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 4, 2018

4. Generating characters and finite Frobenius rings

- Generating characters
- Frobenius rings
- Generalizations to modules

Summary from last time (i)

- Given left R-linear code $C \subseteq A^n$.
- Dual $(\widehat{A}^n : C) \subseteq \widehat{A}^n$ is a right R-linear 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.

Summary from last time (ii)

- We could make some identifications, when $A = R$, provided $\widehat{R} \cong R$.
- If $\psi : R \to \widehat{R}$ is an isomorphism of left R-modules, then $\varrho = \psi(1)$ is a left generating character of R.
- ψ extends to an isomorphism $R^n \to \widehat{R}^n$.
- $x \mapsto \psi_x$, where $\psi_x(y) = \varrho(y \cdot x)$, $x, y \in R^n$.
- When C is a linear code (submodule), $(\widehat{R}^n : C)$ corresponds to $r(C) = \{x \in R^n : C \cdot x = 0\}$.

Today's topics

- When is $\widehat{R} \cong R$ as one-sided modules?
- What are other properties of generating characters?
- Is it possible to construct generating characters?
- Can these ideas be generalized to modules?

Recall: character modules

- If A is a left R-module, then $\widehat{A}$ is a right R-module via $(\varrho r)(a) = \varrho(ra)$, $\varrho \in \widehat{A}$, $r \in R$, $a \in A$.
- For characters in multiplicative form: $\rho^r(a) = \rho(ra)$.
- If B is a right R-module, then $\widehat{B}$ is a left R-module: $(r\varrho)(b) = \varrho(br)$ or ${}^r\rho(b) = \rho(br)$.

Characterizing generating characters

Theorem

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

- Define $\psi : R \to \widehat{R}$ by $\psi(r) = r\varrho$. When is ψ an isomorphism? (Injective is enough, as $|R| = |\widehat{R}|$.)
- $\psi(r) = 0$ iff $(r\varrho)(R) = 0$ iff $\varrho(Rr) = 0$ iff $Rr \subseteq \ker \varrho$.
- Similar result for right 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 (other direction is similar): 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 "$|B| \cdot |(\widehat{A} : B)| = |\widehat{A}|$", $B = \mathbb{Z}r$.)
- Thus $\widehat{R} \cong R$ as left R-modules if and only if $\widehat{R} \cong R$ as right R-modules.

Example: finite fields

- View $\mathbb{F}_p$ as $\mathbb{Z}/p\mathbb{Z}$. Then $\vartheta_p : \mathbb{F}_p \to \mathbb{Q}/\mathbb{Z}$, $\vartheta_p(x) = x/p$, is a generating character of $\mathbb{F}_p$.
- If $q = p^e$, then $\vartheta_q : \mathbb{F}_q \to \mathbb{Q}/\mathbb{Z}$,

$$\vartheta_q(x) = \vartheta_p(x + x^p + \cdots + x^{p^{e-1}}),$$

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

Example: matrix rings

- Let $\operatorname{Tr} P$ be the trace of a square matrix P.
- $M_{k\times k}(\mathbb{F}_q)$ has a generating character: $\varrho(P) = \vartheta_q(\operatorname{Tr} P)$, $P \in M_{k\times k}(\mathbb{F}_q)$.
- Define $\psi : M_{k\times k}(\mathbb{F}_q) \to M_{k\times k}(\mathbb{F}_q)\,\widehat{}\,$:

$$Q \mapsto \psi_Q, \quad \psi_Q(P) = \varrho(PQ).$$

- Then ψ is an isomorphism of bimodules.
- This uses $\operatorname{Tr}(QP) = \operatorname{Tr}(PQ)$ over $\mathbb{F}_q$.

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.

Other structures in modules

- We want to connect the existence of generating characters to other structures in modules.
- A nonzero left R-module S is **simple** if S has no nonzero proper R-submodules.
- The **socle** $\mathrm{Soc}(A)$ of a left R-module A is the submodule generated by (i.e., the sum of) all the simple submodules of A.

