Two Fundamental Theorems of MacWilliams: The Classical Case over Finite Fields

Jay A. Wood

Department of Mathematics
Western Michigan University
Kalamazoo, Michigan
jay.wood@wmich.edu

Huazhong Normal University, Wuhan, Hubei
June 22, 2011
Acknowledgments

- I am pleased to be visiting the city of Wuhan, and I thank my host, Professor Hongwei Liu, for the invitation and for his hospitality.
- I thank the Hubei Province Education Department for sponsoring the program and for their financial support.
Florence Jessie MacWilliams

- 1917–1990
- 1962 doctoral dissertation under Andrew Gleason at Harvard
- “Combinatorial Problems of Elementary Abelian Groups”
- Three sections:
  - Extension theorem on isometries
  - The MacWilliams identities
  - Coverings
Two Fundamental Theorems

- Extension theorem on isometries
- The MacWilliams identities

I will start with the MacWilliams identities.
Some Notation

- Finite field $\mathbb{F}_q$ with $q$ elements; $q$ a prime power.
- Dot product on $\mathbb{F}_q^n$ (all operations in $\mathbb{F}_q$):
  \[ x \cdot y = \sum x_i y_i, \]
  for $x = (x_1, \ldots, x_n), \ y = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$.
- It is a nondegenerate, symmetric bilinear form.
Definitions

- The Hamming weight $\text{wt}(x)$ of a vector $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ is the number of nonzero entries in $x$.
- A linear code over $\mathbb{F}_q$ of dimension $k$ and length $n$ is a $k$-dimensional vector subspace $C \subset \mathbb{F}_q^n$.
- If $C \subset \mathbb{F}_q^n$ is a linear code, then the dual code is

$$C^\perp = \{ y \in \mathbb{F}_q^n : x \cdot y = 0, \text{ all } x \in C \}.$$
Given a linear code $C \subset \mathbb{F}_q^n$, the \textit{Hamming weight enumerator} of $C$ is the two-variable polynomial (generating function):

$$W_C(X, Y) = \sum_{x \in C} X^{n-\text{wt}(x)} Y^{\text{wt}(x)}.$$

$$W_C(X, Y) = \sum_{i=0}^{n} A_i X^{n-i} Y^i,$$

where $A_i$ is the number of elements of $C$ of weight $i$. 

**Hamming Weight Enumerators**
“Standard Properties” of Dual Codes

1. $C^\perp \subset \mathbb{F}_q^n$.
2. $C^\perp$ is a linear code.
3. $\dim C + \dim C^\perp = n$; or $|C||C^\perp| = |\mathbb{F}_q^n|$.
4. $(C^\perp)^\perp = C$.
5. The MacWilliams identities hold:

$$W_{C^\perp}(X, Y) = \frac{1}{|C|} W_C(X + (q - 1)Y, X - Y).$$
Proofs

- The first four items are obvious or follow from basic linear algebra of nondegenerate forms over fields.
- The proof of the MacWilliams identities given will be based on character theory and the Poisson summation formula.
- The proof is due to Gleason.
Let $(G, +)$ be a finite abelian group.

A character $\pi$ of $G$ is a group homomorphism $\pi : (G, +) \to (\mathbb{C}^\times, \times)$, where $(\mathbb{C}^\times, \times)$ is the multiplicative group of nonzero complex numbers.

Example: let $G = \mathbb{Z}/n\mathbb{Z}$ be the integers modulo $n$.

For any integer $a$, $\pi_a(x) = \exp(2\pi i ax/n)$, $x \in G$, is a character of $G$.

$\pi_a = \pi_b$ if and only if $a \equiv b \mod n$. 
Character Group

- The set \( \hat{G} \) of all characters of \( G \) is itself a finite abelian group under pointwise multiplication of functions.
- \( \hat{G} \) is called the character group.
- \( \hat{G} \cong G \) (not naturally); in particular, \( |\hat{G}| = |G| \).
- \( \hat{G} \cong G \) (naturally).
- As elements of the vector space of all functions from \( G \) to \( \mathbb{C} \), the characters are linearly independent.
Two Useful Formulas

\[ \sum_{x \in G} \pi(x) = \begin{cases} |G|, & \pi = 1, \\ 0, & \pi \neq 1. \end{cases} \]

\[ \sum_{\pi \in \hat{G}} \pi(x) = \begin{cases} |G|, & x = 0, \\ 0, & x \neq 0. \end{cases} \]
Fourier Transform

- Given a function $f : G \to V$, with $V$ a complex vector space, its Fourier transform is a function $\hat{f} : \hat{G} \to V$ defined by

$$\hat{f}(\pi) = \sum_{x \in G} \pi(x)f(x), \quad \pi \in \hat{G}.$$  

- Fourier inversion:

$$f(x) = \frac{1}{|G|} \sum_{\pi \in \hat{G}} \pi(-x)\hat{f}(\pi), \quad x \in G.$$
Poisson Summation Formula

