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 9, 2018

7. Converse of the MacWilliams extension theorem

- Axiomatic viewpoint
- Parametrized codes and multiplicity functions
- Failure of EP for landscape matrix modules
- Converse of extension theorem: EP implies Frobenius
- Application: linear one-weight codes

Recall: 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 $x \in C_1$.

Recall: 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!

Recall: 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 $i = 1, \ldots, n$.

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: value function (Chen, et al.), multisets, 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 monoid, 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: $G_{\mathsf{lt}} = \mathcal{U}(R) = \mathsf{GL}(k, \mathbb{F}_q)$; $G_{\mathsf{rt}} = \mathsf{GL}_R(A) = \mathsf{GL}(\ell, \mathbb{F}_q)$.

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 (i)

- 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 $m \times \ell$.

Dimension counting (ii)

- 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).
- Use: 2004 strategy of Dinh and López-Permouth.

Proof (i)

- We will prove the module case. The argument is similar for ring alphabets
- Earlier, we saw: pseudo-injectivity is equivalent to the length 1 case of EP (Dinh, López-Permouth).
- If Soc(A) is not cyclic, then Soc(A) contains a matrix module of the form $A' = M_{k\times\ell}(\mathbb{F}_q)$ with $k < \ell$. So A' is a "landscape" module.
- There exist counter-examples to EP over A'.

Proof (ii)

- There exist counter-examples to EP over A'.
- Because $A' \subseteq \mathrm{Soc}(A) \subseteq A$, we may regard R-linear codes over A' as R-linear codes over A.
- The Hamming weights of elements do not change when the alphabet changes.
- The counter-examples over A' are also counter-examples over A.

Setting for the rest of the lecture

- Finite ring R, alphabet $A = \widehat{R}$, weight w on A, information module M.
- When R is Frobenius, $A = R$.
- W-map: $W : F_0(\mathcal{O}^\sharp, \mathbb{Q}) \to F_0(\mathcal{O}, \mathbb{Q})$.
- EP holds for w if and only if W is injective for every M.

Definition

- An R-linear code $C \subseteq \widehat{R}^n$ is a **one-weight code** if there exists a constant w_0 such that $w(c) = w_0$ for all nonzero $c \in C$.
- Example (Lecture 1): $A = R = \mathbb{F}_2$, $n = 7$, $k = 3$. A **simplex code**:

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

- Codewords: 0000000, 0001111, 0110011, 1010101, 0111100, 1011010, 1100110, 1101001. $w_0 = 4$.

Using multiplicity functions

- Suppose EP holds for weight w on $A = \widehat{R}$.
- Example: the Hamming weight.
- Any R-linear code C over A is modeled by $\Lambda : M \to A^n$, with multiplicity function η.
- C is a one-weight code if and only if $W(\eta) \in F_0(\mathcal{O}, \mathbb{Q})$ is a constant function.

Using EP: uniqueness theorem

- The constant functions form a one-dimensional subspace S of $F_0(\mathcal{O}, \mathbb{Q})$.
- If EP holds for w, $W : F_0(\mathcal{O}^\sharp, \mathbb{Q}) \to F_0(\mathcal{O}, \mathbb{Q})$ is injective. Then $W^{-1}(S)$ has dimension 0 or 1.
- For a fixed M: if one-weight codes exist at all, they are unique up to **replication** (concatenation, repeating columns).
- Weiss (1966, binary), Bonisoli (1983): one-weight codes are replications of simplex codes (as in the example).

Guess and check

- Fix M. If one can **guess** a formula for η and **check** that all weights agree, then every one-weight code modeled on M must be a multiple of η.

Dangers!

- Caveat! η might be a replication of a shorter example.
- A priori, η could have rational values. Clear denominators to get integer values.
- If all the $\pm$-signs are the same, then $\pm\eta$ solves the problem.
- However, if the signs are mixed (some positive, some negative), this proves that classical one-weight codes modeled on M do not exist.

One-weight example/non-example

- Let $R = A = \mathbb{Z}/9\mathbb{Z}$ with Hamming weight, $M = R^2$.
- Generator matrix: columns with multiplicities above.

3	3	3	3	3	3	3	3	3	3	3	3	-2	-2	-2	-2
0	1	1	1	1	1	1	1	1	1	3	3	0	3	3	3
1	0	1	2	3	4	5	6	7	8	1	2	3	0	3	6

- All nonzero codewords have Hamming weight 27.
- Classical linear one-weight code for $M = R^2$ does not exist. (Classical: all $\eta([\lambda]) \geq 0$.)

A sample of results over $\mathbb{Z}/N\mathbb{Z}$

- Hamming weight: one-weight linear codes of arbitrary dimension occur when $N = p$ is prime. (field case; Bonisoli)
- Hamming weight: if N is not prime, need information module M to be free of rank 1.
- Lee or Euclidean weight: always exist when $N = 2^k$ (Carlet in Lee case); relatively rare otherwise (rank restrictions).

Lee and Euclidean weights over $\mathbb{Z}/4\mathbb{Z}$

- Let $R = A = \mathbb{Z}/4\mathbb{Z}$, $M = R^2$.
- Lee ($\mathrm{L}(a)$) and Euclidean ($\mathrm{E}(a)$) weights

a	0	1	2	3
$\mathrm{L}(a)$	0	1	2	1
$\mathrm{E}(a)$	0	1	4	1

- Lecture 8: $\mathbb{Z}/4\mathbb{Z}$ has EP with respect to both weights.

One-weight examples over $\mathbb{Z}/4\mathbb{Z}$

- Generator matrix: column types below, with multiplicities above.

2	2	2	2	2	2	1	1	1
1	1	1	1	1	1	1	1	1
0	1	1	1	1	2	0	2	2
1	0	1	2	3	1	2	0	2

- Upper multiplicities: length 15, $\mathrm{L}(c) = 16$.
- Lower multiplicities: length 9, $\mathrm{E}(c) = 16$.

Other uses of W map

- We will see the W map again.
- Other weight functions (Lecture 8).
- Isometries of additive codes (Research lecture 1).