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 $\text{wt}$ 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 $G : K^k \to L^n$, $x \mapsto xG$, 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 $C \rightarrow C$ is an isometry if it preserves the Hamming weight based on $L$.
- In terms of $f : M \rightarrow M$: $\text{wt}(xG) = \text{wt}(xfG)$, $x \in M$.
- An isometry is necessarily injective.
- Let $	ext{Isom}(C)$ be the group of all isometries of $C$. 
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 $\sigma$ 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
  \[
  \text{Monom}(C) = \{\text{monomial } T : L^n \rightarrow L^n, CT = C\}.
  \]

- Restricting $T \in \text{Monom}(C)$ to $C$ gives an isometry.

- Let $\text{RM}(C) = \{f : M \rightarrow M, f = T|_C, T \in \text{Monom}(C)\}$. “Restricted monomial maps.”

- $\text{RM}(C) \subseteq \text{Isom}(C)$

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

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

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

<table>
<thead>
<tr>
<th>Codeword</th>
<th>0</th>
<th>0</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>$\omega$</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>$\omega$</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>$\omega^2$</td>
<td>$\omega^2$</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>$\omega$</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>$\omega^2$</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>$\omega$</td>
<td>$\omega^2$</td>
<td>1</td>
</tr>
</tbody>
</table>
Example 1 (b)

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

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

$$G_1 = \begin{bmatrix} 1 & \omega & 0 \\ \omega & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}, \quad f_3 G_1 = \begin{bmatrix} 1 & \omega & 0 \\ 1 & 0 & 1 \\ \omega^2 & \omega & 0 \end{bmatrix}.$$
Consider three elements of $GL_K(M) = GL(3, \mathbb{F}_2)$:

\[
\begin{align*}
  f_1 &= \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, &
  f_2 &= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}, &
  f_3 &= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}.
\end{align*}
\]

$f_1, f_2$ 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:

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

▶ What subgroups of $GL_K(M)$ can occur as $\text{RM}(C)$ and $\text{Isom}(C)$?
Necessary conditions

- If subgroups \( H_1 \subseteq H_2 \subseteq GL_K(M) \) are to satisfy \( H_1 = RM(C) \) and \( H_2 = Isom(C) \) for some additive code \( C \) of dimension \( k \), then it is necessary that \( H_1 \) equal \( RM(C_1) \) and \( H_2 = Isom(C_2) \) 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 \( H_1 = RM(C_1) \) and \( H_2 = Isom(C_2) \).
Main results

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

**Corollary**
There exists an additive code $C$ of dimension $k$ with $\text{RM}(C) = \{K^\times \cdot \text{id}_M\}$ and $\text{Isom}(C) = \text{GL}_K(M)$. 
Sketch (a)

Let $\mathcal{O}^\# = \text{Hom}_K(M, L)/\text{GL}_K(L)$ be the set of all possible columns in a generator matrix, up to ‘scalar’ multiples by $\text{GL}_K(L)$.

Up to monomial maps, a generator matrix $G$ is determined by its *multiplicity function* $\eta : \mathcal{O}^\# \to \mathbb{N}$ which counts how many times a given column-type appears in $G$. View $\eta \in F(\mathcal{O}^\#, \mathbb{N})$.

$\text{GL}_K(M)$ acts on $\mathcal{O}^\#$ and $F(\mathcal{O}^\#, \mathbb{N})$.

For $f \in \text{GL}_K(M)$, $f \in \text{RM}(C)$ when $\eta_C \cdot f = \eta_C$. 
Sketch (b)

- Let $\mathcal{O} = K^\times \setminus M$ 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

\[
W : F(\mathcal{O}^\#, \mathbb{N}) \rightarrow F(\mathcal{O}, \mathbb{N})
\]

that assigns to a generator matrix $G$ the function $x \mapsto \text{wt}(xG)$, $x \in M$. Tensor over $\mathbb{Q}$.

