Linear Codes over Finite Rings and Modules

Jay A. Wood

Department of Mathematics
Western Michigan University
http://homepages.wmich.edu/∼jwood

Central China Normal University
Wuhan, Hubei
May 4, 2018

3. Fourier transform and MacWilliams identities

- Fourier transform
- MacWilliams identities
- Making identifications

Additive codes

- Let A be a finite abelian group (additive notation); A will be a module later.
- Recall: an **additive code** of length n over A is an additive subgroup $C \subseteq A^n$.
- The **Hamming weight** on A, $\mathrm{wt} : A \to \mathbb{C}$, is

$$\mathrm{wt}(a) = \begin{cases} 0, & a = 0, \\ 1, & a \neq 0. \end{cases}$$

- Extend to A^n by $\mathrm{wt}(a_1, \ldots, a_n) = \sum \mathrm{wt}(a_i)$.

Hamming weight enumerator

- For an additive code $C \subseteq A^n$, define the **Hamming weight enumerator** of C by

$$\mathrm{hwe}_C(X, Y) = \sum_{x \in C} X^{n-\mathrm{wt}(x)} Y^{\mathrm{wt}(x)}.$$

- $\mathrm{hwe}_C(X, Y) = \sum_{i=0}^{n} A_i X^{n-i} Y^i$, where A_i is the number of codewords in C of Hamming weight i.

Complete weight enumerator

- The **complete weight enumerator** of C is a homogeneous polynomial in $\mathbb{C}[Z_a : a \in A]$:

$$\mathrm{cwe}_C((Z_a)) = \sum_{x \in C} \prod_{i=1}^{n} Z_{x_i}.$$

- Over $A = \mathbb{F}_2$, $\mathrm{cwe}_C = \mathrm{hwe}_C$, with $Z_0 = X$ and $Z_1 = Y$.

MacWilliams Identities

- The MacWilliams identities express the Hamming or complete weight enumerators of C in terms of those of its dual code $(\widehat{A}^n : C)$.
- The expression involves a linear change of variables.
- The Hamming case, with $C^\perp = (\widehat{A}^n : C)$:

$$\mathrm{hwe}_C(X, Y) = \frac{1}{|C^\perp|} \mathrm{hwe}_{C^\perp}(X + (|A| - 1)Y, X - Y).$$

- Proof involves the Fourier transform.

Summation formulas

- Need multiplicative form of characters.
- For $\pi \in \widehat{A}$,

$$\sum_{a \in A} \pi(a) = \begin{cases} |A|, & \pi = 1, \\ 0, & \pi \neq 1. \end{cases}$$

- For $a \in A$,

$$\sum_{\pi \in \widehat{A}} \pi(a) = \begin{cases} |A|, & a = 0, \\ 0, & a \neq 0. \end{cases}$$

Fourier transform

- Given a function $f : A \to V$, V a complex vector space. Define its **Fourier transform** $\hat{f} : \widehat{A} \to V$ by

$$\hat{f}(\pi) = \sum_{a \in A} \pi(a) f(a), \quad \pi \in \widehat{A}.$$

- $\widehat{\ } : F(A, V) \to F(\widehat{A}, V)$.
- Invert:

$$f(a) = \frac{1}{|A|} \sum_{\pi \in \widehat{A}} \pi(-a) \hat{f}(\pi), \quad a \in A.$$

Poisson summation formula

Let B be any subgroup of A, and let $f : A \to V$. Then for any $a \in A$,

$$\sum_{b \in B} f(a+b) = \frac{1}{|(\widehat{A} : B)|} \sum_{\pi \in (\widehat{A}:B)} \pi(-a)\hat{f}(\pi).$$

If $a = 0$, then

$$\sum_{b \in B} f(b) = \frac{1}{|(\widehat{A} : B)|} \sum_{\pi \in (\widehat{A}:B)} \hat{f}(\pi).$$

A Fourier transform example

- Suppose V is a complex algebra.
- Suppose $f : A^n \to V$ has the form

$$f(a_1, \ldots, a_n) = \prod_{i=1}^{n} f_i(a_i),$$

where $f_i : A \to V$.

