

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 10, 2015

5. Isometries of additive codes

- ▶ Additive codes as linear codes over modules
- ▶ Failure of EP
- ▶ Monomial and isometry groups
- ▶ Examples
- ▶ Criteria in terms of multiplicity functions
- ▶ Structure of $\ker W$
- ▶ Building codes with prescribed groups
- ▶ EP for short codes
- ▶ Extreme examples

Additive \mathbb{F}_4 -codes

- ▶ There has been interest in additive codes with alphabet $A = \mathbb{F}_4$.
- ▶ Such codes are the same as R -linear codes over A with $R = \mathbb{F}_2$ and $A = \mathbb{F}_4$, regarding \mathbb{F}_4 as an \mathbb{F}_2 -vector space of dimension 2.
- ▶ Generalize to case of $R = M_{k \times k}(\mathbb{F}_q)$ and $A = M_{k \times \ell}(\mathbb{F}_q)$. Information module will be $M = M_{k \times m}(\mathbb{F}_q)$.
- ▶ Call this the **matrix module context**.

Failure of EP

- ▶ Recall that EP for Hamming weight fails in the matrix module context when $k < \ell$ and $k < m$.
- ▶ In terms of the W -map:

$$W : F_0(\mathcal{O}^\#, \mathbb{Q}) \rightarrow F_0(\mathcal{O}, \mathbb{Q})$$

fails to be injective for all information modules M .

Isometry group

- ▶ General set-up: ring R , alphabet A , weight w on A .
- ▶ Let $C \subseteq A^n$ be an R -linear code.
- ▶ Consider linear isometries $f : C \rightarrow C$; i.e., $w(cf) = w(c)$, for all $c \in C$.
- ▶ When C is given as the image of a parametrized code $\Lambda : M \rightarrow A^n$, we define the **isometry group**:

$$\text{Isom}(C) = \{g \in GL_R(M) : \text{there exists a linear isometry } f : C \rightarrow C \text{ such that } g\Lambda = \Lambda f\}.$$

- ▶ View isometries on M rather than C .

Monomial group

- ▶ Recall that the weight w on A has a right symmetry group G_{rt} .
- ▶ For linear code $C \subseteq A^n$, define the **monomial group**

$$\text{Monom}(C) = \{T : A^n \rightarrow A^n, G_{rt}\text{-monomial transformation, with } CT = C\}.$$

Restriction map

- ▶ Any $T \in \text{Monom}(C)$, when restricted to C , gives an isometry on C . By viewing the isometry on M , we get a group homomorphism

$$\text{restr} : \text{Monom}(C) \rightarrow \text{Isom}(C).$$

- ▶ Denote $\ker \text{restr} = \text{Monom}_0(C)$. Think of repeated columns in a generator matrix.
- ▶ If EP holds, then restr is surjective.

Main question

- ▶ When EP fails, restr may not be surjective for all linear codes C or information modules M .
- ▶ Then $\text{restr}(\text{Monom}(C)) \subseteq \text{Isom}(C) \subseteq GL_R(M)$.
- ▶ What subgroups of $GL_R(M)$ can occur as $\text{restr}(\text{Monom}(C))$ and $\text{Isom}(C)$?

Example 1 (a)

- ▶ Additive code over $\mathbb{F}_4 = \mathbb{F}_2[\omega]/(\omega^2 + \omega + 1)$ with generator matrix G_1 and list of codewords. $M = \mathbb{F}_2^3$.

$$G_1 = \begin{bmatrix} 1 & \omega & 0 \\ \omega & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix},$$

$$\begin{array}{ccc} 0 & 0 & 0 \\ 1 & \omega & 0 \\ \omega & 1 & 0 \\ \omega^2 & \omega^2 & 0 \\ 1 & 0 & 1 \\ 0 & \omega & 1 \\ \omega^2 & 1 & 1 \\ \omega & \omega^2 & 1 \end{array}$$

Example 1 (b)

- ▶ Consider three elements of $GL_R(M) = GL(3, \mathbb{F}_2)$:

$$f_1 = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad f_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \quad f_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

- ▶ f_1, f_2 generate $\text{restr}(\text{Monom}(C))$, a Klein 4-group. But f_1, f_3 generate $\text{Isom}(C)$, a dihedral group of order 8. ($f_2 = f_1 f_3^2$.)
- ▶ Magma found only the cyclic 2-group generated by $f_1 f_2$.

Example 2 (a)

- ▶ Additive code over \mathbb{F}_4 with generator matrix G_2 and list of codewords. Again, $M = \mathbb{F}_2^3$.

$$G_2 = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & \omega & \omega \\ \omega & \omega & 1 & 0 & \omega^2 \end{pmatrix},$$

$$\begin{matrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & \omega & \omega \\ 1 & 1 & 0 & \omega^2 & \omega^2 \\ \omega & \omega & 1 & 0 & \omega^2 \\ \omega & \omega^2 & 0 & 1 & \omega \\ \omega^2 & \omega & 0 & \omega & 1 \\ \omega^2 & \omega^2 & 1 & \omega^2 & 0 \end{matrix}$$

Example 2 (b)

- ▶ Consider three elements of $GL_R(M) = GL(3, \mathbb{F}_2)$:

$$f_4 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad f_5 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}, \quad f_6 = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

- ▶ These elements generate $\text{restr}(\text{Monom}(C)) \cong \Sigma_4$, the symmetric group on 4 elements, while $\text{Isom}(C) = GL(3, \mathbb{F}_2)$, the simple group of order 168.
- ▶ Magma found only a cyclic 4-group generated by $f = f_4 f_5 f_6 f_4 f_5 f_4 f_6$.

