

# Foundational Aspects of Linear Codes: 2. Fourier transform and good duality

Jay A. Wood

Department of Mathematics  
Western Michigan University  
<http://homepages.wmich.edu/~jwood/>

On the Algebraic and Geometric  
Classifications of Projective Varieties  
University of Messina  
June 21, 2016

## 2. Fourier transform and good duality

- ▶ Additive codes
- ▶ Good duality properties
- ▶ Poisson summation formula
- ▶ MacWilliams identities
- ▶ Making identifications when the alphabet is a Frobenius ring
- ▶ Self-duality over module alphabets

# 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  $\hat{A} = \text{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})$  in additive form.
- ▶ The **dual code** of  $C \subseteq A^n$  is the annihilator  $(\hat{A}^n : C) \subseteq \hat{A}^n$ .

# 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  $f : A \rightarrow V$ . Then

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

# A Fourier transform example

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

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

where  $f_i : A \rightarrow V$ .

- ▶ Then

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

# Complete weight enumerator

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

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

- ▶ Then

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

# MacWilliams identities from Poisson summation formula

- ▶ Poisson:

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

- ▶ 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

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

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

- ▶ MacWilliams identities:

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

# Specialize to Hamming weight enumerator

- ▶ Recall  $\text{hwe}_C(X, Y) = \sum_{x \in C} X^{n-\text{wt}(x)} Y^{\text{wt}(x)}$ .
- ▶ Specialize  $\mathbb{C}[Z_a : a \in A] \rightarrow \mathbb{C}[X, Y]$ ,  $Z_0 \mapsto X$ ,  $Z_a \mapsto Y$  for  $a \neq 0$ . Then  $\text{cwe}_C$  becomes  $\text{hwe}_C$ .
- ▶ Using summation formulas for characters:

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

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

- ▶ Suppose the alphabet is the ring itself:  $A = R$ .
- ▶ Let  $R$  be a finite Frobenius ring with generating character  $\rho$ .
- ▶ Define  $\psi : R^n \rightarrow \widehat{R}^n$ ,  $x \mapsto \psi_x$ :

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

- ▶ Then  $\psi$  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  $\psi$ ,  $(\widehat{R}^n : C)$  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:

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

# MacWilliams identities: Hamming weight enumerator

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

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

# Self-duality over module alphabets

- ▶ “Self-dual codes and invariant theory” by Nebe, Rains and Sloane, 2006.
- ▶ Anti-isomorphisms  $\varepsilon$  on rings
- ▶ Using  $\varepsilon$  to swap sides on modules
- ▶ Good duality from characters
- ▶ Alphabets with  $\widehat{A} \cong \varepsilon(A)$
- ▶ Dual code as  $\varepsilon$  of pullback of annihilator
- ▶ Interpret in terms of bi-additive form
- ▶ Compare to generating character
- ▶ Examples
- ▶ Generalization of Gleason’s theorem



# Setting for the rest of the lecture

- ▶ Finite ring  $R$ , alphabet  $A$ , a left  $R$ -module.
- ▶ A left **linear code** is a left  $R$ -submodule  $C \subseteq A^n$ .
- ▶ How to define self-dual codes in this context?
- ▶ Applies to non-commutative ring alphabets as well.
- ▶ We will explain the approach of “Self-dual codes and invariant theory” by Nebe, Rains and Sloane, 2006.

# Anti-isomorphisms

- ▶ Let  $R$  be a finite ring with 1.
- ▶ An **anti-isomorphism** of  $R$  is a map  $\varepsilon : R \rightarrow R$  that is an isomorphism of the additive group of  $R$  and satisfies  $\varepsilon(rs) = \varepsilon(s)\varepsilon(r)$  for all  $r, s \in R$ .
- ▶ An anti-isomorphism  $\varepsilon$  is an **involution** if  $\varepsilon^2 = \text{id}_R$ .

# Examples

- ▶ Let  $S$  be a ring with anti-isomorphism  $\epsilon$ .
- ▶ For any finite group  $G$ , the group ring  $R = S[G]$  has anti-isomorphism  $\varepsilon$ :

$$\varepsilon\left(\sum_{g \in G} c_g g\right) = \sum_{g \in G} \epsilon(c_g) g^{-1}.$$

- ▶ Matrix ring  $R = M_{k \times k}(S)$ , using the transpose:

$$\varepsilon(P) = (\epsilon(P))^T, \quad P \in R.$$

Apply  $\epsilon$  to each entry of  $P$ .

# Swapping sides

- ▶ An anti-isomorphism  $\varepsilon$  on  $R$  allows one to regard left modules as right modules, and vice versa.
- ▶ If  $M$  is a left  $R$ -module, define  $\varepsilon(M)$  to be same abelian group as  $M$ , but equipped with right scalar multiplication defined by

$$xr = \varepsilon(r)x, \quad x \in M, r \in R,$$

where  $\varepsilon(r)x$  is the left scalar multiplication of the module  $M$ .

- ▶ Similar definition for right module to left.

# Character-theoretic duality

- ▶ Recall from earlier: if  $C \subseteq A^n$  is a left  $R$ -linear code, then  $(\widehat{A}^n : C) \subseteq \widehat{A}^n$  is a right  $R$ -linear code.
- ▶ Double annihilator:  $(A^n : (\widehat{A}^n : C)) = C$ .
- ▶ Size:  $|C| \cdot |(\widehat{A}^n : C)| = |A^n|$ .
- ▶ The MacWilliams identities hold (cwe and hwe).

