A PROOF OF MACWILLIAMS' IDENTITY

In memoriam Giuseppe Tallini

Thomas Honold

As shown by MacWilliams the Hamming weight enumerator of a linear code $C$ over a finite field can be expressed by the weight enumerator of its dual code $C^\perp$. A short inductive proof of this formula is given which uses only elementary linear algebra.

Let $C$ be a linear $[n, k]$-code over the finite field $\mathbb{F}_q$ with $q$ elements, i.e. a $k$-dimensional subspace of $\mathbb{F}_q^n = \{x = (x_1, \ldots, x_n); x_i \in \mathbb{F}_q\}$. The Hamming weight of $x \in \mathbb{F}_q^n$ is defined by $\gamma(x) := |\{i; x_i \neq 0\}|$. For any subset $S \subset \mathbb{F}_q^n$ we denote by $A_S(Z)$ its Hamming weight enumerator, i.e. $A_S(Z) := \sum_{0 \leq i \leq n} A_i Z^i \in \mathbb{C}[Z]$ where $A_i = |\{x \in S; \gamma(x) = i\}|$. Similarly, for $S \subset \mathbb{F}_q^n$ let

$$B_S(Z) := (1 + (q-1)Z)^n A_S\left(\frac{1-Z}{1+(q-1)Z}\right).$$

The polynomial $B_S(Z) \in \mathbb{C}[Z]$ is often called MacWilliams transform of $A_S(Z)$. One should note that $B_S(Z)$ as defined here not only depends on $A_S(Z)$ but also on the dimension $n$ of the underlying space $\mathbb{F}_q^n$.

Obviously, $A_{S\cup T}(Z) = A_S(Z) + A_T(Z)$ and $B_{S\cup T}(Z) = B_S(Z) + B_T(Z)$ holds for disjoint subsets $S, T \subset \mathbb{F}_q^n$.

As shown by MacWilliams [6] the weight enumerators of $C$ and its dual code $C^\perp = \{x \in \mathbb{F}_q^n; x_1y_1 + \cdots + x_ny_n = 0 \text{ for all } y \in C\}$ are related by the formula

$$A_{C^\perp}(Z) = \frac{1}{q^k} B_C(Z).$$

The classical proof (cf. [7, Ch. 5] or [2, Kap. 8.8]) is by an application of the Poisson summation formula to the function $f: \mathbb{F}_q^n \rightarrow \mathbb{C}[Z], x \rightarrow Z^{\gamma(x)}$, and thus involves character...
theory of the abelian group \((\mathbb{F}_q^n, +)\). It can be generalized to the so-called complete weight enumerator of a linear code \([7, \text{Ch. 5}]\) and to weight enumerators of codes over certain finite commutative rings \([3, 4, 5]\). Combinatorial proofs of equivalent forms of (2) have also been given; see \([1]\) and \([8]\).

Below I’ll give a short proof of (2) by induction on the length \(n\) of \(C\). The code \(C\) is called **decomposable**, if up to a permutation of coordinates it can be written as \(C = \{(c', c'') \mid c' \in C_1, c'' \in C_2\}\) with linear codes \(C_1, C_2\) of positive length. We denote this by \(C = C_1 \times C_2\).

Clearly, \(C = C_1 \times C_2\) implies \(C^\perp = C_1^\perp \times C_2^\perp\) and

\[
A_C(Z) = A_{C_1}(Z)A_{C_2}(Z), \tag{3}
\]

\[
B_C(Z) = B_{C_1}(Z)B_{C_2}(Z). \tag{4}
\]

**Proof of (2):** If \(n = 1\), either \(C = \{0\}\) or \(C = \mathbb{F}_q\) with weight enumerators 1 and \(1 + (q-1)Z\) respectively. In this case one verifies (2) directly. For instance, if \(C = \mathbb{F}_q\):

\[
\frac{1}{q^k} B_C(Z) = \frac{1}{q} \left(1 + (q-1)Z\right) \left(1 + (q-1)\frac{1-Z}{1+(q-1)Z}\right) = 1 = A_{C^\perp}(Z). \tag{5}
\]

If \(n > 1\) we may assume that \(C\) is indecomposable; otherwise the assertion follows by induction and multiplicativity of both sides in (2), (3) and (4). Let \(C_0 := \{c \in C \mid c_n = 0\}\), \(C_1 := C \setminus C_0\). Since \(C\) is indecomposable, neither \(C\) nor \(C^\perp\) contains a codeword of weight 1. Thus there is \(a = (a_1, \ldots, a_{n-1}, 1) \in C\) such that \(C = C_0 \oplus \langle a \rangle\), and the projection map \(\pi : (x_1, \ldots, x_n) \to (x_1, \ldots, x_{n-1})\) restricts to an injective map to an injective map from \(C\) into \(\mathbb{F}_q^{n-1}\). Therefore,

\[
A_{\pi(C)}(Z) = A_{\pi(C_0)}(Z) + A_{\pi(C_1)}(Z)
= A_{\pi(C_0)}(Z) + A_{C_1}(Z)/Z, \tag{6}
\]

\[
B_{\pi(C)}(Z) = B_{\pi(C_0)}(Z) + \frac{(1 + (q-1)Z)^n}{1-Z}A_{C_1}\left(\frac{1-Z}{1+(q-1)Z}\right)
= B_{\pi(C_0)}(Z) + (1-Z)^{-1}B_{C_1}(Z). \tag{7}
\]

Now \(C^\perp\) is the disjoint union of the sets \(\{(b', 0) \mid b' \in \pi(C)\} \) and \(\{(b', b_n) \mid b' \in \pi(C_0)^\perp \setminus \pi(C)\}, b_n = -a_1b_1 - \cdots - a_{n-1}b_{n-1}(\neq 0)\), and therefore

\[
A_{C^\perp}(Z) = A_{\pi(C)^\perp}(Z) + Z \left(A_{\pi(C_0)^\perp}(Z) - A_{\pi(C_1^\perp)}(Z)\right). \tag{8}
\]

Applying the inductive hypothesis and taking (7) as well as \(\dim \pi(C) = k\), \(\dim \pi(C_0) = k-1\) into account, we find

\[
A_{C^\perp}(Z) = \frac{1-Z}{q^k} B_{\pi(C)}(Z) + \frac{Z}{q^{k-1}} B_{\pi(C_0)}(Z)
= \frac{1}{q^k} \left((1 + (q-1)Z)B_{\pi(C_0)}(Z) + B_{C_1}(Z)\right)
= \frac{1}{q^k} (B_{C_0}(Z) + B_{C_1}(Z))
= \frac{1}{q^k} B_C(Z). \tag{9}
\]