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 10, 2017

6. MacWilliams extension theorem and converse

- Extension property (EP)
- EP for Hamming weight over Frobenius bimodules via linear independence of characters
- Generalization for module alphabets
- Axiomatic viewpoint
- Parametrized codes and multiplicity functions
- Failure of EP for landscape matrix modules
- Converse of extension theorem: EP implies Frobenius

Notation

- Let R be a finite associative ring with 1.
- Let A be a finite unital left R-module: the **alphabet**.
- Let $w : A \to \mathbb{Q}$ be a **weight**: $w(0) = 0$. Extend to A^n by

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

Symmetry groups

- Define the **symmetry groups** of w:

$$G_{\mathrm{lt}} = \{u \in \mathcal{U}(R) : w(ua) = w(a), a \in A\},$$
$$G_{\mathrm{rt}} = \{\phi \in \mathrm{GL}_R(A) : w(a\phi) = w(a), a \in A\}.$$

- $\mathcal{U}(R)$ is the group of units of R, and $\mathrm{GL}_R(A)$ is the group of invertible R-linear homomorphisms $A \to A$.
- I will usually write homomorphisms of left modules on the right side; $f : A \to A$, $(ra)f = r(af)$.

Monomial transformations

- For a subgroup $G \subseteq \mathrm{GL}_R(A)$, a G-**monomial transformation** of A^n is an invertible R-linear homomorphism $T : A^n \to A^n$ 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 $i = 1, 2, \ldots, n$.

Isometries

- Let $C_1, C_2 \subseteq A^n$ be two linear codes. An R-linear isomorphism $f : C_1 \to C_2$ is a linear **isometry** with respect to w if $w(xf) = w(x)$ for all $x \in C_1$.
- Every G_{rt}-monomial transformation is an isometry from A^n to itself.

Extension property (EP)

- Given ring R, alphabet A, and weight w on A.
- The alphabet A has the **extension property** (EP) with respect to w if the following holds: For any left linear codes $C_1, C_2 \subseteq A^n$, if $f : C_1 \to C_2$ is a linear isometry, then f extends to a G_{rt}-monomial transformation $A^n \to A^n$.
- That is, there exists a G_{rt}-monomial transformation $T : A^n \to A^n$ such that $xT = xf$ for all $x \in C_1$.

Slightly different point of view

- Linear codes are often presented by generator matrices. A generator matrix serves as a linear encoder from an information space to a message space.
- If $f : C_1 \to C_2$ is a linear isometry, then C_1 and C_2 are isomorphic as R-modules. Let M be a left R-module isomorphic to C_1 and C_2. Call M the **information module**.
- Then C_1 and C_2 are the images of R-linear homomorphisms $\Lambda : M \to A^n$ and $N : M \to A^n$, respectively. Then, $N = \Lambda f$: inputs on left!

Coordinate functionals

- C_1 was given by $\Lambda : M \to A^n$. Write the individual components as $\Lambda = (\lambda_1, \ldots, \lambda_n)$, with $\lambda_i \in \mathrm{Hom}_R(M, A)$. Call the λ_i **coordinate functionals**.
- Similarly, $N = (\nu_1, \ldots, \nu_n)$, $\nu_i \in \mathrm{Hom}_R(M, A)$.
- The isometry f extends to a G_{rt}-monomial transformation if there exists a permutation σ and $\phi_i \in G_{\mathrm{rt}}$ such that $\nu_i = \lambda_{\sigma(i)}\phi_i$ for all $i = 1, \ldots, \boldsymbol{n}$.

Case of $\widehat{R}$

- Our first result will show that, for any finite ring R, $A = \widehat{R}$ has EP with respect to the Hamming weight.
- It follows that $A = R$ itself has EP with respect to the Hamming weight when R is Frobenius.
- The Frobenius ring case came first (1999).
- The more general $A = \widehat{R}$ case is due to Greferath, Nechaev, and Wisbauer (2004).

Techniques

- For any alphabet A, the summation formulas for characters imply that the Hamming weight wt satisfies

$$\mathrm{wt}(a) = 1 - \frac{1}{|A|} \sum_{\pi \in \widehat{A}} \pi(a), \quad a \in A.$$

- Characters are linearly independent over $\mathbb{C}$.
- Recursive argument using maximal elements in a finite poset.

