Isometry Groups of Additive Codes

Jay A. Wood

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

AMS meeting
Loyola University, Chicago IL
October 4, 2015

Additive codes

- Let $L = \mathbb{F}_q$, $q = p^\ell$, p prime, be a finite field.
- An *additive code* over L is an additive subgroup $C \subseteq L^n$.
- If $q = p$, i.e., $\ell = 1$, then additive codes are the same as linear codes.
- In general, an additive code is $\mathbb{F}_p$-linear, but not $\mathbb{F}_q$-linear. Write $K = \mathbb{F}_p$.
- Use the Hamming weight wt based on L.

Generator matrices

- An additive code $C \subseteq L^n$ has some dimension k as a K-vector space.
- Then C is generated (over K) by the rows of some $k \times n$ matrix G with entries in L. The matrix G has rank k over K.
- The matrix G defines an injective K-linear transformation $G : K^k \longrightarrow L^n$, $x \mapsto xG$, whose image is C.
- View everything as happening on $M := K^k$, the information space.

Additive maps from C to C

- View everything as happening on $M = K^k$, the information space.
- Any additive map $C \to C$ is K-linear and is represented by a K-linear map $f : M \to M$. Then $xG \mapsto xfG$, for $x \in M$.
- For invertible K-linear maps, we have $GL_K(C) \cong GL_K(M) \cong GL(k, K)$.

Isometries of C

- A K-linear map $C \longrightarrow C$ is an *isometry* if it preserves the Hamming weight based on L.
- In terms of $f : M \longrightarrow M$: $\mathrm{wt}(xG) = \mathrm{wt}(xfG)$, $x \in M$.
- An isometry is necessarily injective.
- Let $\mathrm{Isom}(C)$ be the group of all isometries of C.

Additive monomial maps of L^n

- What are the additive maps of L^n that preserve Hamming weight?
- They have the form, for $(y_1, \ldots, y_n) \in L^n$:

$$(y_1, \ldots, y_n)T = (y_{\sigma(1)}\tau_1, \ldots, y_{\sigma(n)}\tau_n),$$

  where σ is a permutation of $\{1, \ldots, n\}$ and each $\tau_i \in GL_K(L)$.
- Call these K-linear *monomial maps* of L^n.

Monomial maps that preserve C

- For an additive code $C \subseteq L^n$, let

$$\mathrm{Monom}(C) = \{\text{monomial } T : L^n \to L^n, CT = C\}.$$

- Restricting $T \in \mathrm{Monom}(C)$ to C gives an isometry.
- Let $\mathrm{RM}(C) = \{f : M \to M, f = T|_C, T \in \mathrm{Monom}(C)\}$. "Restricted monomial maps."
- $\mathrm{RM}(C) \subseteq \mathrm{Isom}(C)$
- Then $f \in \mathrm{RM}(C)$ when $fG = GT$ for some $T \in \mathrm{Monom}(C)$.

Monom(C) versus RM(C)

- Monom(C) is a subgroup of the group of monomial maps of L^n, while RM(C) is a subgroup of $GL_K(M) \cong GL(k, K)$.
- The restriction homomorphism Monom(C) $\to$ RM(C) may have a nontrivial kernel, coming from repeated columns (up to 'scalar' multiples from $GL_K(L)$) in G.
- Kernel is $\{T \in \text{Monom}(C) : GT = G\}$.

RM(C) versus Isom(C)

- We know that $\mathrm{RM}(C) \subseteq \mathrm{Isom}(C) \subseteq GL_K(M)$.
- $f \in \mathrm{RM}(C)$ when $fG = GT$ for some $T \in \mathrm{Monom}(C)$.
- $f \in \mathrm{Isom}(C)$ when $\mathrm{wt}(xfG) = \mathrm{wt}(xG)$ for all $x \in M$.
- Does $\mathrm{RM}(C) = \mathrm{Isom}(C)$?
- If not, how different can the groups be?

Does $\mathrm{RM}(C) = \mathrm{Isom}(C)$?

- If $L = K$ (ordinary linear codes), then yes, MacWilliams 1961-62.
- If $K \subsetneq L$, then no in general. Examples will follow.
- Even when $K \subsetneq L$, yes if the code is sufficiently short: $n \leq |K|$, Serhii Dyshko 2015.

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. $M = \mathbb{F}_2^3$.

$$G_1 = \begin{bmatrix} 1 & \omega & 0 \\ \omega & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}, \qquad \begin{array}{ccc} 0 & 0 & 0 \\ 1 & \omega & 0 \\ \omega & 1 & 0 \\ \omega^2 & \omega^2 & 0 \\ 1 & 0 & 1 \\ 0 & \omega & 1 \\ \omega^2 & 1 & 1 \\ \omega & \omega^2 & 1 \end{array}$$

Example 1 (b)

- Consider an element $f_3 \in GL_K(M) = GL(3, \mathbb{F}_2)$:

$$f_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

$$G_1 = \begin{bmatrix} 1 & \omega & 0 \\ \omega & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}, \quad f_3 G_1 = \begin{bmatrix} 1 & \omega & 0 \\ 1 & 0 & 1 \\ \omega^2 & \omega^2 & 0 \end{bmatrix}$$

Example 1 (c)

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

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

- f_1, f_2 generate RM(C), a Klein 4-group. But f_1, f_3 generate Isom(C), a dihedral group of order 8 (with $f_2 = f_1 f_3^2$).
- Magma found only the cyclic 2-group generated by $f_1 f_2$.