Jacobson radical

- R finite ring with 1.
- The **Jacobson radical** $\mathrm{Rad}(R)$ is the intersection of all maximal left ideals of R.
- $\mathrm{Rad}(R)$ is a two-sided ideal.
- $R/\mathrm{Rad}(R)$ is a semi-simple ring, and

$$R/\mathrm{Rad}(R) \cong \bigoplus_{i=1}^{t} M_{k_i \times k_i}(\mathbb{F}_{q_i}).$$

- Artin-Wedderburn decomposition.

More on simple modules

- If S is simple, and $0 \neq s \in S$, then $S = Rs$.
- If not, we would have $0 \subsetneq Rs \subsetneq S$.
- The annihilator $\operatorname{ann}(s) = \{r \in R : rs = 0\}$ is a maximal left ideal of R; $S \cong R/\operatorname{ann}(s)$.
- For $R \twoheadrightarrow S = Rs$, $r \mapsto rs$, the kernel is $\operatorname{ann}(s)$.
- Submodules of S correspond to left ideals containing $\operatorname{ann}(s)$.
- S is simple if and only if $\widehat{S}$ is simple.

Even more on simple modules

- $\mathrm{Rad}(R)$ annihilates simple modules: $\mathrm{Rad}(R)S = 0$.
- For any $s \in S$, $\mathrm{Rad}(R) \subseteq \mathrm{ann}(s)$, so $\mathrm{Rad}(R)s = 0$.
- Every simple module is a module over $R/\mathrm{Rad}(R)$.
- The multiplication $(r + \mathrm{Rad}(R))s = rs$ is well-defined.
- $\mathrm{Soc}(A)$ is a module over $R/\mathrm{Rad}(R)$, being a sum of simple modules.
- 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 module over $R/\operatorname{Rad}(R)$ and 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 $\operatorname{Soc}(\widehat{A})\operatorname{Rad}(R) = 0$.

Additional characterization for rings

Theorem

For a finite ring R, the following are equivalent.

1. $\widehat{R} \cong R$ as left R-modules.
2. $\widehat{R} \cong R$ as right R-modules.
3. $\mathrm{Soc}(R) \cong R/\mathrm{Rad}(R)$ as left and as right R-modules. ($\mathrm{Soc}(R)$ is cyclic.)

- Such a ring R is called a **Frobenius** ring.

Sketch of proof

- We already know $1 \Leftrightarrow 2$.
- Earlier: if $R = M_{k\times k}(\mathbb{F}_q)$, then $\widehat{R} \cong R$.
- Then general R has $(R/\operatorname{Rad}(R))\widehat{\ } \cong R/\operatorname{Rad}(R)$.
- 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 $\operatorname{Soc}(R) \cong \operatorname{Soc}(\widehat{R}) \cong R/\operatorname{Rad}(R)$.
- For $3 \Rightarrow 1, 2$, we construct a generating character.

Construction

- $R/\operatorname{Rad}(R)$ is a sum of matrix rings. Each matrix ring has a generating character $(P \mapsto \vartheta_q(\operatorname{Tr} P))$.
- The sum of those generating characters is a generating character ϱ for $R/\operatorname{Rad}(R)$.
- $3 \Rightarrow 1, 2$: $\operatorname{Soc}(R) \cong R/\operatorname{Rad}(R)$ has a generating character (still call it ϱ).
- $0 \to \operatorname{Soc}(R) \to R$, so $\widehat{R} \to \operatorname{Soc}(R)\widehat{\ } \to 0$.
- Any lift of ϱ is a generating character of R.

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

For a finite left R-module A, 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 left* R*-submodule.*

More about simple modules

- Let R be a finite ring with 1.
- Exact: $0 \to \mathrm{Rad}(R) \to R \to R/\mathrm{Rad}(R) \to 0$.
- $R/\mathrm{Rad}(R) \cong \oplus_{i=1}^{t} M_{k_i \times k_i}(\mathbb{F}_{q_i})$.
- Each matrix ring $M_{k_i \times k_i}(\mathbb{F}_{q_i})$ has a simple left module $S_i \cong M_{k_i \times 1}(\mathbb{F}_{q_i})$ given by matrix multiplication on column vectors.
- Can regard S_i as a left R-module via $R \to R/\mathrm{Rad}(R)$.

