# Automorphisms of Additive Codes

Jay A. Wood

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

32nd Ohio State-Denison Mathematics Conference
Columbus, Ohio
May 9, 2014

# Acknowledgments/the Question

I thank Philippe Langevin for the following question:
"Let $K$ be a subfield of a finite field $L$.
"Like in the classical case, we see that coordinate permutations and component-wise $K$-linear isomorphisms of $L$ preserve the Hamming weight of $L^n$.
"Now let $C$ be a $K$-subspace of $L^n$, and let $f$ be a $K$-linear isomorphism of $C$ that preserves the Hamming weight.
"I wonder if it is true that $f$ extends as a map like above?" (by email, May 9, 2013)

# Short Answer

- No.

# Definitions

- Let $K$ be a finite field, and let $L$ be a finite dimensional vector space over $K$.
- A *$K$-linear code over $L$* of length $n$ is a $K$-linear subspace $C \subset L^n$.
- We use the Hamming weight on $L$. This is a crucial hypothesis. The Hamming weight on $L$ differs from the Hamming weight on $K^\ell$, where $\ell = \dim_K L$.
- This can be generalized to finite rings $K$ and finite module alphabets $L$.

# Additive Codes

- Let $L = \mathbb{F}_q$, $q = p^\ell$, and $K = \mathbb{F}_p$. Then $K$-linear codes over $L$ are *additive codes* over $L$.
- Such codes are closed under addition. It follows that they are closed under $K$-scalar multiplication.
- 'Monomial' transformations: permutations and component-wise application of $K$-linear isomorphisms of $L$ (not field automorphisms).
- Monomial transformations preserve the Hamming weight coming from $L$.

# Generator Matrix

- A $K$-linear code is often given by a *generator matrix* $G$. The rows of $G$ form a $K$-basis for $C \subset L^n$.
- If $G$ has size $m \times n$, then $G$ defines an injective $K$-linear map $\Lambda : M = K^m \longrightarrow L^n$, whose image is the $K$-linear code $C$. (Inputs on the left.)

# Isometries

- An *isometry* of a $K$-linear code $C \subset L^n$ is an invertible $K$-linear map $f : C \longrightarrow C$ that preserves the Hamming weight.
- In terms of $\Lambda : M \longrightarrow L^n$: an element $f \in GL_K(M)$ such that $\mathrm{wt}(xf\Lambda) = \mathrm{wt}(x\Lambda)$ for all $x \in M$.
- All the isometries of $C$ form a group, the *isometry group* $\mathrm{Isom}(C) \subset GL_K(M)$.

# Monomial Transformations

- A *monomial transformation* of $L^n$ is an invertible $K$-linear transformation $T : L^n \longrightarrow L^n$ of the form

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

  where $\sigma$ is a permutation of $\{1, \ldots, n\}$ and the $\phi_i$ are invertible $K$-linear transformations of $L$.
- Define the *monomial group* $\mathrm{Monom}(C) = \{T \text{ monomial on } L^n : CT = C\}$.

# Restriction Map

- Monomial transformations preserve weight.
- By restricting to $C$, we have a natural map

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

- Langevin's question: is this map onto?
- In matrix terms, if $f \in \text{Isom}(C)$, is there a $T \in \text{Monom}(C)$ such that $fG = GT$?
- If $L = K$, then the restriction map is always onto. (MacWilliams, 1961)

# Example

- Let $K = \mathbb{F}_2$, $L = \mathbb{F}_4 = \mathbb{F}_2[\omega]/(\omega^2 + \omega + 1)$.
- Let $C \subset L^3$ be the additive code generated by:

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

- What are restr(Monom($C$)) and Isom($C$)?

# Monomial Group

- restr(Monom($C$)) is a Klein 4-group, generated by $f_1, f_2$, below.

$$f_1 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad f_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

$$\text{e.g. } f_1 f_2 G = \begin{bmatrix} 1 & \omega & 0 \\ \omega^2 & \omega^2 & 0 \\ 0 & \omega & 1 \end{bmatrix} = G \begin{bmatrix} 0 & \omega & 0 \\ \omega^2 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

# Isometry Group

- However, $\mathrm{Isom}(C)$ is a dihedral group of order 8, generators $f_1$ and $f_3$ (below): $f_1^2 = 1$, $f_3^4 = 1$, $f_1 f_3 f_1 = f_3^{-1}$.
- $$f_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

# Weight Preservation

- List of codewords and their images under $f_3$:

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

# Non-Extendability of $f_3$

- Compare $G$ and $f_3 G$:

$$G = \begin{bmatrix} 1 & \omega & 0 \\ \omega & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \qquad f_3 G = \begin{bmatrix} 1 & \omega & 0 \\ 1 & 0 & 1 \\ \omega^2 & \omega^2 & 0 \end{bmatrix}$$

- The patterns of the columns are not compatible via a monomial transformation.