Symmetry groups for the Hamming weight

- Consider the Hamming weight wt on $A = \widehat{R}$, which is an (R, R)-bimodule.
- Both symmetry groups G_{lt} and G_{rt} equal $\mathcal{U}(R)$.

Posets

- Given a set S, a (non-strict) **partial order** $\preceq$ on S is reflexive, antisymmetric, and transitive. The pair $(S, \preceq)$ is a **partially ordered set** or **poset**.
- Example. Let X be a nonempty set. Then $S = \mathcal{P}(X)$, the set of all subsets of X, with set inclusion, i.e., $U \preceq V$ when $U \subseteq V$, is a poset.
- Example. Let B be a finite right R-module. Then $S = \{bR : b \in B\}$ is the poset of all cyclic right R-submodules of B under set inclusion.
- Fact: $b_1 R = b_2 R$ if and only if $b_1 = b_2 u$, where $u \in \mathcal{U}(R)$.

Proof (a)

- R, $A = \widehat{R}$, with Hamming weight. $C_1, C_2 \subseteq \widehat{R}^n$, with $f : C_1 \to C_2$ linear isometry.
- $\widehat{R}$ has a generating character: $\rho : \widehat{R} \to \mathbb{C}$, $\rho(\pi) = \pi(1)$ for $\pi \in \widehat{R}$. (Evaluate at $1 \in R$.) Every $\pi \in \widehat{R}$ has the form $\pi = {}^r\rho$ for some unique $r \in R$.
- C_1 is image of $\Lambda : M \to \widehat{R}^n$; C_2 is image of $N : M \to \widehat{R}^n$. $N = \Lambda f$.
- Isometry: $\mathrm{wt}(x\Lambda) = \mathrm{wt}(xN)$, for all $x \in M$.

Proof (b)

- Hamming weight as character sum:

$$\sum_{i=1}^{n}\sum_{r\in R} {}^{r}\rho(x\lambda_i) = \sum_{j=1}^{n}\sum_{s\in R} {}^{s}\rho(x\nu_j), \quad x \in M.$$

- That is,

$$\sum_{i=1}^{n}\sum_{r\in R} \rho(x\lambda_i r) = \sum_{j=1}^{n}\sum_{s\in R} \rho(x\nu_j s), \quad x \in M.$$

- This is an equation of characters on M.

Proof (c)

- Let $B = \mathrm{Hom}_R(M, \widehat{R})$, a right R-module. Poset $S = \{\lambda R : \lambda \in \mathrm{Hom}_R(M, \widehat{R})\}$ under $\subseteq$.
- Among the $\lambda_i R, \nu_j R$, choose one that is maximal for $\subseteq$. Say, $\nu_1 R$.
- Let $j = 1$ and $s = 1$ on the right side of the character equation.
- By linear independence of characters, there exists i and $r \in R$ so that $\rho(x\lambda_i r) = \rho(x\nu_1)$ for all $x \in M$.
- Thus $\rho(x(\nu_1 - \lambda_i r)) = 1$ for all $x \in M$. I.e., $M(\nu_1 - \lambda_i r) \subseteq \ker \rho$.

Proof (d)

- By ρ a generating character, $\nu_1 = \lambda_i r$. Thus, $\nu_1 R \subseteq \lambda_i R$.
- By maximality of $\nu_1 R$, $\nu_1 R = \lambda_i R$. Thus, $\nu_1 = \lambda_i u_1$, for some $u_1 \in \mathcal{U}(R)$.
- Then inner sums agree: $\sum_{r \in R} \rho(x \lambda_i r) = \sum_{s \in R} \rho(x \nu_1 s)$, $x \in M$.
- Set $\sigma(1) = i$. Subtract inner sums to reduce the size of the outer sums by 1. Proceed by induction.

