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 11, 2015

7. Self-duality for linear codes over modules

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

Setting for this 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?
- 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 $\varepsilon : R \longrightarrow R$ 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 ε is an **involution** if $\varepsilon^2 = \mathrm{id}_R$.

Examples

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

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

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

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

Apply ϵ to each entry of P.

Swapping sides

- An anti-isomorphism ε 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 $\psi : \varepsilon(A) \longrightarrow \widehat{A}$ 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: $\widehat{A} = \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})$.
- Define $\beta : A \times A \to \mathbb{Q}/\mathbb{Z}$ by $\beta(a, b) = \psi(b)(a)$, for $a, b \in A$. Extend additively to $A^n \times A^n$. Then:
- β 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 β: $C^{\perp} = \{y \in A^n : \beta(C, y) = 0\}$.
- 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 ε.
- Let $A = R$. Then there exists isomorphism $\psi : \varepsilon(A) \longrightarrow \widehat{A}$ if and only if R is Frobenius.
- When a Frobenius ring R has generating character ϱ, then

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

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 ε equaling the matrix transpose and generating character $\varrho(P) = \vartheta_2(\mathrm{Tr}(P))$, $P \in R$.
- Then $\beta(P, Q) = \varrho(\varepsilon^{-1}(Q)P) = \vartheta_2(\mathrm{Tr}(Q^T P))$.
- 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 ε, which left modules A admit an isomorphism $\psi : \varepsilon(A) \longrightarrow \widehat{A}$?
- Can Gleason's theorem be generalized beyond principal ideal rings?