# Alphabets with $\widehat{A} \cong \varepsilon(A)$

- ▶ Starting with a left linear code  $C \subseteq A^n$ , a good candidate for a dual code is the right linear code  $(\widehat{A}^n : C) \subseteq \widehat{A}^n$ .
- ▶ So, assume the existence of an isomorphism  $\psi : \varepsilon(A) \rightarrow \widehat{A}$  of right  $R$ -modules.
- ▶ Define the **dual code** of a left linear code  $C \subseteq A^n$  as

$$C^\perp = \psi^{-1}(\widehat{A}^n : C).$$

- ▶ Can use the same definition for an additive code  $C \subseteq A^n$ .

# Interpret in terms of bi-additive form

- ▶ Use the additive form of characters:  
 $\widehat{A} = \text{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})$ .
- ▶ Define  $\beta : A \times A \rightarrow \mathbb{Q}/\mathbb{Z}$  by  $\beta(a, b) = \psi(b)(a)$ , for  $a, b \in A$ . Extend additively to  $A^n \times A^n$ . Then:
- ▶  $\beta$  is bi-additive.
- ▶  $\beta(rx, y) = \beta(x, \varepsilon(r)y)$  for  $x, y \in A^n, r \in R$ .
- ▶ Impose one more property: there exists a unit  $e \in R$  such that  $\beta(x, y) = \beta(ey, x)$  for  $x, y \in A^n$ .

# Properties of $C^\perp$

- ▶ Recall  $C^\perp = \psi^{-1}(\widehat{A}^n : C)$ .
- ▶ In terms of  $\beta$ :  $C^\perp = \{y \in A^n : \beta(C, y) = 0\}$ .
- ▶ Even if  $C \subseteq A^n$  is just an additive code, we have  $|C| \cdot |C^\perp| = |A^n|$  and the MacWilliams identities.
- ▶ If  $C$  is a left linear code, then so is  $C^\perp$ .
- ▶ If  $C$  is a left linear code, then  $(C^\perp)^\perp = C$ . This uses the  $\beta(x, y) = \beta(ey, x)$  condition.
- ▶ When  $C$  is a left linear code, we also have  $C^\perp = \{x \in A^n : \beta(x, C) = 0\}$ .



# Ring alphabets

- ▶ Suppose  $R$  admits an anti-isomorphism  $\varepsilon$ .
- ▶ Let  $A = R$ . Then there exists isomorphism  $\psi : \varepsilon(A) \rightarrow \widehat{A}$  if and only if  $R$  is Frobenius.
- ▶ When a Frobenius ring  $R$  has generating character  $\varrho$ , then

$$\beta(x, y) = \sum_{i=1}^n \varrho(\varepsilon^{-1}(y_i)x_i),$$

for  $x, y \in R^n$ .

# Example (a)

- ▶ Consider a simple finite ring  $R$ .
- ▶ A left linear code  $C$  of length 1 is a left ideal.
- ▶ Without using characters, one could consider

$$l(C) = \{x \in R : xC = 0\},$$
$$r(C) = \{y \in R : Cy = 0\}.$$

- ▶ If  $C = l(C)$  or  $C = r(C)$ ,  $C$  must be a two-sided ideal. Hence,  $C = 0$  or  $C = R$ .

## Example (b)

- ▶ Consider  $R = M_{k \times k}(\mathbb{F}_2)$ , a Frobenius ring with involution  $\varepsilon$  equaling the matrix transpose and generating character  $\varrho(P) = \vartheta_2(\text{Tr}(P))$ ,  $P \in R$ .
- ▶ Then  $\beta(P, Q) = \varrho(\varepsilon^{-1}(Q)P) = \vartheta_2(\text{Tr}(Q^T P))$ .
- ▶ Thus  $\beta(P, Q) = (1/2) \sum_{i,j} Q_{ij} P_{ij} \in \mathbb{Q}/\mathbb{Z}$ .

# Example (c)

- ▶ For  $k = 2$ , there are proper left ideals ( $a, b \in \mathbb{F}_2$ ):

$$C_1 = \left\{ \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} \right\}, C_2 = \left\{ \begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix} \right\}, C_3 = \left\{ \begin{bmatrix} a & a \\ b & b \end{bmatrix} \right\}.$$

- ▶ Then  $C_1^\perp = C_2$ ,  $C_2^\perp = C_1$ , and  $C_3^\perp = C_3$ .

# Gleason's theorem

- ▶ The Hamming weight enumerators of binary self-dual codes (or binary doubly-even self-dual codes) are invariant under the action of a finite subgroup of  $GL(2, \mathbb{C})$ , because of weight restrictions on the codewords and the MacWilliams identities.
- ▶ Gleason (1970) proved that the Hamming weight enumerators of two specific codes generate the ring of all invariant polynomials under these subgroup actions.
- ▶ Nebe, Rains, and Sloane (2006) have proved a vast generalization of Gleason's theorem, valid over any finite principal ideal ring.

# Questions

- ▶ Which finite rings admit anti-isomorphisms? involutions?
- ▶ Which finite Frobenius rings do?
- ▶ For rings with  $\varepsilon$ , which left modules  $A$  admit an isomorphism  $\psi : \varepsilon(A) \rightarrow \widehat{A}$ ?
- ▶ Can Gleason's theorem be generalized beyond principal ideal rings?