Jurnal Teknologi

Full Paper

THE EQUIVALENT IDENTITIES OF THE MACWILLIAMS IDENTITIES FOR LINEAR CODES

Bao Xiaomin*

School of Mathematics & Statistics, Southwest University, Chongqing, 400715, China

Article history
Received
29 January 2015
Received in revised form
24 March 2015
Accepted
1 August 2015

*Corresponding author
xbao@swu.edu.cn

Abstract

We use derivatives to prove the equivalences between MacWilliams identity and its four equivalent forms, and present new interpretations for the four equivalent forms.

Keywords: Linear code, Hamming weight, MacWilliams identity, equivalent, derivative

1.0 INTRODUCTION

Let $\mathcal{C}$ be a (n, k) linear code on the field F_q=$GF(q)$ and let $\mathcal{C}^{\wedge}$ be its dual code. Define:

$$W_{\mathcal{C}}^{i} := \text{the number of codewords of weight } i \text{ in } \mathcal{C}$$

and

$$W_{\mathcal{C}}(x,y) := W_{\mathcal{C}}^{0}x^{n} + W_{\mathcal{C}}^{1}x^{n-1}y + \cdots + W_{\mathcal{C}}^{n}y^{n} = \sum_{i=0}^{n} W_{\mathcal{C}}^{i}x^{n-i}y^{i}.$$

The following identity is proved by [6] and is called the MacWilliams identity:

$$(1) \qquad W_{\mathcal{C}}(x,y) = \frac{1}{q^{n-k}} W_{\mathcal{C}^{\perp}}(x+(q-1)y, x-y).$$

The following are four equivalent forms of the MacWilliams identity:

$$(2)\ W_{\mathcal{C}}^{r} = \frac{1}{q^{n-k}} \sum_{j=0}^{n} W_{\mathcal{C}^{\perp}}^{j} \sum_{i=0}^{r} (-1)^{i} \binom{n-j}{r-i}\binom{j}{i}(q-1)^{r-i}, \quad r = 0,1,\cdots,n$$

$$(3)\ \sum_{j=0}^{n} \binom{j}{r} W_{\mathcal{C}}^{j} = q^{k-r} \sum_{j=0}^{n} (-1)^{j}(q-1)^{r-j} \binom{n-j}{r-j} W_{\mathcal{C}^{\perp}}^{j}, \quad r = 0,1,\cdots,n$$

$$(4)\ \sum_{j=0}^{n} \binom{n-j}{r} W_{\mathcal{C}}^{j} = q^{k-r} \sum_{j=0}^{n} \binom{n-j}{r-j} W_{\mathcal{C}^{\perp}}^{j}, \quad r = 0,1,\cdots,n$$

$$(5)\ \sum_{j=0}^{n} \binom{j}{t}\binom{n-j}{r-t} W_{\mathcal{C}}^{j} = q^{k-r} \sum_{i=0}^{t} (-1)^{i}(q-1)^{t-i} \sum_{j=0}^{r} \binom{n-j}{r-j}\binom{j}{i}\binom{r-j}{t-i} W_{\mathcal{C}^{\perp}}^{j},$$

$$0 \le t \le r \le n$$

The MacWilliams identity and the four equivalent forms have been studied by many authors [1-6, 8, 9]. In 1963, MacWilliams [6] proved that (2), (3) and (4) are all equivalent to MacWilliams identity (1). In 1983, by using a method different from that of [6], Blahut [1] proved that (1) can be derived from (4). Similar method can also be used to derive (1) from (3). Identity (5) was initially discovered by Brualdi *et al.* in 1980 [2], and they showed that (5) can be derived from (2). In 1997, Goldwasser [4] proved (5) by induction.

It should be pointed out that Brualdi *et al.* presented combinatorial interpretations for (3), (4) and (5) in [2]. Let M be a $q\times n$ matrix whose rows are the codewords of $\mathcal{C}$ in some order. Let r be an integer with $0\le r\le n$. A row of M with weight j contains $\binom{j}{r}$ r-tuples of nonzeros. So the number of r-tuples of nonzero in the rows of M equals $\sum_{j=0}^{n}\binom{j}{r}W_{\mathcal{C}}^{j}$. Hence identity (3) is a consequence of counting the number of r-tuples of nonzeros in the rows of M in two different ways.

Similarly, identity (4) is a consequence of counting the number of *r*-tuples of zeros in the rows *M* in two different ways; while identity (5) is a consequence of counting the number of *r*-tuples of weight *t* in the rows of *M* in two different ways.

According to their interpretations, both (3) and (4) are special cases of (5).