Closure for group actions

- ▶ Some of the hypotheses of the main result involve a notion of **closure** with respect to a group action.
- ▶ This idea goes back at least to Wielandt, 1964.
- ▶ Suppose a finite group G acts on a set X .
- ▶ A subgroup $H \subseteq G$ partitions X into H -orbits.
- ▶ Define the **closure** of H with respect to the action:

$$\bar{H} = \{g \in G : g \text{ orb}_H(x) = \text{orb}_H(x), x \in X\}.$$

- ▶ Subgroup $H \subseteq G$ is **closed** with respect to the action if $\bar{H} = H$.

Closure conditions

- ▶ Usual set-up: ring R , alphabet A , weight w , information module M . Orbit spaces \mathcal{O} and \mathcal{O}^\sharp .
- ▶ $\mathcal{O} = G_{\text{lt}} \backslash M$: $GL_R(M)$ acts on the right, and on the left of $F_0(\mathcal{O}, \mathbb{Q})$.
- ▶ $\mathcal{O}^\sharp = \text{Hom}_R(M, A) / G_{\text{rt}}$: $GL_R(M)$ acts on the left, and on the right of $F_0(\mathcal{O}^\sharp, \mathbb{Q})$: $(\eta f)([\lambda]) = \eta([f \lambda])$.
- ▶ For $H_1 \subseteq H_2 \subseteq GL_R(M)$, will want H_1 to be closed for the \mathcal{O}^\sharp -action and H_2 closed for the \mathcal{O} -action.
- ▶ “Not every subgroup gets to be an isometry group.”

Statement of main result

Theorem

Matrix module context with $k < \ell < m$. For any choice of subgroups $H_1 \subseteq H_2 \subseteq GL_R(M)$ with H_1 closed for the \mathcal{O}^\sharp -action and H_2 closed for the \mathcal{O} -action, there exists a linear code C modeled on M such that $H_1 = \text{restr}(\text{Monom}(C))$ and $H_2 = \text{Isom}(C)$.

Corollary

Same matrix module context. There exists a linear code C modeled on M with $\text{restr}(\text{Monom}(C)) = \{\mathbb{F}_q^\times \cdot \text{id}_M\}$ and $\text{Isom}(C) = GL_R(M)$.

Using multiplicity functions

- ▶ Up to G_{rt} -monomial transformations, a parametrized code $\Lambda : M \rightarrow A^n$ is determined by its multiplicity function $\eta_\Lambda \in F_0(\mathcal{O}^\#, \mathbb{N})$.
- ▶ Recall the W -map: $W : F_0(\mathcal{O}^\#, \mathbb{Q}) \rightarrow F_0(\mathcal{O}, \mathbb{Q})$.
- ▶ Recall the right action of $GL_R(M)$ on $F_0(\mathcal{O}^\#, \mathbb{Q})$:
 $(\eta f)([\lambda]) = \eta([f\lambda])$.
- ▶ For $f \in GL_R(M)$, $f \in \text{restr}(\text{Monom}(\eta))$ if and only if $\eta f = \eta$.
- ▶ For $f \in GL_R(M)$, $f \in \text{Isom}(\eta)$ if and only if $\eta f - \eta \in \ker W$.

Structure of $\ker W$ (a)

- ▶ In the matrix module context, $\mathcal{O}^\#$ is the set of CRE matrices of size $m \times \ell$, while \mathcal{O} is the set of RRE matrices of size $k \times m$.
- ▶ Remember $k < \ell < m$. By dimension counting,

$$\ker W \geq \sum_{i=k+1}^{\ell} \begin{bmatrix} m \\ i \end{bmatrix}_q, \quad (1)$$

using the q -binomial coefficients.

Structure of $\ker W$ (b)

- ▶ The orbit space \mathcal{O}^\sharp is partitioned by rank.
- ▶ By explicit constructions, one produces independent elements $\eta_{[\lambda]} \in \ker W$. For each $i = k + 1, \dots, \ell$, one produces $\binom{m}{i}_q$ of them, each $\eta_{[\lambda]}$ supported on $[\lambda]$ of rank i and on specific elements of smaller rank. (“Triangular.”) This produces as many independent elements of $\ker W$ as the sum in (1).
- ▶ Separately, one shows that W is surjective, so there is equality in (1), and we have an explicit basis for $\ker W$.

Aside: EP for short codes

- ▶ Serhii Dyshko (Toulon) has shown that EP holds even when $k < \ell$, **provided** n is sufficiently small ($n \leq q$ when $k = 1$).
- ▶ Elements of $\ker W$ affect the length of the code.
- ▶ The exact details of this need to be better understood.

