# 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 7, 2018

# 5. Self-duality for linear codes over modules

- Classical examples
- Invariant polynomials
- Gleason's theorem
- "Self-dual codes and invariant theory" by Nebe, Rains and Sloane, 2006.
- Anti-isomorphisms
- Good duality from characters
- Alphabets with extra structure
- Generalization of Gleason's theorem

# Classical setting

- Let $R = \mathbb{F}_q$ and consider linear codes $C \subseteq \mathbb{F}_q^n$.
- Equip $\mathbb{F}_q^n$ with the standard dot product:

$$x \cdot y = \sum_{i=1}^{n} x_i y_i, \quad x, y \in \mathbb{F}_q^n.$$

- Could use an hermitian inner product instead.
- The dual code is $C^\perp = \{y \in \mathbb{F}_q^n : C \cdot y = 0\}$.

# Self-dual codes

- A linear code is **self-orthogonal** if $C \subseteq C^{\perp}$.
- A linear code is **self-dual** if $C = C^{\perp}$.
- If $\dim C = k$, then $\dim C^{\perp} = n - k$. (Analogous to "$|B| \cdot |(\widehat{A} : B)| = |A|$".)
- If $C \subseteq \mathbb{F}_q^n$ is self-dual, then $n = 2k$ is even.

# Binary case

- Let $q = 2$, the binary case.
- For $x \in \mathbb{F}_2^n$, if $x \cdot x = 0$, then $\mathrm{wt}(x)$ is even. (For $q = 3$, $\mathrm{wt}(x) \equiv 0 \bmod 3$. Not true in general.)
- If $C \subseteq \mathbb{F}_2^n$ is self-orthogonal, then every codeword in $C$ has even weight.
- Extra: a binary self-orthogonal code in which every codeword has weight divisible by 4 is **doubly-even** (**singly-even** otherwise).

# A binary example

- The codes generated by $G_2$, $G_8$ are singly-even, self-dual:

$$G_2 = [1\ 1], \quad G_8 = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

- $\mathrm{hwe}_{G_2} = X^2 + Y^2$. Call this $S = \mathrm{hwe}_{G_2}$.
- $\mathrm{hwe}_{G_8} = X^8 + 4X^6Y^2 + 6X^4Y^4 + 4X^2Y^6 + Y^8 = (X^2 + Y^2)^4$.

# Another binary example

- The code generated by $E_8$ is doubly-even, self-dual.

$$E_8 = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}$$

- $\mathrm{hwe}_{E_8} = X^8 + 14X^4Y^4 + Y^8$. Call it $T = \mathrm{hwe}_{E_8}$.

# And another

- Length 24. Start with 1111100100101.
- Take successive shifts of this vector until there is a 1 in position 23. Finish with a row of 1s:

$$G_{24} = \begin{bmatrix} 111110010010100000000000 \\ 011111001001010000000000 \\ 001111100100101000000000 \\ \vdots \\ 000000000011111001001010 \\ 111111111111111111111111 \end{bmatrix}$$

# And another, continued

- The code generated by $G_{24}$ is doubly-even, self-dual.
- Called the **extended Golay code**.
- Dates from 1949.
- $\mathrm{hwe}_{G_{24}} = X^{24} + 759X^{16}Y^{8} + 2576X^{12}Y^{12} + 759X^{8}Y^{16} + Y^{24}$.

# MacWilliams identities

- Recall the MacWilliams identities over $\mathbb{F}_q$ for the Hamming weight enumerator:

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

- Over $\mathbb{F}_2$:

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

# Binary self-dual case

- When the code $C$ is self-dual, $C$ appears on both sides of the MacWilliams identities:

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

- Length is $n = 2k$. $\mathrm{hwe}_C(X, Y)$ is a homogeneous polynomial of degree $n$, so

$$\mathrm{hwe}_C(X, Y) = \mathrm{hwe}_C\left(\frac{X + Y}{\sqrt{2}}, \frac{X - Y}{\sqrt{2}}\right).$$

# Invariance properties

- The group $\mathrm{GL}(2, \mathbb{C})$ acts on $\mathbb{C}[X, Y]$ by linear substitution:

$$f(X, Y) \begin{bmatrix} a & b \\ c & d \end{bmatrix} = f(aX + cY, bX + dY).$$

- For binary self-dual $C$, $\mathrm{hwe}_C$ is invariant under

$$M = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

# More invariance properties

- In addition, singly-even and doubly-even are invariant under, respectively ($i = \sqrt{-1}$):

$$W_s = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad W_d = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}.$$

- Define two subgroups of $\mathrm{GL}(2, \mathbb{C})$: $\mathcal{G}_s = \langle M, W_s \rangle$ and $\mathcal{G}_d = \langle M, W_d \rangle$.
- For singly-even $C$, $\mathrm{hwe}_C \in \mathbb{C}[X, Y]^{\mathcal{G}_s}$.
- For doubly-even $C$, $\mathrm{hwe}_C \in \mathbb{C}[X, Y]^{\mathcal{G}_d}$.

# Gleason's theorem (1970)

- The rings of invariant polynomials are generated by the Hamming weight enumerators of certain codes.
- $\mathbb{C}[X, Y]^{\mathcal{G}_s} = \mathbb{C}[\mathrm{hwe}_{G_2}, \mathrm{hwe}_{E_8}] = \mathbb{C}[S, T]$
- $\mathbb{C}[X, Y]^{\mathcal{G}_d} = \mathbb{C}[\mathrm{hwe}_{E_8}, \mathrm{hwe}_{G_{24}}]$
- Corollary: doubly-even self-dual codes occur only in dimensions divisible by 8.
- $\mathrm{hwe}_{G_{24}} = T^3 + \frac{21}{8}(2S^8T - S^4T^2 - S^{12})$.
- There are versions when $q = 3$ or $q = 4$ (with hermitian inner product).

# Setting for the rest of 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 $\varepsilon : R \to R$ 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 $\varepsilon^2 = \mathrm{id}_R$.
- If $R$ is commutative, then $\mathrm{id}_R$ is an anti-isomorphism.

# Examples

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

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

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

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

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 $\psi : \varepsilon(A) \to \widehat{A}$ 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:
- $\beta$ 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 $x, y \in A^n$.

# Additive 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.
- For an additive code $C$, $e^{-1}C = (C^\perp)^\perp$. This uses the $\beta(x, y) = \beta(ey, x)$ condition.

# Module properties of $C^\perp$

- If $C$ is a left linear code, then so is $C^\perp$.
- If $C$ is a left linear code, then $(C^\perp)^\perp = C$. (Because $e^{-1}C = C$.)
- When $C$ is a left linear code, we also have $C^\perp = \{y \in A^n : \beta(y, C) = 0\}$. (Because $\beta(x, y) = \beta(ey, x) = \beta(y, \varepsilon(e)x)$.)

# Ring alphabets

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

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

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 $\varepsilon$ equaling the matrix transpose and generating character $\varrho(P) = \mathrm{Tr}(P)/2$, $P \in R$.
- Then $\beta(P, Q) = \varrho(\varepsilon^{-1}(Q)P) = \mathrm{Tr}(Q^{\mathsf{T}}P)/2$.
- 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) 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 $\psi : \varepsilon(A) \to \widehat{A}$?
- Can Gleason's theorem be generalized beyond principal ideal rings?