- For a subgroup $H \subset G$, define its annihilator $(\hat{G} : H) = \{ \pi \in \hat{G} : \pi(H) = 1 \}$.
- $| (\hat{G} : H) | = |G|/|H|$.
- For a subgroup $H \subset G$ and any $a \in G$,
  \[ \sum_{h \in H} f(a + h) = \frac{1}{| (\hat{G} : H) |} \sum_{\pi \in (\hat{G} : H)} \pi(-a) \hat{f}(\pi). \]
- In particular, for a subgroup $H \subset G$,
  \[ \sum_{h \in H} f(h) = \frac{1}{| (\hat{G} : H) |} \sum_{\pi \in (\hat{G} : H)} \hat{f}(\pi). \]
Application to MacWilliams Identities (a)

- Let $G = \mathbb{F}_q^n$, an abelian group under addition.
- Let $H = C$, a linear code.
- Let $V = \mathbb{C}[X, Y]$, a complex vector space.
- Let $f : G \to V$ be

$$f(x) = X^{n-\text{wt}(x)} Y^{\text{wt}(x)}.$$
Application to MacWilliams Identities (b)

- Every character of $G = \mathbb{F}_q^n$ has the form $\pi_a$, for some $a \in \mathbb{F}_q^n$, with

$$\pi_a(x) = \exp\left(2\pi i \text{Tr}(a \cdot x)/p\right), \quad x \in \mathbb{F}_q^n,$$

where $\text{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ is the absolute trace map to the prime field. View $\mathbb{F}_p$ as $\mathbb{Z}/p\mathbb{Z}$.

- $\pi_a \in (\hat{G} : H)$ if and only if $a \in C^\perp$.

- $| (\hat{G} : H) | = | C^\perp |$. 
Application to MacWilliams Identities (c)

- For $f(x) = X^{n-\text{wt}(x)} Y^{\text{wt}(x)}$, 

$$ \hat{f}(\pi_a) = (X + (q - 1)Y)^{n-\text{wt}(a)}(X - Y)^{\text{wt}(a)}.$$ 

- This requires some manipulations and use of $\sum \pi(x)$ formulas. (Next slide.)

- Recognize $\hat{f}(\pi_a)$ as summand of $W_{C^\perp}(X + (q - 1)Y, X - Y)$.

- Reverse roles of $C$ and $C^\perp$. 
Idea of Manipulation

Let \( n = 1 \), \( f(x) = X^{1-\text{wt}(x)} Y^{\text{wt}(x)} \).

\[
\hat{f}(\pi_a) = \sum_{x \in \mathbb{F}_q} \pi_a(x) X^{1-\text{wt}(x)} Y^{\text{wt}(x)}
\]

\[
= X + \sum_{x \neq 0} \pi_a(x) Y
\]

\[
= \begin{cases} 
X + (q - 1)Y, & a = 0, \\
X - Y, & a \neq 0,
\end{cases}
\]

\[
= (X + (q - 1)Y)^{1-\text{wt}(a)} (X - Y)^{\text{wt}(a)}
\]
Example, $n = 2$

- Let $C_2 \subset \mathbb{F}_2^2$ be
  \[ C_2 = \{00, 11\}. \]

- $C_2$ is self-dual; i.e., $C_2^\perp = C_2$.

- $W_{C_2}(X, Y) = X^2 + Y^2$. Call this $S$.

- In a binary self-dual code, all elements have even weight.
Example, $n = 8$

- Let $E_8 \subset F_2^8$ be spanned by the rows of

\[
\begin{array}{cccccccc}
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
\end{array}
\]

- $E_8$ is self-dual. Also, all elements $x$ of $E_8$ satisfy $wt(x) \equiv 0 \mod 4$. $E_8$ is *doubly-even*.

- $W_{E_8}(X, Y) = X^8 + 14X^4Y^4 + Y^8$. Call this $T$. 
Extended Golay Code (1949)

- There is a famous binary code $G_{24}$ of length 24, dimension 12, which is self-dual, doubly-even, with minimum weight 8.