Generalize to module alphabets

- For ring R, alphabet A, and Hamming weight wt, EP holds if A: (1) is pseudo-injective and (2) has a cyclic socle (embeds into $\widehat{R}$).
- Pseudo-injective means injective with respect to submodules. That is, if B is a submodule of A and $h : B \to A$ is any injective module homomorphism, then h extends to $\tilde{h} : A \to A$.
- Main idea: use $\widehat{R}$-case to get $\mathrm{GL}_R(\widehat{R})$-monomial extension. Use pseudo-injectivity to show existence of $\mathrm{GL}_R(A)$-monomial extension.

Axiomatic viewpoint

- Assmus and Mattson, "Error-correcting codes: an axiomatic approach," 1963.
- Consider linear codes up to monomial equivalence. What matters?
- Actually, I want to consider parametrized codes up to monomial equivalence.
- Usual set-up: ring R, alphabet A, weight w on A.
- A **parametrized code** is a finite left R-module M and an R-linear homomorphism $\Lambda : M \to A^n$.

Scale classes

- The right symmetry group G_{rt} acts on $\mathrm{Hom}_R(M, A)$ on the right: $\lambda \mapsto \lambda\phi$.
- Call the orbit space $\mathcal{O}^\sharp = \mathrm{Hom}_R(M, A)/G_{\mathrm{rt}}$. Denote orbit/"scale class" of λ by $[\lambda]$.
- Up to G_{rt}-monomial equivalence, a parametrized code $\Lambda : M \to A^n$ is completely determined by the number of coordinate functionals λ_i belonging to the various classes $[\lambda] \in \mathcal{O}^\sharp$.

Multiplicity functions

- Let $F(\mathcal{O}^\sharp, \mathbb{N})$ denote the set of functions $\eta : \mathcal{O}^\sharp \to \mathbb{N}$. Call these **multiplicity functions**.
- Given a parametrized code $\Lambda : M \to A^n$, define its multiplicity function η_Λ by

$$\eta_\Lambda([\lambda]) = |\{i : \lambda_i \in [\lambda]\}|.$$

- Other authors: multisets, value function (Chen, et al.), projective systems, etc.
- No zero columns: $F_0(\mathcal{O}^\sharp, \mathbb{N}) = \{\eta : \eta([0]) = 0\}$.

Weights of elements

- Given $\Lambda : M \to A^n$, consider the weights $w(x\Lambda)$ for $x \in M$.
- The weights $w(x\Lambda)$, $x \in M$, depend only on η_Λ, not Λ itself: G_{rt}-monomial transformations are isometries. In fact:

$$w(x\Lambda) = \sum_{[\lambda] \in \mathcal{O}^\sharp} w(x\lambda)\eta_\Lambda([\lambda]), \quad x \in M.$$

Invariance under G_{lt}

- If $u \in G_{\mathrm{lt}}$, then $w((ux)\Lambda) = w(u(x\Lambda)) = w(x\Lambda)$, for all $x \in M$.
- G_{lt} acts on M on the left: $x \mapsto ux$, $x \in M$. Denote orbit space by $\mathcal{O} = G_{\mathrm{lt}} \backslash M$.
- $w(0\Lambda) = w(0) = 0$.
- Denote $F_0(\mathcal{O}, \mathbb{Q}) = \{f : \mathcal{O} \to \mathbb{Q}, f(0) = 0\}$.

Well-defined W map

- We get a well-defined map

$$W : F_0(\mathcal{O}^\sharp, \mathbb{N}) \to F_0(\mathcal{O}, \mathbb{Q}),$$

with

$$W(\eta)(x) = \sum_{[\lambda] \in \mathcal{O}^\sharp} w(x\lambda)\eta([\lambda]),$$

for $x \in \mathcal{O}$, $\eta \in F_0(\mathcal{O}^\sharp, \mathbb{N})$.