Idea of proof (a)

- ▶ Elements $[x] \in \mathcal{O}$ have a well-defined rank, $\text{rk}[x]$. The $GL_R(M)$ -action preserves this rank.
- ▶ Pick a function w on \mathcal{O} that (1) is constant on each and separates the H_2 -orbits on \mathcal{O} and (2) is an increasing function of $\text{rk}[x]$.
- ▶ Because W is surjective, there exists η with $W(\eta) = w$. A priori, η has rational values.
- ▶ Can modify η to have non-negative integer values and still satisfy (1) and (2).

Idea of proof (b)

- ▶ Replace η by an averaged version so that η is also constant of the H_2 -orbits on \mathcal{O}^\sharp . This does not change $W(\eta)$. Clear denominators of η , which scales everything.
- ▶ At this point, η has non-negative integer values, is constant on H_2 -orbits on \mathcal{O}^\sharp , and is constant on and separates H_2 -orbits on \mathcal{O} .

Idea of proof (c)

- ▶ Claim $\text{restr}(\text{Monom}(\eta)) = \text{Isom}(\eta) = H_2$.
- ▶ From η constant on H_2 -orbits on \mathcal{O}^\sharp ,
 $H_2 \subseteq \text{restr}(\text{Monom}(\eta))$.
- ▶ We always have $\text{restr}(\text{Monom}(\eta)) \subseteq \text{Isom}(\eta)$.
- ▶ Suppose $f \in \text{Isom}(\eta)$. Because $w = W(\eta)$ separates H_2 -orbits on \mathcal{O} , $w(xf) = w(x)$ implies $f \in \bar{H}_2$. The closure hypothesis implies $f \in H_2$.

Idea of proof (d)

- ▶ Modify η using $\eta_{[\lambda]} \in \ker W$ to separate H_1 -orbits on \mathcal{O}^\sharp (rank-by-rank, from rank ℓ down to rank $k + 1$).
- ▶ Because of “triangular” form of $\eta_{[\lambda]}$, a change at rank i does not disturb changes at higher ranks.
- ▶ The final η preserves H_1 -orbits on \mathcal{O}^\sharp , so $H_1 \subseteq \text{restr}(\text{Monom}(\eta))$. Conversely, any $f \in \text{restr}(\text{Monom}(\eta))$ preserves H_1 -orbits on \mathcal{O}^\sharp (η separates), so $f \in \bar{H}_1$. Closure implies $f \in H_1$.
- ▶ Because modifications were made by $\eta_{[\lambda]} \in \ker W$, $W(\eta)$ has not changed. We still have $\text{Isom}(\eta) = H_2$.

Extreme example (a)

- ▶ $R = \mathbb{F}_2$, $A = \mathbb{F}_4$, $M = \mathbb{F}_2^3$. Multiplicities as indicated. Length $n = 28$.

| multiplicity | 1 | 4 | 2 | 2 | 4 | 1 | 3 | 5 | 6 |
|--------------|---|---|---|----------|----------|----------|------------|----------|----------|
| G | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 |
| | 0 | 1 | 1 | ω | ω | ω | ω | 0 | 1 |
| | 1 | 0 | 1 | 0 | ω | 1 | ω^2 | ω | ω |

- ▶ All codewords have weight 22, so $\text{Isom}(C) = GL(3, \mathbb{F}_2)$, while $\text{restr}(\text{Monom}(C)) = \{\text{id}_M\}$.

Extreme example (b)

- Additive code over $\mathbb{F}_9 = \mathbb{F}_3[\omega]/(\omega^2 - \omega - 1)$.

| | | | | | | | | | | | | |
|----------|----------|----------|----------|----------|----------|--------------|--------------|-----------|---------------|---------------|----------|----------|
| mult. | 5 | 3 | 6 | 1 | 1 | 1 | 2 | 2 | 2 | 4 | 3 | 2 |
| G_3 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | -1 | -1 | -1 |
| | 1 | 1 | -1 | 0 | 1 | -1 | 0 | 1 | -1 | 0 | 1 | -1 |
| 6 | 3 | 7 | 8 | 9 | 6 | 4 | 5 | 2 | 3 | 1 | | |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 0 | 1 | ω | ω | ω | ω | ω | ω | ω | ω | ω | ω | ω |
| ω | ω | 0 | 1 | -1 | ω | $\omega + 1$ | $\omega - 1$ | $-\omega$ | $-\omega + 1$ | $-\omega - 1$ | | |

Extreme example (b) continued

- ▶ Code has length $n = 86$; all codewords have weight 72.
- ▶ $\text{Isom}(C) = GL(3, \mathbb{F}_3)$, of order 11, 232.
- ▶ $\text{restr}(\text{Monom}(C)) = \{\pm \text{id}_M\}$ is minimum possible.

Other alphabets

- ▶ Most of the result carries over to any alphabet with non-cyclic socle, such as non-Frobenius rings.
- ▶ Get $\text{restr}(\text{Monom}(\eta)) \subseteq H_1$ only, but still have $H_2 = \text{Isom}(\eta)$.
- ▶ This is enough to get the extreme cases.