] (3)

If \( x = \sum_i x_i \overline{C}_i \in (C\theta)^\perp_G \), \( x' = \sum_i (x_i/m_i) \overline{C}_i \) and \( y = \sum_i y_i \overline{C}_i \in C\theta \), we have
\[ (x', y) = \sum_i m_i (x_i/m_i) y_i = (x, y)_G = 0. \]

This shows that
\[ x' \in (C\theta)^\perp. \] (4)

Since \( x' \in U = V\theta \), (4) and Proposition 1 imply that \( x' \in C^\perp\theta \).

Hence, \( x = x'M \in (C^\perp\theta)M \). Now we proved that
\[ (C\theta)^\perp_G \subseteq (C^\perp\theta)M. \] (5)

From (2) and (5) it follows that
\[ (C\theta)^\perp_G = (C^\perp\theta)M. \] (6)

Here notice that MacWilliams theorem [3. pp 146] for the ordinary weight enumerator of the code \( C\theta \) in \( U (= V\theta) \) holds in this case, too.

**MacWilliams theorem.**
\[ W((C\theta)^\perp_G)(x, y) = \frac{1}{|C\theta|} W_{C\theta}(x + (q-1)y, x-y). \]

Now we will finish the proof of Theorem 1. By the above MacWilliams theorem and (6), we obtain the following.
\[ W((C^\perp\theta)M)(x, y) = \frac{1}{|C\theta|} W_{C\theta}(x + (q-1)y, x-y). \] (7)

Since \( W((C^\perp\theta)M)(x, y) = W_{C^\perp\theta}(x, y) \), it follows from (7) 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 $U$, (extending $F_q$ if necessary) we have where $(C\theta)^\perp_U$ is the dual in terms of this basis

$$(C\theta)^\perp_U = C^\perp \theta.$$

So our result (6) is a generalization of Proposition 2 in a sense.

**The Case a finite Group $G$ acts on Lattice**

3. **Definitions from Lattice Theory**

In [5] Yoshida raised the following problem.

**Problem.** What can we say about lattices with groups action? Can we define the equivariant version of theta functions?

He showed in [5] that there is a generalization of MacWilliams identity [3] to codes with group action. In this paper we will prove that there is a lattice version of this result. In order to state our theorem we introduce notation and terminology in lattice theory. Let $V$ be the real $n$-dimensional space $\mathbb{R}^n$. A lattice $\Lambda$ [4] is a subgroup of $V$ satisfying one of the following equivalent conditions:

i) $\Lambda$ is discrete and $V/\Lambda$ is compact;

ii) $\Lambda$ is discrete and generates the $\mathbb{R}$-vector space $V$;

iii) There exists an $\mathbb{R}$-basis $(e_1, \ldots, e_n)$ of $V$ which is a $\mathbb{Z}$-basis of $\Lambda$ (i.e. $\Lambda = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_n$).

Let the coordinates of the basis vectors be

$e_1 = (e_{11}, \ldots, e_{1n}),$

$e_2 = (e_{12}, \ldots, e_{2n}),$

\[ \vdots \]

$e_n = (e_{1n}, \ldots, e_{nn}).$

The $n \times n$ matrix $M$ with $(i, j)$-entry equal to $e_{ij}$ is called a generator matrix for $\Lambda$. The determinant of $\Lambda$ is defined to be $\det \Lambda = |\det M|$. Given two vectors $u = (u_1, \ldots, u_n)$,
\( \mathbf{v} = (v_1, \ldots, v_n) \) of \( V \), their inner product will be denoted by \( \mathbf{u} \cdot \mathbf{u} \) or \( (\mathbf{u}, \mathbf{u}) \). The dual lattice is defined by

\[ \Lambda^\perp = \{ \mathbf{u} \in \mathbb{R}^n \mid \mathbf{u} \cdot \mathbf{v} = u_1 v_1 + \cdots + u_n v_n \in \mathbb{Z} \text{ for all } \mathbf{v} \in \Lambda \}. \]

The theta series \( \Theta_{\Lambda}(z) \) of a lattice \( \Lambda \) is given by

\[ \Theta_{\Lambda}(z) = \sum_{\mathbf{u} \in \Lambda} q^{\mathbf{u} \cdot \mathbf{u}}, \]

where \( q = e^{\pi iz} \). Jacobi's formula for the theta series of the dual lattice:

\[ \Theta_{\Lambda^\perp}(z) = (\det \Lambda)(i/z)^{n/2} \Theta_{\Lambda}(-1/z). \] (8)

The main purpose of this paper is to generalize equation (8) when a finite group \( G \) acts on \( \Lambda \). From now on we assume that \( G \) is a finite permutation group on the coordinates of \( V \). Then we can define a natural action of \( G \) on \( V \) as follows: If \( \mathbf{v} = (v_1, \ldots, v_n) \in V \) 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 \( RG \)-module. A \( G \)-lattice is a lattice which is also an \( \mathbb{Z}G \)-submodule of \( V \). As in [1], the operator \( \theta \) is defined by