- Weight enumerator:

$$W_{G_{24}}(X, Y) = X^{24} + 759X^{16}Y^{8} + 2576X^{12}Y^{12} + 759X^{8}Y^{16} + Y^{24}. $$
Gleason’s Theorem (1970)

- The weight enumerator of any binary self-dual code is a polynomial expression in the weight enumerators $S$ and $T$ of $C_2$ and $E_8$.
- $W_{G_{24}}(X, Y) = T^3 + \frac{21}{8}(2S^8 T - S^4 T^2 - S^{12})$.
- The weight enumerator of any binary self-dual, doubly-even code is a polynomial expression in the weight enumerators of $E_8$ and $G_{24}$. So, $n \equiv 0 \mod 8$.
Code Equivalence

- When should two linear codes be considered the same?
- Monomial equivalence (external)
- Linear isometries (internal)
- These notions are the same—MacWilliams extension theorem
Monomial equivalence

- Still work over a finite field $\mathbb{F}_q$.
- A permutation $\sigma$ of $\{1, \ldots, n\}$ and invertible elements $u_1, \ldots, u_n$ in $\mathbb{F}_q$ determine a monomial transformation $T : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ by

$$T(x_1, \ldots, x_n) = (u_1 x_{\sigma(1)}, \ldots, u_n x_{\sigma(n)}).$$

- Two linear codes $C_1, C_2 \subset \mathbb{F}_q^n$ are monomially equivalent if there exists a monomial transformation $T$ such that $C_2 = T(C_1)$. 
Linear Isometries

- Still work with the Hamming weight on $\mathbb{F}_q^n$.
- A linear isomorphism $f : C_1 \to C_2$ between linear codes $C_1, C_2 \subset \mathbb{F}_q^n$ is an isometry if it preserves Hamming weight: $\text{wt}(f(x)) = \text{wt}(x)$, for all $x \in C_1$.
- If $T$ is a monomial transformation with $C_2 = T(C_1)$, then the restriction of $T$ to $C_1$ is an isometry.
- Is the converse true? Does every linear isometry come from a monomial transformation?
MacWilliams Extension Theorem

Assume $C_1$, $C_2$ are linear codes in $\mathbb{F}_q^n$. If a linear isomorphism $f : C_1 \rightarrow C_2$ preserves Hamming weight, then $f$ extends to a monomial transformation of $\mathbb{F}_q^n$.

- MacWilliams (1961); Bogart, Goldberg, Gordon (1978)
Proof 1 (a)

- Fix a basis for $C_1$. Write basis vectors as rows of a matrix $G_1$, called a generator matrix for $C_1$.
- Apply $f$ to those basis vectors. Get a generator matrix $G_2$ for $C_2$.
- It will suffice to show that the columns of $G_2$ are the same as those of $G_1$, up to a permutation and scaling by invertible elements.
- So, count the number of columns in each scale class.
Proof 1 (b)

- Every element $c$ of $C_1$ has the form $xG_1$, for some $k$-tuple $x = (x_1, \ldots, x_k)$. Here, $k = \dim C_1$. Then, $f(c)$ in $C_2$ has the form $xG_2$.
- The Hamming weight of $xG_i$ counts the number of nonzero entries. The entries are the dot products of $x$ with the columns of $G_i$.
- Form matrix $M$ with rows and columns indexed by scale classes of $k$-tuples. Entry of $M$ at position $x, y$ is 1 if $x \cdot y \neq 0$, and it is 0 if $x \cdot y = 0$.
- Key computation: $M$ is invertible.
Proof 1 (c)

- Count the scale classes of columns of $G_i$. Put results into a column vector $r_i$.
- Multiply $M r_i$. The result is the list of Hamming weights of the elements of $C_i$.
- Since $f$ preserves Hamming weight and $M$ is invertible, we get $r_1 = r_2$, as desired.
Proof 2 (a)

- View $C_i$ as the image of a linear map $g_i : \mathbb{F}_q^k \rightarrow \mathbb{F}_q^n$, with $g_2 = f \circ g_1$.
- Component functionals $g_i = (g_{i,1}, \ldots, g_{i,n})$.
- Denote the characters of $\mathbb{F}_q$ by $\pi_a$, $a \in \mathbb{F}_q$.
- Observe, for $x \in \mathbb{F}_q^k$:

$$\text{wt}(g_i(x)) = n - \sum_{j=1}^{n} \frac{1}{q} \sum_{a \in \mathbb{F}_q} \pi_a(g_{i,j}(x)).$$
Proof 2 (b)

- Weight preservation yields, for all \( x \in \mathbb{F}_q^k \),

\[
\sum_{j=1}^{n} \sum_{a \in \mathbb{F}_q} \pi_a(g_{1,j}(x)) = \sum_{l=1}^{n} \sum_{b \in \mathbb{F}_q} \pi_b(g_{2,l}(x)).
\]

- This is an equation of characters of \( \mathbb{F}_q^k \).

- Use linear independence of characters to match up terms (with care).
What’s to Come?

- Virtually all the arguments given in this lecture generalize to the context of linear codes defined over finite Frobenius rings, i.e., to left submodules $C \subset R^n$, where $R$ is a finite Frobenius ring.
- The details of these generalizations are the subject of subsequent lectures.