Completion over $\mathbb{Q}$

- $F_0(\mathcal{O}^\sharp, \mathbb{N})$ is an additive semi-group, and $F_0(\mathcal{O}, \mathbb{Q})$ is a $\mathbb{Q}$-vector space. The map W is additive.
- The addition in $F_0(\mathcal{O}^\sharp, \mathbb{N})$ corresponds to concatenation of generator matrices.
- By tensoring over $\mathbb{Q}$, we get a $\mathbb{Q}$-linear transformation of $\mathbb{Q}$-vector spaces:

$$W : F_0(\mathcal{O}^\sharp, \mathbb{Q}) \to F_0(\mathcal{O}, \mathbb{Q}).$$

Re-interpretation of EP

- An alphabet A has EP with respect to a $\mathbb{Q}$-valued weight w if and only if the linear map
$$W : F_0(\mathcal{O}^\sharp, \mathbb{Q}) \to F_0(\mathcal{O}, \mathbb{Q})$$
is injective for all information modules M.
- Bogart, et al., 1978.
- Greferath, 2002.

Matrix modules and Hamming weight

- What does W look like for matrix module alphabets?
- Let $R = M_{k\times k}(\mathbb{F}_q)$, $A = M_{k\times\ell}(\mathbb{F}_q)$, with Hamming weight wt.
- Symmetry groups: $G_{\mathrm{lt}} = \mathcal{U}(R) = \mathrm{GL}(k, \mathbb{F}_q)$; $G_{\mathrm{rt}} = \mathrm{GL}_R(A) = \mathrm{GL}(\ell, \mathbb{F}_q)$.

Orbit spaces

- For $M = M_{k\times m}(\mathbb{F}_q)$, $\mathrm{Hom}_R(M, A) = M_{m\times\ell}(\mathbb{F}_q)$.
- Then $\mathcal{O} = G_{\mathrm{lt}}\backslash M = \mathrm{GL}(k, \mathbb{F}_q)\backslash M_{k\times m}(\mathbb{F}_q)$, which is represented by the set of row reduced echelon (RRE) matrices of size $k \times m$.
- And $\mathcal{O}^\sharp = \mathrm{Hom}_R(M, A)/G_{\mathrm{rt}} = M_{m\times\ell}(\mathbb{F}_q)/\,\mathrm{GL}(\ell, \mathbb{F}_q)$, which is represented by the set of column reduced echelon (CRE) matrices of size $m \times \ell$.

Dimension counting

- First note that $\dim_{\mathbb{Q}} F_0(\mathcal{O}, \mathbb{Q}) = |\mathcal{O}| - 1$ and $\dim_{\mathbb{Q}} F_0(\mathcal{O}^\sharp, \mathbb{Q}) = |\mathcal{O}^\sharp| - 1$.
- So, $\dim_{\mathbb{Q}} F_0(\mathcal{O}, \mathbb{Q})$ is the number of nonzero RRE matrices of size $k \times m$.
- And $\dim_{\mathbb{Q}} F_0(\mathcal{O}^\sharp, \mathbb{Q})$ is the number of nonzero CRE matrices of size $m \times \ell$.
- If $k < \ell$ and $k < m$, there are more of the CRE matrices than the RRE matrices; i.e.,

$$\dim_{\mathbb{Q}} F_0(\mathcal{O}^\sharp, \mathbb{Q}) > \dim_{\mathbb{Q}} F_0(\mathcal{O}, \mathbb{Q}).$$

- This says that EP fails when $k < \ell$. ("Landscape")

Converse of EP for Hamming weight

- We claim: if an alphabet A has EP for the Hamming weight, then A (1) is pseudo-injective and (2) has a cyclic socle.
- Likewise: if a ring R has EP for the Hamming weight, then R is Frobenius (which means $\mathrm{Soc}(R)$ is cyclic).
- We follow a strategy of Dinh and López-Permouth, 2004.

Proof

- If $\mathrm{Soc}(A)$ is not cyclic (same idea for R), then $\mathrm{Soc}(A)$ contains a matrix module of the form $A' = M_{k\times\ell}(\mathbb{F}_q)$ with $k < \ell$.
- There exist counter-examples to EP over A'.
- Regard these codes as codes over A: $A' \subseteq \mathrm{Soc}(A) \subseteq A$.
- They are also counter-examples over A.
- Pseudo-injectivity is equivalent to the length 1 case of EP (Dinh, López-Permouth).

Other uses of W map

- We will see the W map again.
- Other weight functions.
- Isometries of additive codes.