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 8, 2015

Acknowledgments

- Thanks to André Leroy for organizing the conference, for inviting me to speak, and for his kind hospitality.

0. Overview of lectures

- Basic terminology
- Duality and weight enumerators
- Extension problem

Basic vocabulary

- Let R be a finite associative ring with 1.
- Let A be a finite unital left R-module; A will be the **alphabet**.
- A left R-**linear code** over A of **length** n is a left R-submodule $C \subseteq A^n$.
- Right linear codes are defined similarly.
- Due to Nechaev and collaborators, 1999.

Weights

- A **weight** on A is any function $w : A \to \mathbb{C}$ with $w(0) = 0$.
- Extend to $w : A^n \to \mathbb{C}$ by

$$w(a_1, a_2, \ldots, a_n) = \sum_{i=1}^{n} w(a_i).$$

- Restrict w to linear code $C \subseteq A^n$.

Examples

- Hamming weight: for any alphabet A, define the **Hamming weight** wt by

$$\mathrm{wt}(a) = \begin{cases} 1, & a \neq 0, \\ 0, & a = 0. \end{cases}$$

- Lee weight: for $R = A = \mathbb{Z}/N\mathbb{Z}$, restrict $-N/2 < a \leq N/2$ and set $w_L(a) = |a|$ (ordinary absolute value).
- Homogeneous weight (later).

Hamming weight enumerator

- For a linear code $C \subseteq A^n$, define the **Hamming weight enumerator** of C by
$$\mathrm{hwe}_C(X, Y) = \sum_{x \in C} X^{n-\mathrm{wt}(x)} Y^{\mathrm{wt}(x)}.$$
- $\mathrm{hwe}_C(X, Y) = \sum_{i=0}^{n} A_i X^{n-i} Y^i$, where A_i is the number of codewords in C of Hamming weight i.

Dual codes

- Let $A = R$ itself. Define the **dot product** on R^n by

$$x \cdot y = \sum_{i=1}^{n} x_i y_i,$$

where $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$.

- For a linear code $C \subseteq R^n$, define **annihilators**

$$l(C) = \{y \in R^n : y \cdot C = 0\},$$
$$r(C) = \{y \in R^n : C \cdot y = 0\}.$$

Questions

- Are the annihilators well-behaved?
- Is there a nice relationship between the Hamming weight enumerators of C and its annihilators?
  - Yes: the MacWilliams identities.
- We will discuss these questions later today.

Isometries

- Let $C_1, C_2 \subseteq A^n$ be two linear codes. An R-linear isomorphism $f : C_1 \longrightarrow C_2$ is a linear **isometry** with respect to a weight w if $w(xf) = w(x)$ for all $x \in C_1$.
- I will usually write homomorphisms of left modules M on the right side, so that $(rx)f = r(xf)$ for $r \in R$, $x \in M$.

Symmetry groups

- Suppose the alphabet A has weight w. Define **symmetry groups** by

$$
\begin{aligned}
G_{\mathrm{lt}} &= \{u \in \mathcal{U}(R) : w(ua) = w(a), a \in A\}, \\
G_{\mathrm{rt}} &= \{\phi \in GL_R(A) : w(a\phi) = w(a), a \in A\}.
\end{aligned}
$$

- Here, $\mathcal{U}(R)$ is the group of units of R, and $GL_R(A)$ is the group of invertible R-linear homomorphisms of A to itself.

Monomial transformations

- Let $G \subseteq GL_R(A)$ be a subgroup. A G-**monomial transformation** of A^n is an invertible R-linear homomorphism $T : A^n \longrightarrow A^n$ of the form

$$(a_1, a_2, \ldots, a_n)T = (a_{\sigma(1)}\phi_1, a_{\sigma(2)}\phi_2, \ldots, a_{\sigma(n)}\phi_n),$$

  for $(a_1, a_2, \ldots, a_n) \in A^n$.
- Here, σ is a permutation of $\{1, 2, \ldots, n\}$ and $\phi_i \in G$ for $i = 1, 2, \ldots, n$.

Monomial transformations are isometries

- Easy: G_{rt}-monomial transformations are isometries of A^n with respect to the weight w.
- Let $C_1 \subseteq A^n$ be a linear code and let T be a G_{rt}-monomial transformation of A^n. Set $C_2 = C_1 T$. Then the restriction of T to C_1 is a linear isometry from C_1 to C_2.
- Is the converse true? That is, does every linear isometry between linear codes extend to a G_{rt}-monomial transformation? Call this the "Extension Problem."
- More on this in the days ahead.

1. Characters

- Definitions
- Properties
- Fourier transform
- Character modules
- Generating characters

Definitions

- Let A be a finite abelian group (additive notation); A will be a module later.
- A **character** of A is a group homomorphism

$$\pi : A \longrightarrow \mathbb{C}^{\times},$$

  where $\mathbb{C}^{\times}$ is the multiplicative group of nonzero complex numbers.
- The set $\widehat{A}$ of all characters of A is a multiplicative abelian group under pointwise multiplication.
- Additive version: $\widehat{A} \cong \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})$.