- Then

$$\hat{f}(\pi_1, \ldots, \pi_n) = \prod_{i=1}^{n} \hat{f}_i(\pi_i).$$

Complete weight enumerator

- $V = \mathbb{C}[Z_a : a \in A]$, a complex algebra.
- $f : A^n \to V$,

$$f(a_1, \ldots, a_n) = \prod_{i=1}^{n} Z_{a_i}.$$

- Then

$$\hat{f}(\pi_1, \ldots, \pi_n) = \prod_{i=1}^{n} \left(\sum_{a_i \in A} \pi_i(a_i) Z_{a_i} \right)$$

MacWilliams identities from Poisson summation formula

- Poisson:

$$\sum_{b\in B} f(b) = \frac{1}{|(\widehat{A} : B)|} \sum_{\pi\in(\widehat{A}:B)} \hat{f}(\pi).$$

- Replace A by A^n, B by additive code C, $(\widehat{A} : B)$ by dual code $(\widehat{A^n} : C)$.

MacWilliams identities: complete weight enumerator

- $Z = (Z_a)_{a \in A}$; $f(a_1, \ldots, a_n) = \prod_{i=1}^{n} Z_{a_i}$.
- Complete weight enumerator:

$$\mathrm{cwe}_C(Z) = \sum_{x \in C} f(x) = \sum_{a \in C} \prod_{i=1}^{n} Z_{a_i}.$$

- MacWilliams identities:

$$\mathrm{cwe}_C(Z) = \frac{1}{|(\widehat{A}^n : C)|} \mathrm{cwe}_{(\widehat{A}^n : C)}\Big(\sum_{a \in A} \pi(a) Z_a\Big).$$

Specialize to Hamming weight enumerator

- Recall $\mathrm{hwe}_C(X, Y) = \sum_{x \in C} X^{n-\mathrm{wt}(x)} Y^{\mathrm{wt}(x)}$.
- Specialize $\mathbb{C}[Z_a : a \in A] \to \mathbb{C}[X, Y]$, $Z_0 \mapsto X$, $Z_a \mapsto Y$ for $a \neq 0$. Then $\mathrm{cwe}_C(Z) \mapsto \mathrm{hwe}_C(X, Y)$.
- What happens to $\mathrm{cwe}_{(\widehat{A}^n : C)}(\sum_{a \in A} \pi(a) Z_a)$ on the right side?

Specialization

$$\sum_{a\in A}\pi(a)Z_a = \pi(0)Z_0 + \sum_{a\neq 0}\pi(a)Z_a$$

$$\mapsto X + \left(\sum_{a\neq 0}\pi(a)\right) Y$$

$$= \begin{cases} X + (|A|-1)Y, & \text{if } \pi = 1, \\ X - Y, & \text{if } \pi \neq 1. \end{cases}$$

MacWilliams identities: Hamming weight enumerator

$$\mathrm{cwe}_C(Z) = \frac{1}{|(\widehat{A}^n : C)|}\,\mathrm{cwe}_{(\widehat{A}^n:C)}\Big(\sum_{a\in A}\pi(a)Z_a\Big)$$

specializes to

$$\mathrm{hwe}_C(X,Y) = \frac{1}{|C^\perp|}\,\mathrm{hwe}_{C^\perp}(X+(|A|-1)Y, X-Y),$$

where $C^\perp = (\widehat{A}^n : C)$.

Summary of good duality properties: additive codes

- Given an additive code $C \subseteq A^n$.
- Dual $(\widehat{A}^n : C) \subseteq \widehat{A}^n$ is an additive code over $\widehat{A}$.
- Double annihilator: $(A^n : (\widehat{A}^n : C)) = C$.
- Size: $|C| \cdot |(\widehat{A}^n : C)| = |A^n|$.
- The MacWilliams identities.

