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 7, 2017

5. Exercise Session

- Exercise: every character of $\mathbb{Z}/k\mathbb{Z}$ has the form $\rho_b(a) = \exp(2\pi i ab/k)$, $a \in \mathbb{Z}/k\mathbb{Z}$, 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 $\rho_b \longleftrightarrow b$.

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: $(A : (\widehat{A} : B)) = B$.

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

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

where $f_i : A \to V$.

- Then

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

Character modules

- Extra information: the left R-module structure on A induces a right R-module structure on $\widehat{A}$.
- For $r \in R$ and $\varpi \in \widehat{A}$, define $\varpi r \in \widehat{A}$ by $(\varpi r)(a) = \varpi(ra)$, $a \in A$; $(\pi^r)(a) = \pi(ra)$.
- If A is a right module, then $\widehat{A}$ is a left module: $(r\varpi)(a) = \varpi(ar)$; $({}^r\pi)(a) = \pi(ar)$.

Annihilators are submodules

- Suppose $B \subseteq A$ is a left R-submodule.
- Then the annihilator $(\widehat{A} : B) \subseteq \widehat{A}$ is a right R-submodule.
- If $\varrho \in (\widehat{A} : B)$ and $r \in R$, then

$$(\varrho r)(B) = \varrho(rB) \subseteq \varrho(B) = 0,$$

because B is a left submodule.

Characterizing generating characters

Theorem

A character $\varrho \in \widehat{R}$ is a right generating character if and only if $\ker \varrho$ *contains no nonzero right ideal of R.*

- Define $\psi : R \to \widehat{R}$ by $\psi(r) = \varrho r$. When is ψ an isomorphism? (Injective is enough, as $|R| = |\widehat{R}|$.)
- $\psi(r) = 0$ iff $(\varrho r)(R) = 0$ iff $\varrho(rR) = 0$ iff $rR \subseteq \ker \varrho$.
- Similar result for left generating characters.

Left/right symmetry

Theorem

A character $\varrho \in \widehat{R}$ is a left generating character if and only if ϱ is a right generating character.

- Left implies right: Suppose $rR \subseteq \ker \varrho$. Then $\varrho(rs) = 0$ for all $s \in R$.
- Then $(s\varrho)(r) = 0$ for all $s \in R$. I.e., $\varpi(r) = 0$ for all $\varpi \in \widehat{R}$, as ϱ left generates.
- Thus $r = 0$. (Uses "$|B| \cdot |(\widehat{A} : B)| = |\widehat{A}|$", $B = \mathbb{Z}r$.)

A generalization for modules

- R finite ring with 1; A finite unital left R-module.
- An R-module is **cyclic** if it is generated by one element. Say M is generated by $m \in M$. Then $R \to M$, $r \mapsto rm$, is onto.

Theorem

The following are equivalent:

1. $\widehat{A}$ *is a cyclic right* R*-module.*
2. A *injects into* $\widehat{R}$*:* $A \hookrightarrow \widehat{R}$.
3. *There exists* $\varrho \in \widehat{A}$ *such that* $\ker \varrho$ *contains no nonzero left* R*-submodule.*

Proof

- $1 \leftrightarrow 2$. Contravariant exact functor: $0 \to A \to \widehat{R}$ dualizes to $R \to \widehat{A} \to 0$, and vice versa.
- Fix $\varrho \in \widehat{A}$. Define $A \to \widehat{R}$ by $a \mapsto (r \mapsto \varrho(ra))$.
- $2 \leftrightarrow 3$: $a \in A$ is in the kernel of the map above iff $\varrho(Ra) = 0$ iff $Ra \subseteq \ker \varrho$.
- Call such a ϱ a **generating character** for A.

More on simple modules

- If S is simple, and $0 \neq s \in S$, then $S = Rs$.
- The annihilator $\operatorname{ann}(s) = \{r \in R : rs = 0\}$ is a maximal left ideal of R; $S \cong R/\operatorname{ann}(s)$.
- $\operatorname{Rad}(R)$ annihilates simple modules: $\operatorname{Rad}(R)S = 0$.
- Every simple module is a module over $R/\operatorname{Rad}(R)$.
- $\operatorname{Soc}(A)$ is a module over $R/\operatorname{Rad}(R)$.
- Same idea for right modules; reverse sides.