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

Here we note that \( V \theta = \{ \mathbf{v} \in V \mid \mathbf{v} g = \mathbf{v} \text{ for all } g \in G \} \) 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 \( 1/\sqrt{m_i} \) as its entry for every point of \( C_i \) and 0 elsewhere. (This definition of the \( \overline{C}_i \)'s is similar to 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

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

If \( \mathbf{a} = \sum_{i=1}^{t} a_i \overline{C}_i \) and \( \mathbf{b} = \sum_{i=1}^{t} b_i \overline{C}_i \) are any two vectors in \( V \theta \), then inner product \( \mathbf{a} \circ \mathbf{b} \) of \( \mathbf{a} \) and \( \mathbf{b} \) is defined by

\[ \mathbf{a} \circ \mathbf{b} = a_1 b_1 + \cdots + a_t b_t. \] (9)

Let \( D \) be a lattice in \( V \theta \). \( D_G^\perp \) is the dual of \( D \) in \( V \theta \) with respect to the inner product (9).

The norm of \( \mathbf{u} \in D \) is \( \mathbf{u} \circ \mathbf{u} \).

We describe the theta series \( \Theta_D(z) \) of a sublattice \( D \) as follows:

\[ \Theta_D(z) = \sum_{\mathbf{u} \in D} q^{\mathbf{u} \circ \mathbf{u}}, \]
where $q = e^{\pi iz}$.

For notation and terminology, we will refer the following book and paper: [4] for lattice theory; [5] for lattices with group action.

4. G-Lattices

We have the following:

**Theorem 2.** If $\Lambda$ is a G-lattice and $\Lambda_0 = \{ r \in \Lambda \mid r\theta \in \Lambda \}$, then

$$\Theta_{\Lambda_0 \theta}(z) = (\det \Lambda_0 \theta)(i/z)^{n/2}\Theta_{\Lambda_0 \theta}(-1/z).$$

Note that $\Lambda_0 \theta = \Lambda \cap \Lambda \theta = \{ v \in \Lambda \mid v\theta = v \text{ for all } g \in G \}$.

In order to prove Theorem 2 we need the following proposition.

**Proposition 3.** Let $V$ be the vector space $\mathbb{R}^n$. Assume that $G$ is a finite permutation group on the coordinates of $V$. If $\Lambda$ is a G-lattice and $\Lambda_0 = \{ r \in \Lambda \mid r\theta \in \Lambda \}$, then

$$(\Lambda_0 \theta)^\perp = \text{Ker} \theta \oplus \Lambda_0^\perp \theta.$$
This implies that

\[(\Lambda_0\theta)^\perp \subseteq \text{Ker } \theta + \Lambda_0^\perp \theta. \quad (11)\]

(10) and (11) complete the proof of Proposition 3. \(\blacksquare\)

We will prove Theorem 2. If \(x = \sum_i x_i \overline{C}_i \in \Lambda_0\theta\) and \(y = \sum_i y_i \overline{C}_i \in \Lambda_0^\perp \theta\), by Proposition 3 we have

\[x \circ y = (x, y) \in Z.\]

So

\[\Lambda_0^\perp \theta \subseteq (\Lambda_0\theta)^\perp. \quad (12)\]

Now take \(x = \sum_i x_i \overline{C}_i \in (\Lambda_0\theta)^\perp, \ y = \sum_i y_i \overline{C}_i \in \Lambda_0\theta\), and observe

\[(x, y) = x \circ y \in Z.\]

This shows that

\[x \in (\Lambda_0\theta)^\perp. \quad (7)\]

Since \(x \in V\theta\), (13) and Proposition 3 imply that \(x \in \Lambda_0^\perp \theta\).

Now we proved that

\[(\Lambda_0\theta)^\perp \subseteq \Lambda_0^\perp \theta. \quad (14)\]

From (12) and (14) it follows that

\[(\Lambda_0\theta)^\perp_G = \Lambda_0^\perp \theta. \quad (15)\]

Now we will finish the proof of Theorem 2. Jacobi's formula for the theta series of the dual lattice \((\Lambda_0\theta)^\perp_G\) in \(V\theta\):

\[\Theta_{(\Lambda_0\theta)^\perp_G}(z) = (\det \Lambda_0\theta)(i/z)^{n/2} \Theta_{\Lambda_0\theta}(-1/z).\]

Hence \((\Lambda_0\theta)^\perp_G = \Lambda_0^\perp \theta\) establishes our theorem. \(\blacksquare\)

**Remark.** It is easy to prove that

\[\Lambda/\Lambda_0 \cong \Lambda\theta/\Lambda \cap \Lambda\theta,\]

\[\Lambda_0 = (\Lambda \cap \text{Ker } \theta) \oplus (\Lambda \cap \Lambda\theta).\]
References


Department of Mathematics
Faculty of Science
Kagoshima University
Kagoshima 890
Japan