Even more about simple modules

- Up to isomorphism, the S_i are the *only* simple left R-modules.
- That is: the S_i are simple; $S_i \ncong S_j$ for $i \neq j$; and any simple left R-module is isomorphic to one of the S_i.

More about the socle

- Let A be a finite left R-module.
- By definition, the socle $\mathrm{Soc}(A)$ is a sum of simple left R-submodules of A.
- Thus $\mathrm{Soc}(A) \cong \oplus_{i=1}^{t} S_i^{s_i} \cong \oplus_{i=1}^{t} M_{k_i \times s_i}(\mathbb{F}_{q_i})$.
- $\mathrm{Soc}(A)$ is cyclic if and only if $s_i \leq k_i$ for all i.

More about generating characters

- Let A be a finite left R-module.
- Suppose $B \subseteq A$ is a left R-submodule.
- If ϱ is a generating character of A, then the restriction of ϱ is a generating character of B.
- Any submodule of $B \cap \ker \varrho$ is a submodule of $\ker \varrho$.
- Or: $B \hookrightarrow A \hookrightarrow \widehat{R}$ induces $R \twoheadrightarrow \widehat{A} \twoheadrightarrow \widehat{B}$.

Generating characters for matrix modules

- Focus on $R = M_{k\times k}(\mathbb{F}_q)$ and $A = M_{k\times s}(\mathbb{F}_q)$.
- Claim: $M_{k\times s}(\mathbb{F}_q)$ has a generating character if and only if $s \leq k$.
- ($\Leftarrow$): If $s \leq k$, then $A \hookrightarrow R$ as the first s columns.
- The restriction of the generating character of R is a generating character of A.

The character module of a matrix module

- Continue with $R = M_{k\times k}(\mathbb{F}_q)$ and $A = M_{k\times s}(\mathbb{F}_q)$.
- Claim: $\widehat{A} \cong M_{s\times k}(\mathbb{F}_q)$ as right R-modules.
- Let $\psi : M_{s\times k}(\mathbb{F}_q) \to \widehat{A}$, $Q \mapsto \psi_Q$, with $\psi_Q(P) = \vartheta_q(\mathrm{Tr}(QP))$ for $P \in A$.
- Then ψ is an isomorphism of right R-modules.
- Injective: Consider P with only one non-zero entry r at position j, i.
- Then $\mathrm{Tr}(QP) = rq_{i,j} \in \ker \vartheta_q$. Thus $q_{i,j} = 0$.

No generating character when $s > k$

- ($\Rightarrow$): If $s > k$, we show that every character ψ_Q has a nonzero left submodule in $\ker \psi_Q$.
- Because $s > k$, the rows of Q are linearly dependent over $\mathbb{F}_q$. (The rows are s vectors in $\mathbb{F}_q^k$.)
- Let x be a nonzero row vector of length s with $xQ = 0$.
- Let X be a $k \times s$ matrix with every row equal to x.
- Then $XQ = 0$ with X nonzero.

A nonzero submodule in $\ker \psi_Q$

- Claim: the left principal ideal RX is in $\ker \psi_Q$.
- For any $P \in R$,
  $\psi_Q(PX) = \vartheta_q(\mathrm{Tr}(Q(PX))) = \vartheta_q(\mathrm{Tr}(XQ)P) = 0.$
- This uses $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$ over $\mathbb{F}_q$.
- Thus every ψ_Q fails to be a generating character.
- This finishes the proof that $M_{k\times s}(\mathbb{F}_q)$ has a generating character if and only if $s \leq k$.

Final steps on theorem

- Theorem said A has a generating character if and only if $\mathrm{Soc}(A)$ is cyclic.
- ($\Rightarrow$): A generating character of A restricts to one of $\mathrm{Soc}(A)$, which restricts to one of each matrix module $M_{k_i \times s_i}(\mathbb{F}_{q_i})$.
- That implies $s_i \leq k_i$, all i. Thus $\mathrm{Soc}(A)$ is cyclic.
- ($\Leftarrow$): $\mathrm{Soc}(A)$ cyclic implies $s_i \leq k_i$, implies each $M_{k_i \times s_i}(\mathbb{F}_{q_i})$ has a generating character.
- Their sum is a generating character for $\mathrm{Soc}(A)$. Extend to A as in the ring case.