Character-Theoretic Tools for Studying Linear Codes over Rings and Modules

Jay A. Wood

Department of Mathematics
Western Michigan University
http://sites.google.com/a/wmich.edu/jaywood

Algebraic Methods in Coding Theory
CIMPA School
Ubatuba, Brazil
July 4, 2017

2. Additive Codes and Characters

- Definitions
- Properties
- Fourier transform
- MacWilliams identities
- Exercises throughout

Additive codes

- Let A be a finite abelian group (additive notation); A will be a module later.
- 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.

How to form a dual code?

- We would like to form a dual code, but there is no dot product immediately available.
- Form a dual code abstractly!

Characters

- A **character** of A is a group homomorphism

$$\pi : A \to \mathbb{C}^\times,$$

  where $\mathbb{C}^\times$ is the multiplicative group of nonzero complex numbers: $\pi(a+b) = \pi(a)\pi(b)$, $a, b \in A$.
- *Representation theory: π is the character of a 1-dimensional complex representation of A. Because A is abelian, every irreducible complex representation of A is 1-dimensional.*

Character group

- The set $\widehat{A}$ of all characters of A is a multiplicative abelian group under pointwise multiplication.

$$(\pi\psi)(a) = \pi(a)\psi(a), \quad a \in A, \quad \pi, \psi \in \widehat{A}.$$

- Exercise: every character of $\mathbb{Z}/k\mathbb{Z}$ has the form $\rho_b(a) = \exp(2\pi iab/k)$, $a \in \mathbb{Z}/k\mathbb{Z}$, for some $b \in \mathbb{Z}/k\mathbb{Z}$. [What is $\rho(1)$?]
- Thus, $(\mathbb{Z}/k\mathbb{Z})\widehat{\ } \cong \mathbb{Z}/k\mathbb{Z}$, via $\rho_b \longleftrightarrow b$.

Additive form of character group

- Original, multiplicative form: $\widehat{A} = \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{C}^{\times})$.
- Additive version: $\widehat{A} \cong \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})$.
- $\varrho \in \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})$ corresponds to $\rho \in \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{C}^{\times})$ by $\rho(a) = \exp(2\pi i \varrho(a))$.
- $\rho(a+b) = \rho(a)\rho(b)$, while $\varrho(a+b) = \varrho(a) + \varrho(b)$.

Duality functor

- Pontryagin duality: $A \mapsto \widehat{A}$
- Exact contravariant functor:

$$0 \to A_1 \to A_2 \to A_3 \to 0$$

induces

$$0 \to \widehat{A}_3 \to \widehat{A}_2 \to \widehat{A}_1 \to 0.$$

- $\widehat{A} \cong A$, but not naturally. (*Uses fundamental theorem of finitely generated abelian groups.*)
- $\widehat{\widehat{A}} \cong A$, naturally: $a \mapsto (\pi \mapsto \pi(a))$.
- $(A \times B)\widehat{\ } \cong \widehat{A} \times \widehat{B}$.

Annihilators

- Let $B \subseteq A$ be any subgroup.
- Define the **annihilator** $(\widehat{A} : B)$:

$$(\widehat{A} : B) = \{\rho \in \widehat{A} : \rho(B) = 1\} = \{\varrho \in \widehat{A} : \varrho(B) = 0\}.$$

- $(\widehat{A} : B) \cong (A/B)\widehat{\ }$.
- $|B| \cdot |(\widehat{A} : B)| = |A|$.
- Double annihilator: $(A : (\widehat{A} : B)) = B$.

Application to additive codes

- Let A be a finite abelian group, and let $C \subseteq A^n$ be an additive code.
- View $C \subseteq A^n$ as an example of "$B \subseteq A$".
- The **dual code** of $C \subseteq A^n$ is the annihilator $(\widehat{A}^n : C) \subseteq \widehat{A}^n$.

Good duality properties

- 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. (Coming next.)

Two weight enumerators

- The Hamming weight enumerator of C is

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

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

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

MacWilliams Identities

- The MacWilliams identities express the Hamming or complete weight enumerators of C in terms of those of its dual code $(A^n : C)$.
- 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

$$
\begin{aligned}
\sum_{a \in A} \pi(a) Z_a &= \pi(0) Z_0 + \sum_{a \neq 0} \pi(a) Z_a \\
&\mapsto X + \left(\sum_{a \neq 0} \pi(a) \right) Y \\
&= \begin{cases} X + (|A| - 1) Y, & \text{if } \pi = 1, \\ X - Y, & \text{if } \pi \neq 1. \end{cases}
\end{aligned}
$$

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

Next steps

- What happens when A is a left module over a finite ring R and $C \subseteq A^n$ is a linear code?
- Is the dual code $(\widehat{A^n} : C)$ linear?
- What duality properties hold?
- If $A = R$, can $(\widehat{R^n} : C)$ be expressed in terms of the dot product on R^n?