TAIWANESE JOURNAL OF MATHEMATICS
Vol. 8, No. 3, pp. 499-502, September 2004
This paper is available online at http://www.math.nthu.edu.tw/tjm/

AN ELEMENTARY PROOF OF MACWILLIAMS-DELSARTE IDENTITY

Rongzheng Jiao and Hongwen Lu

Abstract. The MacWilliams-Delsarte identity is very important in coding theory. We will give a new proof of the identity using elementary method in this paper, which is much simpler than the original one [1].

1. Introduction

The MacWilliams-Delsarte identity is very important in coding theory. There is a proof in the widespread encyclopedic book *the theory of error-correcting codes* [1]. First let's introduce some notations. Let $V(n,2)$ be the binary vector space of dimension n , $d_H(\cdot,\cdot)$ and $\omega_H(\cdot)$ denote the hamming distance and weight respectively, and $< \cdot,\cdot >$ be the scalar product of two binary vectors. For any set E, $|E|$ denote the number of the elements in E.

Let C be a binary code of length n with M codewords. Let

$$D_i = \frac{1}{M^2}|\{(a,b) : a,b \in C, d_H(a,b) = i\}|, i = 0,1,\ldots,n, \tag{1}$$

where $\{D_i\}_0^n$ is the distribution of code C, and

$f(z) = \sum_{i=0}^{n} D_i z^i$ be the distance enumerator of code C. Let

$$\overline{D}_i = \frac{1}{M^2} \sum_{\substack{u\in V(n,2):\\ \omega_H(u)=i}} [\sum_{a\in C}(-1)^{<u,a>}]^2, i = 0,1,\ldots,n. \tag{2}$$

Obviously, $\overline{D}_i \geq 0$. Set $g(z) = \sum_{i=0}^{n} \overline{D}_i z^i$.

Received April 15, 2003.
Communicated by S. B. Hsu.
2000 *Mathematics Subject Classification*: 94A24; 11T06.
Key words and phrases: MacWilliams-Delsarte identity; binary code, length, distance enumerator, scalar product.
Supported by NSFC (Grant No.10171076) and by Foundation of China Scholarship Council (No. 2003832099). We thank the referee for the valuable suggestions given to us.

The MacWilliams-Delsarte identity assert the relationship between these two kinds of distance enumerator of code C as follow:

Theorem (the MacWilliams-Delsarte identity)

$$g(z) = (1+z)^n f(\frac{1-z}{1+z}), \tag{3}$$

$$f(z) = \frac{1}{2^n}(1+z)^n g(\frac{1-z}{1+z}). \tag{4}$$

2. Proof of the Identity

Obviously, the equations (3) and (4) are equivalent: replacing z by $\frac{1-z}{1+z}$ in (3) we obtain (4), and similary replacing z by $\frac{1-z}{1+z}$ in (4) we obtain (3). So we need only to prove (3).

For u, v in $V(n,2)$, let $u = (u_1, u_2, \ldots, u_n)$ and $v = (v_1, v_2, \ldots, v_n)$. First we define the scalar product

$$< u, v >= |\{i : u_i = v_i = 1, \}|, \tag{5}$$

(i.e. $< u, v >$ denote the number of positions where both binary vectors u and v is 1), then it follows that and

$$< 1-u, 1-v >= |\{i : u_i = v_i = 0, \}|, \tag{6}$$

where $1 = (1, 1, \ldots, 1) \in V(n,2)$. (i.e. $< 1-u, 1-v >$ denote the number of positions where both binary vectors u and v is 0.) On the other hand, we have

$$\begin{aligned} &< 1-u, 1-v >=< 1, 1 > - < 1, v > - < u, 1 > - < u, v > \\ &= n - \omega_H(u) - \omega_H(v) + < u, v >, \end{aligned} \tag{7}$$

and obviously we have

$$d_H(u,v) = n - < 1-u, 1-v > - < u, v > . \tag{8}$$

From (6),(7)and(8) we obtain

$$< u, v >= \frac{\omega_H(u) + \omega_H(v) - d_H(u,v)}{2}. \tag{9}$$

From (2), the definition of $\overline{D}_i$, we have

$$
\begin{aligned}
\overline{D}_i &= \frac{1}{M^2}\sum_{\substack{u\in V(n,2):\\ \omega_H(u)=i}}[\sum_{a\in C}(-1)^{<u,a>}]^2\\
&= \frac{1}{M^2}\sum_{\substack{u\in V(n,2):\\ \omega_H(u)=i}}\sum_{a\in C}(-1)^{<u,a>}\sum_{b\in C}(-1)^{-<u,b>}\\
&= \frac{1}{M^2}\sum_{\substack{u\in V(n,2):\\ \omega_H(u)=i}}\sum_{a\in C}\sum_{b\in C}(-1)^{<u,a-b>}.
\end{aligned}
\tag{10}
$$