- For $f \in GL_K(M)$, $f \in \text{Isom}(C)$ when $W(\eta_C \cdot f) = W(\eta_C)$.

- The map $W$ is not injective when $K \subsetneq L$. 
Sketch (c)

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

- There is a nice basis for \( \text{ker } W \subseteq F(O^\#, \mathbb{Q}) \).
- Can modify \( \eta \) by elements of \( \text{ker } W \) so that \( \eta \) separates the \( H_1 \)-orbits on \( O^\# \).
- This does not change \( \text{Isom}(\eta) = H_2 \), but now can show \( \text{RM}(\eta) = H_1 \). This step uses the Hypothesis for \( H_1 \).
- Rescale and modify so that \( \eta \) has values in \( \mathbb{N} \).
Example 2 (a)

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

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

$$\begin{array}{cccccc}
0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 1 & \omega & \omega & \\
1 & 1 & 0 & \omega^2 & \omega^2 & \\
\omega & \omega & 1 & 0 & \omega^2 & \\
\omega^2 & 0 & 1 & \omega & \\
\omega^2 & \omega & 0 & \omega & 1 \\
\omega^2 & \omega^2 & 1 & \omega^2 & 0
\end{array}$$
Example 2 (b)

- Consider three elements of $GL_R(M) = GL(3, \mathbb{F}_2)$:
  
  $f_4 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$,  
  $f_5 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$,  
  $f_6 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$.

- These elements generate $RM(C) \cong \Sigma_4$, the symmetric group on 4 elements, while $Isom(C) = GL(3, \mathbb{F}_2)$, the simple group of order 168.

- Magma found only a cyclic 4-group generated by $f = f_4f_5f_6f_4f_5f_4f_6$. 
Extreme example (a)

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

<table>
<thead>
<tr>
<th>multiplicity</th>
<th>1</th>
<th>4</th>
<th>2</th>
<th>2</th>
<th>4</th>
<th>1</th>
<th>3</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$G$</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>$\omega$</td>
<td>$\omega$</td>
<td>$\omega$</td>
<td>$\omega$</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>$\omega$</td>
<td>1</td>
<td>$\omega^2$</td>
<td>$\omega$</td>
<td>$\omega$</td>
</tr>
</tbody>
</table>

- All codewords have weight 22, so $\text{Isom}(C) = GL(3, \mathbb{F}_2)$, while $\text{RM}(C) = \{\text{id}_M\}$. 
Extreme example (b)

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

<table>
<thead>
<tr>
<th>mult.</th>
<th>5</th>
<th>3</th>
<th>6</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>2</th>
<th>2</th>
<th>2</th>
<th>4</th>
<th>3</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>$G_3$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>-1</td>
<td>-1</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>0</td>
<td>1</td>
<td>-1</td>
<td>0</td>
<td>1</td>
<td>-1</td>
<td>0</td>
<td>1</td>
<td>-1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6</th>
<th>3</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>6</th>
<th>4</th>
<th>5</th>
<th>2</th>
<th>3</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>$\omega$</td>
<td>$\omega$</td>
<td>$\omega$</td>
<td>$\omega$</td>
<td>$\omega$</td>
<td>$\omega$</td>
<td>$\omega$</td>
<td>$\omega$</td>
<td>$\omega$</td>
</tr>
<tr>
<td>$\omega$</td>
<td>$\omega$</td>
<td>0</td>
<td>1</td>
<td>-1</td>
<td>$\omega$</td>
<td>$\omega$+1</td>
<td>$\omega$-1</td>
<td>$-\omega$</td>
<td>$-\omega$+1</td>
<td>$-\omega$-1</td>
</tr>
</tbody>
</table>
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.
- $\text{RM}(C) = \{ \pm \text{id}_M \}$ is minimum possible.
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 $\text{RM}(C) \subseteq H_1$ only, but still have $H_2 = \text{Isom}(C)$.

This is enough to get the extreme cases.