In the following section we will use derivatives to prove the equivalence between anyone of (2), (3), (4), (5) and (1), our proofs also unveil new relationships between MacWilliams identity and its equivalent forms.

2.0 PROOFS OF EQUIVALENCES

The following two lemmas are needed in our equivalence proofs:

Lemma 1. Let $X=x+(q-1)y, Y=x-y, f=X^sY^t$, then for any non-negative integers *l*, *m* we have

$$\frac{\partial^l f}{\partial x^l}=\sum_{i=0}^{l} l!\binom{s}{l-i}\binom{t}{i}X^{s-l+i}Y^{t-i},$$

$$\frac{\partial^m f}{\partial y^m}=\sum_{i=0}^{m}(-1)^i(q-1)^{m-i}m!\binom{s}{m-i}\binom{t}{i}X^{s-m+i}Y^{t-i}.$$

Lemma 2. Let $f(x,y)$ and $g(x,y)$ be two homogeneous polynomials of degree *n* in *x*, *y*. If

$$\left.\frac{\partial^r f}{\partial y^r}\right|_{x=1,y=0}=\left.\frac{\partial^r g}{\partial y^r}\right|_{x=1,y=0},\quad 0\le r\le n$$

or

$$\left.\frac{\partial^r f}{\partial y^r}\right|_{x=0,y=1}=\left.\frac{\partial^r g}{\partial y^r}\right|_{x=0,y=1},\quad 0\le r\le n$$

or

$$\left.\frac{\partial^r f}{\partial y^r}\right|_{x=y=1}=\left.\frac{\partial^r g}{\partial y^r}\right|_{x=y=1},\quad 0\le r\le n$$

then $f(x,y)=g(x,y)$.

Proof of Lemma 1. We only prove the second identity, the first one can be proved similarly.

If *m* = 0, the result is obvious. Now let *m*>0, and suppose

$$\frac{\partial^{m-1} f}{\partial y^{m-1}}=\sum_{i=0}^{m-1}(-1)^i(q-1)^{m-1-i}(m-1)!\binom{s}{m-1-i}\binom{t}{i}X^{s-m+1+i}Y^{t-i}.$$

Then from $\frac{\partial^m f}{\partial y^m}=\frac{\partial(\partial^{m-1}f/\partial y^{m-1})}{\partial y}$ we can get

$$\begin{aligned}\frac{\partial^m f}{\partial y^m}&=\sum_{i=0}^{m-1}(-1)^i(q-1)^{m-i}(m-1)!(m-i)\binom{s}{m-i}\binom{t}{i}X^{s-m+i}Y^{t-i}\\&\quad+\sum_{i=0}^{m-1}(-1)^{i+1}(q-1)^{m-(i+1)}(m-1)!(i+1)\binom{s}{m-(i+1)}\binom{t}{i+1}X^{s-m+(i+1)}Y^{t-(i+1)}\\&=\sum_{i=0}^{m-1}(-1)^i(q-1)^{m-i}(m-1)!(m-i)\binom{s}{m-i}\binom{t}{i}X^{s-m+i}Y^{t-i}\\&\quad+\sum_{i=1}^{m}(-1)^i(q-1)^{m-i}(m-1)!i\binom{s}{m-i}\binom{t}{i}X^{s-m+i}Y^{t-i}\\&=\sum_{i=0}^{m}(-1)^i(q-1)^{m-i}m!\binom{s}{m-i}\binom{t}{i}X^{s-m+i}Y^{t-i}\end{aligned}$$

the other two cases can be proved similarly.

Let

$$f(x,y)=\sum_{i=0}^{n}f_i x^{n-i}y^i,\quad g(x,y)=\sum_{i=0}^{n}g_i x^{n-i}y^i,$$

then from (6) we can get the following equations:

$$\begin{aligned}&n!\,f_n=n!\,g_n,\\&(n-1)!\sum_{i=n-1}^{n}\binom{i}{n-1}f_i=(n-1)!\sum_{i=n-1}^{n}\binom{i}{n-1}g_i\\&(n-2)!\sum_{i=n-2}^{n}\binom{i}{n-2}f_i=(n-2)!\sum_{i=n-2}^{n}\binom{i}{n-2}g_i\\&\vdots\qquad\qquad\vdots\\&2!\sum_{i=2}^{n}\binom{i}{2}f_i=2!\sum_{i=2}^{n}\binom{i}{2}g_i\\&\sum_{i=1}^{n}\binom{i}{1}f_i=\sum_{i=1}^{n}\binom{i}{1}g_i\end{aligned}$$

Solving these equations we get

$$f_n=g_n, f_{n-1}=g_{n-1}, \cdots, f_1=g_1, f_0=g_0.$$

Therefore $f(x,y)=g(x,y)$.

