The MacWilliams Identities

Theorem 1 (The Binary MacWilliams Identities). *Let $A(z)$ and $B(z)$ denote the weight enumerators for an (n, k) binary linear code C and its dual code $C^\perp$, i.e.,*

$$A(z) = \sum_{i=0}^{n} A_i z^i \tag{1}$$

$$B(z) = \sum_{j=0}^{n} B_j z^j \tag{2}$$

where A_i denotes the number of words of weight i in C, and B_j denotes the number of words of weight j in $C^\perp$. Then $A(z)$ and $B(z)$ are related by the formula

$$B(z) = \frac{1}{2^k} \sum_{i=0}^{n} A_i (1-z)^i (1+z)^{n-i}. \tag{3}$$

Alternatively, equating coefficients of z^j on both sides of (3), we have

$$B_j = \frac{1}{2^k} \sum_{i=0}^{n} A_i K_{i,j}^{(n)} \qquad \text{for } j = 0, \ldots, n, \tag{4}$$

where $K_{i,j}^{(n)}$ is the coefficient of z^j in $(1-z)^i(1+z)^{n-i}$, i.e.,

$$K_{i,j}^{(n)} = \sum_h (-1)^h \binom{i}{h} \binom{n-i}{j-h}. \tag{5}$$

What (4) says is that the weight enumerator *vectors* $\boldsymbol{a} = (A_0, A_1, \ldots, A_n)$ and $\boldsymbol{b} = (B_0, B_1, \ldots, B_n)$ are related by the formula

$$\boldsymbol{b} = \frac{1}{2^k} \boldsymbol{a} K^{(n)}, \tag{6}$$

where $K^{(n)}$ is the $(n+1) \times (n+1)$ matrix whose (i, j) entry is $K_{i,j}^{(n)}$. For example, with $n = 4$ we have

$$K^{(4)} = \begin{pmatrix} 1 & 4 & 6 & 4 & 1 \\ 1 & 2 & 0 & -2 & -1 \\ 1 & 0 & -2 & 0 & 1 \\ 1 & -2 & 0 & 2 & -1 \\ 1 & -4 & 6 & -4 & 1 \end{pmatrix}.$$

Proof : First, some preliminaries. If $\boldsymbol{x} = (x_1, \ldots, x_m)$ is a binary vector of any length, $|\boldsymbol{x}|$ denotes its Hamming weight, i.e., the number of nonzero components of $\boldsymbol{x}$. In particular, if x is a *scalar*, i.e., $m = 1$, then

$$|x| = \begin{cases} 0 & \text{if } x = 0 \\ 1 & \text{if } x = 1. \end{cases} \tag{7}$$

If $\boldsymbol{x} = (x_1, \ldots, x_m)$ and $\boldsymbol{y} = (y_1, \ldots, y_m)$ are two binary vectors, we define the *inner product* of $\boldsymbol{x}$ and $\boldsymbol{y}$ as follows:

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle = (-1)^{x_1 y_1 + \cdots + x_m y_m}, \tag{8}$$

where $(-1)^0 = 1$, $(-1)^1 = -1$. Thus for example, $\langle 011, 110 \rangle = (-1)^1 = -1$ and $\langle 011, 111 \rangle = (-1)^0 = +1$.

Our proof of the MacWilliams identities is based on two fairly easy technical lemmas about $\langle \boldsymbol{x}, \boldsymbol{y} \rangle$.

Lemma 1. *If C is an (n, k) linear code over $GF(2)$, and if $\boldsymbol{y}$ is an arbitrary n-vector over $GF(2)$, then*

$$\sum_{\boldsymbol{x} \in C} \langle \boldsymbol{x}, \boldsymbol{y} \rangle = \begin{cases} 2^k & \text{if } \boldsymbol{y} \in C^\perp \\ 0 & \text{if } \boldsymbol{y} \notin C^\perp. \end{cases} \tag{9}$$

Proof : If $\boldsymbol{y} \in C^\perp$, then $\langle \boldsymbol{x}, \boldsymbol{y} \rangle = 1$ for all $\boldsymbol{x} \in C$, so that the first alternative holds. If, on the other hand, $\boldsymbol{y} \notin C^\perp$, then there is at least one codeword $\boldsymbol{x}_0 \in C$ such that $\langle \boldsymbol{x}, \boldsymbol{y} \rangle = -1$. Then in the pairing

$$\boldsymbol{x} \leftrightarrow \boldsymbol{x} + \boldsymbol{x}_0,$$

if $\langle \boldsymbol{x}, \boldsymbol{y} \rangle = +1$, then $\langle \boldsymbol{x} + \boldsymbol{x}_0, \boldsymbol{y} \rangle = -1$, and vice-versa, so that in the sum (9), the values $+1$ and -1 occur equally often, which means the sum is zero. ∎