Duality functor

- Pontryagin duality: $A \mapsto \widehat{A}$
- $\widehat{\widehat{A}} \cong A$, naturally.
- $\widehat{A} \cong A$, but not naturally.
- $(A \times B)\widehat{\ } \cong \widehat{A} \times \widehat{B}$.
- Exact contravariant functor:

$$0 \longrightarrow A_1 \longrightarrow A_2 \longrightarrow A_3 \longrightarrow 0$$

induces

$$0 \longrightarrow \widehat{A}_3 \longrightarrow \widehat{A}_2 \longrightarrow \widehat{A}_1 \longrightarrow 0.$$

Summation formulas

- For $a \in A$,

$$\sum_{\pi \in \widehat{A}} \pi(a) = \begin{cases} |A|, & a = 0, \\ 0, & a \neq 0. \end{cases}$$

- For $\pi \in \widehat{A}$,

$$\sum_{a \in A} \pi(a) = \begin{cases} |A|, & \pi = 1, \\ 0, & \pi \neq 1. \end{cases}$$

Linear independence

- Let $F(A, \mathbb{C}) = \{f : A \to \mathbb{C}\}$, a complex vector space of dimension $|A|$.
- The elements of $\widehat{A}$ form a basis for $F(A, \mathbb{C})$.
- In particular, characters are linearly independent over $\mathbb{C}$.
- Need multiplicative form of characters for linear independence and for the summation formulas.

Annihilators

- Let $B \subseteq A$ be any subgroup.
- Define the **annihilator** $(\widehat{A} : B)$:

$$(\widehat{A} : B) = \{\pi \in \widehat{A} : \pi(B) = 1\}.$$

- $(\widehat{A} : B) \cong (A/B)\widehat{\ }$.
- $|B| \cdot |(\widehat{A} : B)| = |A|$.
- Double annihilator: $(A : (\widehat{A} : B)) = B$.

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

$$\sum_{b \in B} f(b) = \frac{1}{|(\widehat{A} : B)|} \sum_{\pi \in (\widehat{A}:B)} \hat{f}(\pi).$$

Character modules

- Now suppose R is a finite ring with 1 and A is a finite unital left R-module.
- Then $\widehat{A}$ becomes a right R-module by

$$\pi^r(a) = \pi(ra), \quad a \in A.$$

  $({}^r\pi(a) = \pi(ar)$ for right to left case.)
- $\widehat{\ }$ is an exact contravariant functor of R-modules.
- For left R-submodule $B \subseteq A$, $(\widehat{A} : B)$ is a right R-submodule of $\widehat{A}$.

Top-bottom duality

- An R-module is **simple** if it has no nontrivial proper submodules.
- The Jacobson **radical** $\mathrm{Rad}(R)$ is the intersection of all maximal left ideals of R.
- For a left R-module A, the **socle** $\mathrm{Soc}(A)$ is the left R-submodule generated by all simple left R-submodules of A.
- $(A/\mathrm{Rad}(A)A)\widehat{\ } \cong \mathrm{Soc}(\widehat{A})$

Generating characters

- Left R-module A.
- A character $\rho \in \widehat{A}$ is a **generating character** if $\ker \rho$ contains no nonzero left R-submodules.
- Not every module admits a generating character.

Embedding

- Suppose ρ is a generating character for A.
- Define $\alpha : A \longrightarrow \widehat{R}$ by $(a\alpha)(r) = \rho(ra)$, $a \in A$, $r \in R$.
- α is an injective homomorphism of left R-modules.
- Dual map $R \longrightarrow \widehat{A}$, $r \mapsto \rho^r$, is surjective homomorphism of right R-modules.
- ρ generates $\widehat{A}$.
- Conversely: if $\widehat{A}$ is cyclic, or A embeds in $\widehat{R}$, then A has a generating character.

Frobenius rings

- Recall: $|\widehat{R}| = |R|$.
- Consider R as a module over itself.
- If R has a generating character, then $\widehat{R} \cong R$ as left and as right R-modules.
- $\mathrm{Soc}(R) = \mathrm{Soc}(\widehat{R}) \cong (R/\operatorname{Rad}(R))\widehat{\ } \cong R/\operatorname{Rad}(R)$.
- Such a finite ring is a **Frobenius** ring.

Some examples of generating characters

- $\mathbb{Z}/N\mathbb{Z}$ admits $\theta_N(a) = \exp(2\pi ia/N)$, $a \in \mathbb{Z}/N\mathbb{Z}$.
- exp is the standard complex exponential function.
- $\mathbb{F}_q$ admits $\theta_q(a) = \theta_p(\mathrm{Tr}_{q\to p}(a))$, $a \in \mathbb{F}_q$.
- $R = M_{k\times k}(\mathbb{F}_q)$ admits $\rho(P) = \theta_q(\mathrm{Tr}\, P)$, $P \in R$.
- $A = M_{k\times \ell}(\mathbb{F}_q)$, $k > \ell$, admits $\rho|_A$.
- When $k < \ell$, A does not admit a generating character. $\pi_Q(P) = \theta_q(\mathrm{Tr}(PQ))$, for $Q \in M_{\ell\times k}(\mathbb{F}_q)$. Find nonzero $X \in M_{k\times \ell}(\mathbb{F}_q)$ with $XQ = 0$, as $k < \ell$. Then $RX \subseteq \ker \pi_Q$.

Cyclic socle

- Suppose A has cyclic socle $\mathrm{Soc}(A)$.
- $\mathrm{Soc}(A)$ is a sum of matrix modules with $k \geq \ell$.
- $\mathrm{Soc}(A)$ admits a generating character: multiply together those from matrix modules.
- Extension exists, by exactness. Any extension is a generating character for A.