Linear Codes from the Axiomatic Viewpoint

Jay A. Wood

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

Noncommutative rings and their applications, IV
University of Artois, Lens
June 8, 2015

2. MacWilliams identities

- Additive codes
- Good duality properties
- Poisson summation formula
- MacWilliams identities
- Making identifications over Frobenius rings

Additive codes

- Let A be a finite abelian group. (Later, a module.)
- An **additive code** over A is an additive subgroup $C \subseteq A^n$.
- Think of $\widehat{A} = \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})$ in additive form.
- The **dual code** of $C \subseteq A^n$ is the annihilator $(\widehat{A}^n : C) \subseteq \widehat{A}^n$.

Good duality properties

- Assume 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.)

Recall Poisson summation formula

Let B be any subgroup of A, V a complex vector space, and $f : A \to V$. 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 $f : A^n \longrightarrow V$ has the form

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

  where $f_i : A \longrightarrow V$.
- 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.
- $f : A^n \longrightarrow V$,

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

- 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 cwe_C becomes hwe_C.
- Using summation formulas for characters:

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

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

Linear codes over modules

- When A is a left R-module and $C \subseteq A^n$ is a left R-submodule (a left linear code over A), then $(\widehat{A}^n : C)$ is a right linear code over $\widehat{A}$.
- The duality properties and the MacWilliams identities have exactly the same form.

Frobenius rings: making identifications

- Let R be a finite Frobenius ring with generating character ρ.
- Define $\psi : R^n \longrightarrow \widehat{R}^n$, $x \mapsto \psi_x$:

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

- Then ψ is an isomorphism of left R-modules.

Character annihilator vs. dot product

- Recall:
$$\psi_x(y) = \rho(y \cdot x), \quad y \in R^n.$$
- Additive subgroup $C \subseteq R^n$. Under ψ, $(\widehat{R}^n : C)$ corresponds to
$$r_\rho(C) = \{x \in R^n : \rho(C \cdot x) = 1\}.$$
- $r(C) \subseteq r_\rho(C)$ in general
- $r(C) = r(RC) = r_\rho(RC) \subseteq r_\rho(C)$ in general.
- $r(C) = r_\rho(C)$ when C is a left submodule.

MacWilliams identities: complete weight enumerator

For a left linear code $C \subseteq R^n$, R Frobenius:

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

MacWilliams identities: Hamming weight enumerator

For a left linear code $C \subseteq R^n$, R Frobenius:

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