Groups of Isometries of Additive Codes over $GF(q)$

Jay A. Wood

Department of Mathematics
Western Michigan University
http://sites.google.com/a/wmich.edu/jaywood

Finite Algebraic Combinatorics and Applications
Mathematical Congress of the Americas
Montréal, Québec
July 28, 2017

Outline

- Additive codes
- Additive codes as linear codes over modules
- Monomial and isometry groups
- Extension property and its failure
- EP for short codes
- Examples
- Necessary conditions
- Building codes with prescribed groups
- Extreme examples

Additive codes

- There has been interest in additive codes with alphabet $A = \mathbb{F}_4$.
- Same ideas apply to $A = \mathbb{F}_q$.
- An **additive $\mathbb{F}_q$-code** is an additive subgroup $C \subseteq \mathbb{F}_q^n$.
- Linear codes are examples, but additive codes need not be closed under (all) scalar multiplications.

Additive codes as linear codes over modules

- Given a finite ring R with 1 and a finite unital left R-module A (the 'alphabet'), an R-**linear code** over A is a left R-submodule $C \subseteq A^n$.
- An additive $\mathbb{F}_q$-code is the same as an R-linear code over A with $R = \mathbb{F}_p$ and $A = \mathbb{F}_q$, regarding $\mathbb{F}_q$ as an $\mathbb{F}_p$-vector space of dimension ℓ, where $q = p^\ell$.
- Can generalize to case of $R = M_{k\times k}(\mathbb{F}_q)$ and $A = M_{k\times \ell}(\mathbb{F}_q)$, and the same theory and results will apply.
- Call this the **matrix module context**.

Parametrized codes

- Linear codes are often presented as the row space of a **generator matrix** or, equivalently, as the image of a linear transformation (an **encoder**).
- For linear codes over modules, we will view a linear code $C \subseteq A^n$ as the image of a homomorphism $\Lambda : M \to A^n$ of left R-modules. Refer to M as the **information module**.

Weights

- Given ring R, alphabet A, suppose we have a **weight** w on A; i.e., $w : A \to \mathbb{C}$ with $w(0) = 0$.
- Extend w to A^n: $w(\vec{a}) = \sum_{i=1}^{n} w(a_i)$.
- Let $C \subseteq A^n$ be an R-linear code.
- A homomorphism $f : C \to A^n$ is a w-**isometry** if $w(cf) = w(c)$, for all $c \in C$. (Inputs on left.)

Isometry group

- Remember isometry condition: $w(cf) = w(c)$, for all $c \in C$.
- Now suppose $f : C \to C$ is an isometry of C to itself.
- When C is the image of $\Lambda : M \to A^n$, we define the **isometry group** of C:

$$\begin{aligned}\mathrm{Isom}(C) = \{&g \in \mathrm{GL}_R(M) : \text{there exists a linear} \\ &\text{isometry } f : C \to C \text{ such that } g\Lambda = \Lambda f\}.\end{aligned}$$

- View isometries on M rather than C.

Monomial group

- Any weight w on A has a **right symmetry group** $G_{\mathrm{rt}} = \{\phi \in \mathrm{GL}_R(A) : w(a\phi) = w(a), a \in A\}$.
- A G_{rt}-**monomial transformation** $T : A^n \to A^n$ has the form

$$(a_1, \ldots, a_n) \mapsto (a_{\sigma(1)}\phi_1, \ldots, a_{\sigma(n)}\phi_n),$$

  for a permutation σ of $\{1, \ldots, n\}$ and $\phi_i \in G_{\mathrm{rt}}$.
- For linear code $C \subseteq A^n$, the **monomial group** is

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

Restriction map

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

$$\mathrm{restr} : \mathrm{Monom}(C) \to \mathrm{Isom}(C).$$

- Denote $\ker \mathrm{restr} = \mathrm{Monom}_0(C)$. Think of repeated columns in a generator matrix.

Extension Property

- The alphabet A has the **extension property** (EP) with respect to the weight w if every w-isometry extends to a G_{rt}-monomial transformation.
- If EP holds, then restr is surjective.