Main question

- We know:

$$\mathrm{RM}(C) \subseteq \mathrm{Isom}(C) \subseteq GL_K(M).$$

- What subgroups of $GL_K(M)$ can occur as $\mathrm{RM}(C)$ and $\mathrm{Isom}(C)$?

Necessary conditions

- If subgroups $H_1 \subseteq H_2 \subseteq GL_K(M)$ are to satisfy $H_1 = \mathrm{RM}(C)$ and $H_2 = \mathrm{Isom}(C)$ for some additive code C of dimension k, then it is necessary that H_1 equal $\mathrm{RM}(C_1)$ and $H_2 = \mathrm{Isom}(C_2)$ for some additive codes C_1, C_2 of dimension k.
- Not every subgroup of $GL_K(M)$ gets to be an isometry or restricted monomial group.
- Hypothesis: there exist additive codes C_1 and C_2 of dimension k such that $H_1 = \mathrm{RM}(C_1)$ and $H_2 = \mathrm{Isom}(C_2)$.

Main results

Theorem

Let $K \subsetneq L$, and let M be a K-vector space of dimension $k = \dim_K M > \dim_K L$. For any choice of subgroups $H_1 \subseteq H_2 \subseteq GL_K(M)$ satisfying the Hypothesis above, there exists an additive code C over L with $\dim_K C = k$ such that $H_1 = \mathrm{RM}(C)$ and $H_2 = \mathrm{Isom}(C)$. (The length of C may be large.)

Corollary

There exists an additive code C of dimension k with $\mathrm{RM}(C) = \{K^\times \cdot \mathrm{id}_M\}$ and $\mathrm{Isom}(C) = GL_K(M)$.

Sketch (a)

- Let $\mathcal{O}^\sharp = \mathrm{Hom}_K(M, L)/GL_K(L)$ be the set of all possible columns in a generator matrix, up to 'scalar' multiples by $GL_K(L)$.
- Up to monomial maps, a generator matrix G is determined by its *multiplicity function* $\eta : \mathcal{O}^\sharp \to \mathbb{N}$ which counts how many times a given column-type appears in G. View $\eta \in F(\mathcal{O}^\sharp, \mathbb{N})$.
- $GL_K(M)$ acts on $\mathcal{O}^\sharp$ and $F(\mathcal{O}^\sharp, \mathbb{N})$.
- For $f \in GL_K(M)$, $f \in \mathrm{RM}(C)$ when $\eta_C \cdot f = \eta_C$.

Sketch (b)

- Let $\mathcal{O} = K^\times \backslash M$ be the projective space of M. $GL_K(M)$ acts on $\mathcal{O}$ and on $F(\mathcal{O}, \mathbb{N})$.
- There is a well-defined additive map

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

  that assigns to a generator matrix G the function $x \mapsto \mathrm{wt}(xG)$, $x \in M$. Tensor over $\mathbb{Q}$.
- For $f \in GL_K(M)$, $f \in \mathrm{Isom}(C)$ when $W(\eta_C \cdot f) = W(\eta_C)$.
- The map W is not injective when $K \subsetneq L$.

Sketch (c)

- For $H_1 \subseteq H_2 \subseteq GL_K(M)$, pick a function $w \in F(\mathcal{O}, \mathbb{N})$ that separates the H_2-orbits on $\mathcal{O}$.
- The map W is surjective, so there exists $\eta \in F(\mathcal{O}^\sharp, \mathbb{Q})$ with $W(\eta) = w$.
- Replace η with its average over H_2. Can then show that $\mathrm{RM}(\eta) = \mathrm{Isom}(\eta) = H_2$. This step makes use of the Hypothesis for H_2.

Sketch (d)

- There is a nice basis for $\ker W \subseteq F(\mathcal{O}^\sharp, \mathbb{Q})$.
- Can modify η by elements of $\ker W$ so that η separates the H_1-orbits on $\mathcal{O}^\sharp$.
- This does not change $\mathrm{Isom}(\eta) = H_2$, but now can show $\mathrm{RM}(\eta) = H_1$. This step uses the Hypothesis for H_1.
- Rescale and modify so that η has values in $\mathbb{N}$.

Example 2 (a)

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

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

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

Example 2 (b)

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

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

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

Extreme example (a)

- $K = \mathbb{F}_2$, $L = \mathbb{F}_4$, $M = \mathbb{F}_2^3$. 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 $\mathrm{Isom}(C) = GL(3, \mathbb{F}_2)$, while $\mathrm{RM}(C) = \{\mathrm{id}_M\}$.

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

Other contexts

- The same results apply to matrix modules: $K = M_{k\times k}(\mathbb{F}_q)$, $L = M_{k\times \ell}(\mathbb{F}_q)$, with $k < \ell$.
- Most of the results carry over to any alphabet A over a finite ring R with socle of A non-cyclic. For example, $A = R$, a non-Frobenius ring.
- Get $\mathrm{RM}(C) \subseteq H_1$ only, but still have $H_2 = \mathrm{Isom}(C)$.
- This is enough to get the extreme cases.