2.1 Derive (2) or (3) from (1)

By taking *r*-th partial derivative with respect to y on both sides of (1), we get

$$\sum_{j=0}^{n} r!\binom{j}{r}W_C^j x^{n-j}y^{j-r}=\frac{1}{q^{n-k}}\sum_{j=0}^{n}W^j\sum_{C^\perp}\sum_{i=0}^{r}(-1)^i r!\binom{n-j}{r-i}\binom{j}{i}(q-1)^{r-i}[x+(q-1)y]^{n-j-r+i}(x-y)^{j-i}$$

- Substituting 1 for x, 0 for *y* in the above equation we get

$$W_{\mathcal{C}}^{r} = \frac{1}{q^{n-k}} \sum_{j=0}^{n} W_{\mathcal{C}^{\perp}}^{j} \sum_{i=0}^{r} (-1)^{i} \binom{n-j}{r-i} \binom{j}{i} (q-1)^{r-i},$$

So from (1) we can derive (2).

- Substituting 1 for both x and y we get

$$\sum_{j=0}^{n} \binom{j}{r} W_{\mathcal{C}}^{j} = \sum_{j=r}^{n} \binom{j}{r} W_{\mathcal{C}}^{j} \qquad (\text{if } j < r \text{ then } \binom{j}{r} = 0)$$

$$= \frac{1}{q^{n-k}} \sum_{j=0}^{n} W_{\mathcal{C}^{\perp}}^{j} (-1)^{j} \binom{n-j}{r-j} (q-1)^{r-j} q^{n-r}$$

$$= q^{k-r} \sum_{j=0}^{n} (-1)^{j} (q-1)^{r-j} \binom{n-j}{r-j} W_{\mathcal{C}^{\perp}}^{j}$$

Therefore, from (1) we can derive (3).

2.2 Derive (4) from (1)

By taking *r*-th partial derivative with respect to x on both sides of (1), we get

$$\sum_{j=0}^{n} r! \binom{n-j}{r} W_{\mathcal{C}}^{j} x^{n-j-r} y^{j} = \frac{1}{q^{n-k}} \sum_{j=0}^{n} W_{\mathcal{C}^{\perp}}^{j} \sum_{i=0}^{r} r! \binom{n-j}{r-i} \binom{j}{i} [x+(q-1)y]^{n-j-r+i} (x-y)^{j-i}$$

Let x=y=1, then we get

$$\sum_{j=0}^{n} \binom{n-j}{r} W_{\mathcal{C}}^{j} = \frac{1}{q^{n-k}} \sum_{j=0}^{n} W_{\mathcal{C}^{\perp}}^{j} \binom{n-j}{r-j} q^{n-r}$$

$$= q^{k-r} \sum_{j=0}^{n} \binom{n-j}{r-j} W_{\mathcal{C}^{\perp}}^{j}.$$

So from (1) we can derive (4).

2.3 Derive (5) from (1)

$$f(x,y) = \sum_{j=0}^{n} W_{\mathcal{C}}^{j} x^{n-j} y^{j}$$

Let $f(x,y) = W_{\mathcal{C}}(x,y)$. For $0 \le t \le r \le n$, by taking *r*-th mixed partial derivatives on both sides of

we can get

$$\frac{\partial^{r} f}{\partial x^{r-t} \partial y^{t}} = \frac{\partial^{r-t}}{\partial x^{r-t}} \left(t! \sum_{j=0}^{n} \binom{j}{t} W_{\mathcal{C}}^{j} x^{n-j} y^{j-t} \right)$$

$$= t!(r-t)! \sum_{j=0}^{n} \binom{j}{t} \binom{n-j}{r-t} W_{\mathcal{C}}^{j} x^{n-j-r+t} y^{j-t}$$

From

and lemma 1 we get

$$\frac{\partial^{r} f}{\partial x^{r-t} \partial y^{t}} = \frac{1}{q^{n-k}} t!(r-t)! \sum_{j=0}^{n} W_{\mathcal{C}^{\perp}}^{j} \sum_{s=0}^{r-t} \binom{n-j}{r-t-s} \binom{j}{s} \sum_{i=0}^{t} (-1)^{i} (q-1)^{t-i} \binom{n-j-r+t+s}{t-i} \binom{j-s}{i} [x+(q-1)y]^{n-j-r+s+i} (x-y)^{j-s-i}$$