Some facts about EP

- Ring alphabets with Hamming weight: if $A = R$ and w is the Hamming weight, then EP holds iff R is a Frobenius ring.
- Module alphabets with Hamming weight: EP holds iff A is pseudo-injective and $\mathrm{Soc}(A)$ is cyclic.
- For the matrix module context ($A = M_{k\times\ell}(\mathbb{F}_q)$) with Hamming weight: EP holds iff $k \geq \ell$.
- EP for Hamming weight fails for additive $\mathbb{F}_q$-codes when $q > p$.

Aside: EP for short codes

- Serhii Dyshko (Toulon) has shown that EP holds in the matrix module context even when $k < \ell$, **provided** n is sufficiently small ($n \leq q$ when $k = 1$).

Main question

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

Example 1 (a)

- Additive code C_1 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)

- Let $f_1 \in \mathrm{GL}_R(M) = \mathrm{GL}(3, \mathbb{F}_2)$ and $T_1 \in \mathrm{restr}(\mathrm{Monom}(C_1))$:

$$f_1 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad T_1 = \begin{bmatrix} \omega \leftrightarrow \omega^2 & 0 & 0 \\ 0 & 1 \leftrightarrow \omega^2 & 0 \\ 0 & 0 & \mathrm{id} \end{bmatrix}.$$

- Verify that $f_1 G_1 = G_1 T_1$.

Example 1 (c)

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

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

- f_1, f_2 generate $\mathrm{restr}(\mathrm{Monom}(C_1))$, a Klein 4-group. But f_1, f_3 generate $\mathrm{Isom}(C_1)$, 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 C_2 over $\mathbb{F}_4$ with generator matrix G_2 and list of codewords. Again, $M = \mathbb{F}_2^3$.

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

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

Example 2 (b)

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

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

- These elements generate $\mathrm{restr}(\mathrm{Monom}(C_2)) \cong \Sigma_4$, the symmetric group on 4 elements, while $\mathrm{Isom}(C_2) = \mathrm{GL}(3, \mathbb{F}_2)$, the simple group of order 168.
- Magma found only a cyclic 4-group generated by $f = f_4 f_5 f_6 f_4 f_5 f_4 f_6$.

Necessary conditions

- Recall $\mathrm{restr}(\mathrm{Monom}(C)) \subseteq \mathrm{Isom}(C) \subseteq \mathrm{GL}_R(M)$.
- Main question: What subgroups H_1, H_2 of $\mathrm{GL}_R(M)$ can occur as $\mathrm{restr}(\mathrm{Monom}(C))$ and $\mathrm{Isom}(C)$?
- Necessary: $H_1 \subseteq H_2$.
- Necessary: H_1 must equal $\mathrm{restr}(\mathrm{Monom}(C_1))$ for some code C_1.
- Necessary: H_2 must equal $\mathrm{Isom}(C_2)$ for some C_2.

Statement of main result

Theorem

Matrix module context with $k < \ell < m$. *For any choice of subgroups* $H_1 \subseteq H_2 \subseteq \mathsf{GL}_R(M)$ *satisfying the necessary conditions above, there exists a linear code* C *modeled on* M *such that* $H_1 = \mathsf{restr}(\mathsf{Monom}(C))$ *and* $H_2 = \mathsf{Isom}(C)$.

Corollary

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

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
	1	0	0	1	1	1	1	1	1
G	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 $\mathrm{Isom}(C) = \mathrm{GL}(3, \mathbb{F}_2)$, while $\mathrm{restr}(\mathrm{Monom}(C)) = \{\mathrm{id}_M\}$.

Extreme example (b)

- Additive code C_3 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
	0	0	0	1	1	1	1	1	1	1	1	1
G_3	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
0	1	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 C_3 has length $n = 86$; all codewords have weight 72.
- $\mathrm{Isom}(C_3) = \mathrm{GL}(3, \mathbb{F}_3)$, of order $11,232$.
- $\mathrm{restr}(\mathrm{Monom}(C_3)) = \{\pm \mathrm{id}_M\}$ is minimum possible.

Other alphabets

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

Thank you

- Thank you for kind attention.

Thank you

- Thank you for kind attention.
- On behalf of all the participants, thanks to the organizers for their efforts and their hospitality.