Good duality properties: linear codes

- Given left R-linear code $C \subseteq A^n$.
- Dual $(\widehat{A}^n : C) \subseteq \widehat{A}^n$ is a right R-linear code over $\widehat{A}$.
- Double annihilator: $(A^n : (\widehat{A}^n : C)) = C$.
- Size: $|C| \cdot |(\widehat{A}^n : C)| = |A^n|$.
- The MacWilliams identities.

Identifications

- Over finite fields, code C and its dual $C^{\perp}$ both belonged to $\mathbb{F}^n$.
- For linear codes, is it possible to identify $(\widehat{A}^n : C)$ with a submodule of A^n?
- We will focus on the case of a ring alphabet: $A = R$.
- Suppose $\widehat{R} \cong R$ as one-sided modules.

Generating characters

- Suppose $\psi : R \to \widehat{R}$ is an isomorphism of left R-modules.
- Then $\varrho = \psi(1)$ generates $\widehat{R}$ as a left R-module.
- Indeed, any $\varpi \in \widehat{R}$ has the form $\varpi = \psi(r) = \psi(r1) = r\psi(1) = r\varrho$.
- Note that $\varpi(s) = (r\varrho)(s) = \varrho(sr)$, for $s \in R$.
- Call any generator ϱ a left **generating character** of R.

A key feature of a generating character

- Suppose ϱ is a left generating character of R.
- Claim: $\ker \varrho$ contains no nonzero left ideals of R.
- Fix $r \in R$ such that $sr \in \ker \varrho$ for all $s \in R$.
- Then $0 = \varrho(sr) = (r\varrho)(s) = \psi(r)(s)$ for all $s \in R$.
- This says that $\psi(r)$ is the zero character in $\widehat{R}$.
- Because ψ is injective, we have $r = 0$.

More identifications

- Suppose R has left generating character ϱ.
- Dot product on R^n: $y \cdot x = \sum_{i=1}^{n} y_i x_i \in R$.
- Define $\psi : R^n \to \widehat{R}^n$, $x \mapsto \psi_x$:

$$\psi_x(y) = \varrho(y \cdot x), \quad y \in R^n.$$

- Then ψ is an isomorphism of left R-modules.
- $\psi_{rx}(y) = \varrho(y \cdot rx) = \varrho(yr \cdot x) = \psi_x(yr) = (r\psi_x)(y)$.

Character annihilator vs. dot product

- Recall: $\psi_x(y) = \varrho(y \cdot x), \quad y \in R^n$.
- Additive subgroup $C \subseteq R^n$. Under ψ, $(\widehat{R}^n : C)$ corresponds to $r_\varrho(C) = \{x \in R^n : \varrho(C \cdot x) = 0\}$.
- Set $r(C) = \{x \in R^n : C \cdot x = 0\}$.
- $r(C) \subseteq r_\varrho(C)$ in general.
- $r(C) = r(RC) = r_\varrho(RC) \subseteq r_\varrho(C)$ in general.
- Important: $r(C) = r_\varrho(C)$ when C is a left submodule, as $C \cdot x$ is a left ideal in $\ker \varrho$.

MacWilliams identities: complete weight enumerator

For a left linear code $C \subseteq R^n$, with $\widehat{R} \cong R$:

$$\begin{aligned} \mathrm{cwe}_C(Z) &= \frac{1}{|r(C)|}\,\mathrm{cwe}_{r(C)}\Big(\sum_{b\in R}\psi_a(b)Z_b\Big) \\ &= \frac{1}{|r(C)|}\,\mathrm{cwe}_{r(C)}\Big(\sum_{b\in R}\rho(ba)Z_b\Big). \end{aligned}$$

(Need multiplicative form ρ of ϱ.)

MacWilliams identities: Hamming weight enumerator

For a left linear code $C \subseteq R^n$, with $\widehat{R} \cong R$:

$$\mathrm{hwe}_C(X, Y) = \frac{1}{|r(C)|} \mathrm{hwe}_{r(C)}(X + (|R| - 1)Y, X - Y).$$

Next steps

- When is $R \cong \widehat{R}$?
- How does one construct a generating character?
- That, plus more, in Lecture 4.