So we have

$$\sum_{j=0}^{n} \binom{j}{t} \binom{n-j}{r-t} W_{\mathcal{C}}^{j} x^{n-j-r+t} y^{j-t} = \frac{1}{q^{n-k}} \sum_{j=0}^{n} W_{\mathcal{C}^{\perp}}^{j} \sum_{s=0}^{r-t} \binom{n-j}{r-t-s} \binom{j}{s} \sum_{i=0}^{t} (-1)^{i} (q-1)^{t-i} \binom{n-j-r+t+s}{t-i} \binom{j-s}{i} [x+(q-1)y]^{n-j-r+s+i} (x-y)^{j-s-i}$$

Substituing 1 for both x and *y*, and also notice that $(x\text{-}y)^{j-s-i}=0$ when $j \ne s+i$ we get

$$\sum_{j=0}^{n} \binom{j}{t} \binom{n-j}{r-t} W_{\mathcal{C}}^{j} = \frac{1}{q^{n-k}} \sum_{j=0}^{r} W_{\mathcal{C}^{\wedge}}^{j} \sum_{i=0}^{t} \binom{n-j}{r-t-j+i} \binom{j}{j-i} (-1)^{i} (q-1)^{t-i} \binom{n-r+t-i}{t-i} q^{n-r}$$

$$= q^{k-r} \sum_{i=0}^{t} (-1)^{i} (q-1)^{t-i} \sum_{j=0}^{r} \binom{n-j}{r-j} \binom{j}{i} \binom{r-j}{t-i} W_{\mathcal{C}^{\wedge}}^{j}$$

So (5) holds.

2.4 Derive (1) from (2)

Let

$$f(x,y) = W_{\mathcal{C}}(x,y) = \sum_{j=0}^{n} W_{\mathcal{C}}^{j} x^{n-j} y^{j}$$

$$g(x,y) = \frac{1}{q^{n-k}} W_{\mathcal{C}^{\wedge}}(x+(q-1)y, x-y)$$

$$= \frac{1}{q^{n-k}} \sum_{j=0}^{n} W_{\mathcal{C}^{\wedge}}^{j} [x+(q-1)y]^{n-j} (x-y)^{j}$$

Then both $f(x,y)$ and $g(x,y)$ are homogeneous polynomials of degree *n* in x, *y*.

For any non-negative integer $r \le n$, by lemma 1 we have

$$\left.\frac{\partial^r f}{\partial y^r}\right|_{x=1,y=0} = r!W_{\mathcal{C}}^r$$

$$\left.\frac{\partial^r g}{\partial y^r}\right|_{x=1,y=0} = \frac{1}{q^{n-k}}\sum_{j=0}^{n} W_{\mathcal{C}^\wedge}^j\, r!\sum_{i=0}^{r}(-1)^i(q-1)^{r-i}\binom{n-j}{r-i}\binom{j}{i}$$

$$\left.[x+(q-1)y]^{n-j-r+i}(x-y)^{j-i}\right|_{x=1,y=0}$$

$$= r!\frac{1}{q^{n-k}}\sum_{j=0}^{n} W_{\mathcal{C}^\wedge}^j \sum_{i=0}^{r}(-1)^i(q-1)^{r-i}\binom{n-j}{r-i}\binom{j}{i}$$

Since (2) holds, we get

$$\left.\frac{\partial^r f}{\partial y^r}\right|_{x=1,y=0} = \left.\frac{\partial^r g}{\partial y^r}\right|_{x=1,y=0}, \quad 0 \le r \le n$$

By lemma 2 we obtain

$$W_{\mathcal{C}}(x,y) = f(x,y) = g(x,y) = \frac{1}{q^{n-k}}W_{\mathcal{C}^\perp}(x+(q-1)y, x-y).$$

2.5 Derive (1) from (3) or (4)

We only prove that from (3) we can derive (1). Let

$$f(x,y) = W_{\mathcal{C}}(x,y) = \sum_{j=0}^{n} W_{\mathcal{C}}^j x^{n-j}y^j$$

$$g(x,y) = \frac{1}{q^{n-k}}W_{\mathcal{C}^\perp}(x+(q-1)y, x-y)$$

$$= \frac{1}{q^{n-k}}\sum_{j=0}^{n} W_{\mathcal{C}^\perp}^j [x+(q-1)y]^{n-j}(x-y)^j$$

