Foundational Aspects of Linear Codes: 4. Extension property: necessary conditions

Jay A. Wood

Department of Mathematics
Western Michigan University
http://homepages.wmich.edu/∼jwood/

On the Algebraic and Geometric Classifications of Projective Varieties
University of Messina
June 23, 2016

4. Extension property: necessary conditions

- Axiomatic viewpoint
- Parametrized codes and multiplicity functions
- W map
- 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

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

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

- $\mathcal{U}(R)$ is the group of units of R, and $GL_R(A)$ is the group of invertible R-linear homomorphisms $A \to A$.
- Recall that I will usually write homomorphisms of left modules on the right side.

Axiomatic viewpoint

- Assmus and Mattson, "Error-correcting codes: an axiomatic approach," 1963.
- Consider linear codes up to monomial equivalence.
- 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: $G_{\text{lt}} = \mathcal{U}(R) = GL(k, \mathbb{F}_q)$; $G_{\text{rt}} = GL_R(A) = GL(\ell, \mathbb{F}_q)$.

Orbit spaces

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

Compare to previous lecture

- We have seen the W map before.
- Suppose $M = R$. Then $\mathrm{Hom}_R(R, A) = A$ because $r\lambda = r(1\lambda) = ra$, where $a = 1\lambda$.
- This yields the W matrix of the last lecture.
- Rank condition for W matrix is equivalent to W map being injective.

Other uses of W map

- Linear one-weight codes: next.
- Isometries groups of additive codes: research seminar.

One-weight and relative one-weight codes: overview

- Definitions
- Using EP: uniqueness theorem
- Guess and check
- Homogeneous weight
- Key lemma: sum over submodules of $\mathrm{Hom}_R(M, A)$
- Converse: only way to get relative one-weight codes
- Concatenate to get certain two-weight codes
- Examples

Setting

- 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 information module M.

Definitions

- 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 $c \in C$.
- Fix an R-linear code $C \subseteq \widehat{R}^n$ and a linear subcode C_1. (Liu-Chen) C is a **relative one-weight code** with respect to C_1 if there exists a constant w_0 such that $w(c) = w_0$ for all $c \in C$ with $c \notin C_1$.

Using multiplicity functions

- Suppose EP holds for weight w on $A = \widehat{R}$.
- Examples: an egalitarian weight or 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, Bonisoli: binary one-weight codes are replications of simplex codes.

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.
- Caveat! 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.

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.

Egalitarian weight

- Recall that an egalitarian weight w has the property that there exists a constant γ such that

$$\sum_{b \in B} w(a_0 + b) = \gamma |B|,$$

  for any nonzero submodule B of $A = \widehat{R}$ and $a_0 \in A$.
- For any M, set $\eta(\lambda) = 1$ for all nonzero $\lambda \in \mathrm{Hom}_R(M, A)$. (Use every column-type once.)
- Then η defines a one-weight code with weight $\gamma |\mathrm{Hom}_R(M, A)|$.

Proof

- Take any nonzero $x \in M$. Define

$$\check{x} : \mathrm{Hom}_R(M, A) \to A, \quad \lambda \mapsto x\lambda.$$

  $\check{x}$ is a homomorphism of right R-modules.
- Image $\mathrm{im}\,\check{x}$ is a nonzero submodule of A.

$$\begin{aligned} W(\eta)(x) &= \sum_{\lambda} w(x\lambda) = |\ker \check{x}| \sum_{b \in \mathrm{im}\,\check{x}} w(b) \\ &= \gamma |\mathrm{im}\,\check{x}||\ker \check{x}| = \gamma |\mathrm{Hom}_R(M, A)| \end{aligned}$$

Key lemma: sum over cosets in $\mathrm{Hom}_R(M, A)$

- Generalize this idea: let $E \subseteq \mathrm{Hom}_R(M, A)$ be a right R-submodule.
- Define $E^\circ = \{x \in M : x\lambda = 0, \lambda \in E\}$, left submodule of M.
- Let λ_0 be any element of $\mathrm{Hom}_R(M, A)$. Then

$$\sum_{\lambda \in \lambda_0 + E} w(x\lambda) = \begin{cases} w(x\lambda_0)|E|, & x \in E^\circ, \\ \gamma|E|, & x \notin E^\circ. \end{cases}$$

Producing relative one-weight codes

- Set $E = M_1^\circ = \{\lambda \in \mathrm{Hom}_R(M, A) : M_1\lambda = 0\}$, for submodule $M_1 \subset M$. Then $E^\circ = M_1$.

Theorem

Suppose η is constant along the cosets of E in $\mathrm{Hom}_R(M, A)$. Then η defines a relative one-weight code relative to M_1.

- Apply key lemma on each coset. $W(\eta)(x)$ does not depend on x provided $x \notin M_1$.
- Converse is true, but harder.

Concatenate to get certain two-weight codes

- Addition of multiplicity functions corresponds to concatenation of generator matrices. Weights of codewords add.
- Key lemma with $\lambda_0 = 0$:

$$\sum_{\lambda \in E} w(x\lambda) = \begin{cases} 0, & x \in E^\circ, \\ \gamma|E|, & x \notin E^\circ. \end{cases}$$

- Put these together for different choices of E.

Example (a)

- Let $M_1 \subset M$. Set $E_1 = M_1^{\circ}$.
- Define $\eta_1(\lambda) = s_1$ for $\lambda \in E_1$ and 0 elsewhere.
  Define $\eta_2(\lambda) = s_2$ for all $\lambda \in \mathrm{Hom}_R(M, A)$.
- For $\eta = \eta_1 + \eta_2$ and $x \neq 0$:

$$W(\eta)(x) = \begin{cases} s_2\gamma|\mathrm{Hom}_R(M, A)|, & x \in M_1, \\ s_1\gamma|E| + s_2\gamma|\mathrm{Hom}_R(M, A)|, & x \notin M_1. \end{cases}$$

Example (b)

- More specifically, let $R = A = \mathbb{F}_q$, $M = \mathbb{F}_q^m$, $M_1 = \{(*, 0, \ldots, 0)\} \cong \mathbb{F}_q$.
- Then $|\mathrm{Hom}_R(M, A)| = q^m$ and $|E| = q^{m-1}$.
- Set $s_2 = 1$, $s_1 = -1$, $\gamma = (q-1)/q$ (Hamming). Then, $n = (q-1)q^{m-1}$ and, for $x \neq 0$:

$$W(\eta)(x) = \begin{cases} (q-1)q^{m-1}, & x \in M_1, \\ (q-1)^2 q^{m-2}, & x \notin M_1. \end{cases}$$

- A $(q-1)$-fold replicate of a generalized Reed-Muller code $GRM(m-1, 1, q)$.