Foundational Results on Linear Codes over Rings and Modules

Jay A. Wood

Department of Mathematics
Western Michigan University
http://sites.google.com/a/wmich.edu/jaywood

Centennial
Universidad Michoacana de San Nicolás de Hidalgo
Instituto de Física y Matemáticas
Morelia, Michoacán
March 7, 2018

3. Linear codes and their duals

- Linear codes
- Character modules
- Generating characters
- Frobenius rings
- Making identifications

Summary from last time

- For an additive code $C \subseteq A^n$, the annihilator $(\widehat{A}^n : C)$ satisfied some good duality properties.
- $(\widehat{A}^n : C) \subseteq \widehat{A}^n$ 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 hold.

Character modules

- Let R be a finite ring with 1 and A be a finite unital left R-module. (**Unital**: $1a = a$, all $a \in A$.)
- All of yesterday's discussion of characters, etc., applies to the additive group of A.
- 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.
- Indeed: 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.

Linear codes over modules

- A left **linear code** of length n over A is a left R-submodule $C \subseteq A^n$.
- Similarly, right linear codes are right submodules of a right module alphabet.
- For a left linear code $C \subseteq A^n$, 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.

Good duality properties

- For a left linear code $C \subseteq A^n$:
- $(\widehat{A}^n : C) \subseteq \widehat{A}^n$ is a right linear code.
- Double annihilator: $(A^n : (\widehat{A}^n : C)) = C$.
- Size: $|C| \cdot |(\widehat{A}^n : C)| = |A^n|$.
- The MacWilliams identities hold.

How does this relate to classical dual codes?

- In classical coding theory, the dual code is the annihilator with respect to a dot product.
- Can we do that here?
- For the rest of today, we will (mostly) work in the ring alphabet case. That is, let $A = R$.

Making identifications

- As above, a left linear code $C \subseteq R^n$ has annihilator $(\widehat{R}^n : C) \subseteq \widehat{R}^n$.
- We will aim to identify R and $\widehat{R}$ **as modules**.
- It will be enough to have $\widehat{R} \cong R$ as one-sided R-modules.
- We begin a long aside on when $\widehat{R} \cong R$ happens.

Generating characters

- When is $\widehat{R} \cong R$ as one-sided modules?
- Suppose $\psi : R \to \widehat{R}$ is an isomorphism of right R-modules.
- Then $\varrho = \psi(1)$ generates $\widehat{R}$ as a right R-module.
- Indeed: any $\varpi \in \widehat{R}$ has the form $\varpi = \psi(r) = \psi(1r) = \psi(1)r = \varrho r$.
- Call any generator ϱ a right **generating character** of R.

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.

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 $S = Rs$.
- 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 $\operatorname{Soc}(\widehat{A})\operatorname{Rad}(R) = 0$.

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. $\operatorname{Soc}(R) \cong R/\operatorname{Rad}(R)$ as left and as right R-modules. ($\operatorname{Soc}(R)$ is cyclic.)

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

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 $\mathbb{F}_q$.

Construction, continued

- The sum of the ϱ's is a generating character of general $R/\operatorname{Rad}(R)$.
- $3 \Rightarrow 1, 2$: $\operatorname{Soc}(R) \cong R/\operatorname{Rad}(R)$ has a generating character (still call it ϱ).
- $\widehat{R} \to \operatorname{Soc}(R)\widehat{\ } \to 0$ is onto.
- 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

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.*

- End of long aside.

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 $\ker \varrho$.

MacWilliams identities: Hamming weight enumerator

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

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

What if R is not Frobenius?

- If R is not Frobenius, the size condition fails; i.e., there exists a left ideal I of R with $|I| \cdot |r(I)| < |R|$.
- The MacWilliams identities also fail: evaluation at $X = Y = 1$ yields $|C| \cdot |r(C)| = |R|^n$.