Lemma 2. *Let $\boldsymbol{x}$ be a fixed vector of length n over $GF(2)$, with $|\boldsymbol{x}| = i$, and let V_j denote the set of all binary vectors of length n and weight j. Then*

$$\sum_{\boldsymbol{y} \in V_j} \langle \boldsymbol{x}, \boldsymbol{y} \rangle = K_{i,j}^{(n)}. \tag{10}$$

Proof : Without loss of generality we may assume $\boldsymbol{x}$ has the form

$$\boldsymbol{x} = (\overbrace{11\cdots1}^{i}\ \overbrace{00\cdots0}^{n-i}).$$

There are then exactly $\binom{i}{h}\binom{n-i}{j-h}$ binary vectors $\boldsymbol{y}$ of length n and weight j which share h ones with $\boldsymbol{x}$, and each of these $\boldsymbol{y}$'s has $\langle \boldsymbol{x}, \boldsymbol{y} \rangle = (-1)^h$. Thus

$$\sum_{\boldsymbol{y} \in V_j} \langle \boldsymbol{x}, \boldsymbol{y} \rangle = \sum_h (-1)^h \binom{i}{h} \binom{n-i}{j-h},$$

which, by (5), equals $K_{i,j}^{(n)}$. ▪

Our proof of the MacWilliams Identities is now simply a matter of noting that

$$\sum_{\boldsymbol{y}\in V_j}\sum_{\boldsymbol{x}\in C}\langle \boldsymbol{x},\boldsymbol{y}\rangle = \sum_{\boldsymbol{x}\in C}\sum_{\boldsymbol{y}\in V_j}\langle \boldsymbol{x},\boldsymbol{y}\rangle,$$

and that by Lemma 1,

$$\sum_{\boldsymbol{y}\in V_j}\sum_{\boldsymbol{x}\in C}\langle \boldsymbol{x},\boldsymbol{y}\rangle = \sum_{\boldsymbol{y}\in V_j\cap C^\perp} 2^k = 2^k B_j,$$

while by Lemma 2,

$$\sum_{\boldsymbol{x}\in C}\sum_{\boldsymbol{y}\in V_j}\langle \boldsymbol{x},\boldsymbol{y}\rangle = \sum_{\boldsymbol{x}\in C} K_{|\boldsymbol{x}|,j}^{(n)} = \sum_{i=0}^{n} A_i K_{i,j}^{(n)}.$$

Thus $2^k B_j = \sum_{i=0}^{n} A_i K_{i,j}^{(n)}$, the same as (4). ▪

The MacWilliams identities can be generalized to linear codes over nonbinary alphabets. Here is the generalization. We omit the proof.

Theorem 2 (The q-ary MacWilliams Identities). *Let $A(z)$ and $B(z)$ denote the weight enumerators for an (n,k) q-ary linear code C and its dual code $C^\perp$, i.e.,*

$$A(z) = \sum_{i=0}^{n} A_i z^i \tag{11}$$

$$B(z) = \sum_{j=0}^{n} B_j z^j \tag{12}$$

where A_i denotes the number of words of weight i in C, and B_j denotes the number of words of weight j in $C^\perp$. Then $A(z)$ and $B(z)$ are related by the formula

$$B(z) = \frac{1}{q^k}\sum_{i=0}^{n} A_i (1-z)^i (1+(q-1)z)^{n-i}. \tag{13}$$

Alternatively, equating coefficients of z^j on both sides of (13), we have

$$B_j = \frac{1}{q^k}\sum_{i=0}^{n} A_i K_{i,j}^{(n)} \qquad \text{for } j = 0,\ldots,n, \tag{14}$$

where $K_{i,j}^{(n)}$ is the coefficient of z^j in $(1-z)^i(1+(q-1)z)^{n-i}$, i.e.,

$$K_{i,j}^{(n)} = \sum_{h}(-1)^h \binom{i}{h}\binom{n-i}{j-h}(q-1)^{j-h}. \tag{15}$$