Using (9) we have

$$
\begin{aligned}
\overline{D}_i &= \frac{1}{M^2}\sum_{\substack{u\in V(n,2):\\ \omega_H(u)=i}}\sum_{a\in C}\sum_{b\in C}(-1)^{\frac{\omega_H(u)+\omega_H(a-b)-d_H(u,a-b)}{2}}\\
&= \frac{1}{M^2}\sum_{\substack{u\in V(n,2):\\ \omega_H(u)=i}}\sum_{a\in C}\sum_{b\in C}(-1)^{\frac{i+\omega_H(a-b)-d_H(u,a-b)}{2}}.
\end{aligned}
\tag{11}
$$

It follows that

$$
\begin{aligned}
&\sum_{\substack{u\in V(n,2):\\ \omega_H(u)=i}}\sum_{a\in C}\sum_{b\in C}(-1)^{\frac{i+\omega_H(a-b)-d_H(u,a-b)}{2}}\\
&= \sum_{\substack{u\in V(n,2):\\ \omega_H(u)=i}}\sum_{j=0}^{n}\sum_{a\in C}\sum_{\substack{b\in C,\\ d_H(a,b)=j}}(-1)^{\frac{i+j-d_H(u,a-b)}{2}}\\
&= \sum_{j=0}^{n}\sum_{a\in C}\sum_{\substack{b\in C,\\ d_H(a,b)=j}}\sum_{\substack{u\in V(n,2):\\ \omega_H(u)=i}}(-1)^{\frac{i+j-d_H(u,a-b)}{2}}.
\end{aligned}
\tag{12}
$$

We shall deal with the summand $\sum_{u\in V(n,2):\omega_H(u)=i}(-1)^{\frac{i+j-d_H(u,a-b)}{2}}$ in the identity (12) with $d_H(a,b)=j$ in the following segment. There are j positions in the n-dim binary vector $a-b$ where is 1, since $d_H(a,b)=j$. At first we suppose that there are s positions where is 1 both in vectors $a-b$ and u. In this case $\frac{i+j-d_H(u,a-b)}{2}=s$, and the number s ranges from 0 to j, for every such fixed pair (a,b) of binary vectors. For every such binary vector $a-b$, there are $\binom{j}{s}\cdot\binom{n-j}{i-s}$ such binary vectors u, because $\omega_H(u)=i$.

From the definition of D_i , (11), (12) and the above, we have

$$\overline{D}_i = \sum_{j=0}^{n} \sum_{s=0}^{j} D_j (-1)^s \binom{j}{s} \binom{n-j}{i-s}. \tag{13}$$

Now we complete the proof of (3) by (13)

$$(1+z)^n f(\frac{1-z}{1+z}) = \sum_{j=0}^{n} D_j (1+z)^{n-j} (1-z)^j$$

$$= \sum_{j=0}^{n} D_j \sum_{s=0}^{j} \binom{j}{s} (-1)^s z^s \sum_{t=0}^{n-j} \binom{n-j}{t} z^t$$

$$= \sum_{j=0}^{n} \sum_{s=0}^{j} \sum_{t=0}^{n-j} (-1)^s \binom{j}{s} \binom{n-j}{t} z^{s+t} D_j = g(z).$$

References

1. F. J. MacWilliams, and N. J. A. Sloane, The theory of error-correcting codes. North-Holland, Amsterdam (third printing), (1981), 135-141.

Rongzheng Jiao
Department of Mathematics,
Yangzhou University,
Yangzhou 225002,
China
E-mail: rongzhengjiao@yahoo.com.cn

Hongwen Lu
Institute of Mathematics,
Tongji University,
Shanghai 200092,
China
E-mail: ljghw@online.sh.cn