Top-bottom duality

- R finite ring with 1; A finite left R-module.
- $A/\operatorname{Rad}(R)A$ is the "top quotient" of A; it is a sum of simple modules.
- $\operatorname{Soc}(\widehat{A}) = (\widehat{A} : \operatorname{Rad}(R)A) \cong (A/\operatorname{Rad}(R)A)\widehat{\ }$.
- $\supseteq$: $(A/\operatorname{Rad}(R)A)\widehat{\ }$ is a sum of simple modules.
- $\subseteq$: because $\operatorname{Soc}(\widehat{A})\operatorname{Rad}(R) = 0$.

Sketch of proof

- We already know $1 \leftrightarrow 2$.
- Fact: if $R = M_{k\times k}(\mathbb{F}_q)$, then $\widehat{R} \cong R$.
- Then general $(R/\operatorname{Rad}(R))\widehat{\ } \cong R/\operatorname{Rad}(R)$.
- So $\operatorname{Soc}(\widehat{R}) \cong (R/\operatorname{Rad}(R))\widehat{\ } \cong R/\operatorname{Rad}(R)$.
- $1, 2 \Rightarrow 3$: If $\widehat{R} \cong R$, then $\operatorname{Soc}(R) \cong \operatorname{Soc}(\widehat{R}) \cong R/\operatorname{Rad}(R)$.

Construction

- $M_{k\times k}(\mathbb{F}_q)$ has a generating character: $\varrho(P) = \vartheta_q(\operatorname{Tr} P)$, $P \in M_{k\times k}(\mathbb{F}_q)$.
- $\operatorname{Tr} P$ is the matrix trace of P.
- If $q = p^e$ and $x \in \mathbb{F}_q$, then

$$\vartheta_q(x) = (x + x^p + \cdots x^{p^{e-1}})/p \in \mathbb{Q}/\mathbb{Z}.$$

- ϑ_q is a generating character of $\mathbb{F}_q$.

Why does ϱ generate?

- Suppose $B \subseteq \ker \varrho$ is a left ideal of R.
- Then $\mathrm{Soc}(B) = B \cap \mathrm{Soc}(R) \subseteq \ker \varrho \cap \mathrm{Soc}(R)$.
- But ϱ is a generating character of $\mathrm{Soc}(R)$, so $\mathrm{Soc}(B) = 0$.
- Thus $B = 0$; ϱ is a left generating character of R.

Similar characterization for modules

Theorem

The following are equivalent:

1. $\widehat{A}$ *is a cyclic right* R*-module.*
2. A *injects into* $\widehat{R}$*:* $A \hookrightarrow \widehat{R}$.
3. *There exists* $\varrho \in \widehat{A}$ *such that* $\ker \varrho$ *contains no nonzero left* R*-submodule.*
4. $\mathrm{Soc}(A) \subseteq A$ *is a cyclic* R*-submodule.*

More identifications

- R finite Frobenius ring with generating character ϱ.
- Dot product on R^n: $y \cdot x = \sum_{i=1}^n y_i x_i$.
- Define $\psi : R^n \to \widehat{R}^n$, $x \mapsto \psi_x$:

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

- Then ψ is an isomorphism of left R-modules.
- $\psi_{rx}(y) = \varrho(y \cdot rx) = \varrho(yr \cdot x) = \psi_x(yr) = (r\psi_x)(y)$.

Character annihilator vs. dot product

- Recall: $\psi_x(y) = \varrho(y \cdot x), \quad y \in R^n$.
- Additive subgroup $C \subseteq R^n$. Under ψ, $(\widehat{R}^n : C)$ corresponds to $r_\varrho(C) = \{x \in R^n : \varrho(C \cdot x) = 0\}$.
- Set $r(C) = \{x \in R^n : C \cdot x = 0\}$.
- $r(C) \subseteq r_\varrho(C)$ in general
- $r(C) = r(RC) = r_\varrho(RC) \subseteq r_\varrho(C)$ in general.
- $r(C) = r_\varrho(C)$ when C is a left submodule, as $C \cdot x$ is a left ideal in $\ker \varrho$.

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. (This is also true for $q = 3$, but not 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:

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

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

Another binary example

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

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

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

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, 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, $\mathrm{hwe}_C \in \mathbb{C}[X, Y]^{\mathcal{G}_d}$.

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.

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 $C^\perp = \{x \in A^n : \beta(x, C) = 0\}$.

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 $C_3^\perp = C_3$.