Then both $f(x,y)$ and $g(x,y)$ are homogeneous polynomials of degree n in x, y. For any non-negative integer $r \le n$, by lemma 1 we get

$$\left.\frac{\partial^r f}{\partial y^r}\right|_{x=1,y=1} = r!\sum_{j=0}^{n}\binom{j}{r}W_{\mathcal{C}}^r$$

$$\left.\frac{\partial^r g}{\partial y^r}\right|_{x=1,y=1} = \frac{1}{q^{n-k}}\sum_{j=0}^{n} W_{\mathcal{C}^\wedge}^j\, r!\sum_{i=0}^{r}(-1)^i(q-1)^{r-i}\binom{n-j}{r-i}\binom{j}{i}$$

$$\left.[x+(q-1)y]^{n-j-r+i}(x-y)^{j-i}\right|_{x=1,y=1}$$

$$= r!\,q^{k-r}\sum_{j=0}^{n}(-1)^j(q-1)^{r-j}\binom{n-j}{r-j}W_{\mathcal{C}^\wedge}^j.$$

From (3) we get

2.6 Derive (1) from (5)

If $t = 0$, then (5) reduces to (4), while if $t = r$, then (5) reduces to (3). Since (1) can be derived from (3) or (4), (1) can also be derived from (5).

$$\left.\frac{\partial^r f}{\partial y^r}\right|_{x=1,y=1} = \left.\frac{\partial^r g}{\partial y^r}\right|_{x=1,y=1}, \quad 0 \le r \le n$$

By lemma 2 we obtain $f(x,y)=g(x,y)$, which means that

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

3.0 CONCLUSION

A homogeneous polynomial of degree n in two variables is uniquely determined by its $n+1$ coefficients, and any properly selected $n+1$ points on the range of the polynomial can be used to determined these coefficients. From the proofs in the last section we see that identities (2), (3), (4) and (5) are actually four different groups of conditions that can be used to determine the coefficients of (1), and they can be written respectively in the following four forms:

$$(2') \quad \left.\frac{\partial^r W_{\mathcal{C}}(x,y)}{\partial y^r}\right|_{x=1,y=0} = \left.\frac{\partial^r W_{\mathcal{C}^\perp}(x+(q-1)y, x-y)}{\partial y^r}\right|_{x=1,y=0}$$

$$(3') \quad \left.\frac{\partial^r W_{\mathcal{C}}(x,y)}{\partial y^r}\right|_{x=1,y=1} = \left.\frac{\partial^r W_{\mathcal{C}^\perp}(x+(q-1)y, x-y)}{\partial y^r}\right|_{x=1,y=1}$$

$$(4') \quad \left.\frac{\partial^r W_{\mathcal{C}}(x,y)}{\partial x^r}\right|_{x=1,y=1} = \left.\frac{\partial^r W_{\mathcal{C}^\perp}(x+(q-1)y, x-y)}{\partial x^r}\right|_{x=1,y=1}$$

$$(5') \quad \left.\frac{\partial^r W_{\mathcal{C}}(x,y)}{\partial x^{r-t}\partial y^t}\right|_{x=1,y=1} = \left.\frac{\partial^r W_{\mathcal{C}^\perp}(x+(q-1)y, x-y)}{\partial x^{r-t}\partial y^t}\right|_{x=1,y=1}$$

Therefore more equivalent forms of (1) can be written out in this way.

References

[1] Blahut R. E. 1984. *Theory and Practice of Error Control Codes*. Readings, Mass: Addison Wesley.

[2] Brualdi R. A., V. S. Pless and J. Beissinger. 1988. On the MacWilliams Identities for Linear Codes. *Linear Algebra Appl.* 107: 181-189.

[3] Chang, S. C. and J. K. Wolf. 1980. A Simple Derivation of the MacWilliams' Identity for Linear Codes. *IEEE Tran. On Inform. Theory.* IT-26(4): 476-477.

[4] Goldwasser, J. L. 1997. *Shortened and Punctured Codes and the MacWilliams Identities. Linear Algebra Appl.* 253: 1-13.

[5] Honold, T. 1996. A Proof of MacWilliams' Identity. *J. of Geometry.* 57: 120-122.

[6] MacWilliams, F. J. 1963. A Theorem on the Distribution of Weights in a Systematic Code. *Bell System Tech. J.* 42: 79-94.

[7] MacWilliams, F. J. and N. J. A. Sloane. 1977. *The Theory of Error-Correcting Codes*. New York: North-Holland Publishing Company.

[8] Pless, V. S. 1989. *Introduction to the Theory of Error-Correcting Codes.* 2nd ed. New York：Wiley-Interscience.

[9] Zierler, N. 1973. On the MacWilliams Identity. *J. Combinatorial Theory (A)*. 15: 333-337.