# How Bad Can Things Get?

Generalize to linear codes over matrix modules:

$$K = M_{k\times k}(\mathbb{F}_q), L = M_{k\times \ell}(\mathbb{F}_q), M = M_{k\times m}(\mathbb{F}_q).$$

## Theorem

*Assume $k < \ell < m$. Pick any two subgroups $G_1 \subset G_2 \subset GL_K(M)$ (subject to a closure condition). Then there exists a $K$-linear code $C \subset L^n$ with underlying module $M$ such that* $\mathrm{Isom}(C) = G_2$ *and* $\mathrm{restr}(\mathrm{Monom}(C)) = G_1$. *(Length $n$ could be very big.)*

# Linear Codes via Functionals (a)

- Assmus-Mattson (1963). Let $K$ be a finite ring and $L$, $M$ be finite left $K$-modules; $L$ is the alphabet, and $M$ is the information space.
- Given functionals $\lambda_1, \ldots, \lambda_n \in M^\sharp := \mathrm{Hom}_K(M, L)$, the image of $\Lambda : M \longrightarrow L^n$, $x \mapsto (x\lambda, \ldots, x\lambda_n)$, is a $K$-linear code in $L^n$.
- If one fixes a set of generators $x_1, \ldots, x_k$ for $M$, then the matrix with $(i, j)$-entry $x_i\lambda_j$ is a generator matrix for this $K$-linear code.

# Linear Codes via Functionals (b)

- $G = GL_K(L)$, the group of $K$-linear isomorphisms of $L$, acts on $M^\sharp = \mathrm{Hom}_K(M, L)$.
- Up to monomial equivalence, all that matters is the number of times the $G$-orbit of a functional $\lambda \in M^\sharp$ appears in the list $\lambda_1, \ldots, \lambda_n$: call this number the *multiplicity* $\eta(\lambda)$.
- Conversely, a multiplicity function $\eta : M^{\sharp G} \longrightarrow \mathbb{N}$ determines a linear code, up to monomial equivalence.

# Linear Codes via Functionals (c)

- For the Hamming weight wt on $L$, the weight of a codeword is

$$\mathrm{wt}(x) = \sum_{\lambda \in M^{\sharp G}} \mathrm{wt}(x\lambda)\,\eta(\lambda), \quad x \in M.$$

- This defines an additive map of function spaces

$$W : F(M^{\sharp G}, \mathbb{N}) \to F(M, \mathbb{N}).$$

- For linear codes over matrix modules and the Hamming weight, $W$ has a nonzero kernel exactly when $k < \ell$.

# Linear Codes via Functionals (d)

- Tensor over $\mathbb{Q}$ to get a $\mathbb{Q}$-linear transformation

$$W : F(M^{\sharp G}, \mathbb{Q}) \to F(M, \mathbb{Q}).$$

- For linear codes over matrix modules and the Hamming weight, if $k < \ell$, then it is possible to write down an explicit basis for $\ker W$.

# Action by $GL_K(M)$

- The $K$-linear isomorphisms $GL_K(M)$ act on $M^\sharp = \mathrm{Hom}_K(M, L)$, on $M^{\sharp G}$, and on $F(M^{\sharp G}, \mathbb{Q})$.
- A linear code $C$ with underlying module $M$ corresponds, up to monomial equivalence, to a multiplicity function $\eta \in F(M^{\sharp G}, \mathbb{Q})$.
- Let $f \in GL_K(M)$. Then $f \in \mathrm{restr}(\mathrm{Monom}(C))$ when $f^*\eta = \eta$, and $f \in \mathrm{Isom}(C)$ when $f^*\eta - \eta \in \ker W$.

# Sketch of Proof of Theorem

- By averaging if necessary, find $\eta \in F(M^{\sharp G}, \mathbb{Q})$ that is invariant under the group $G_2$ but not invariant under any larger subgroup. (This is where the closure condition plays a role.)
- So far, $\mathrm{restr}(\mathrm{Monom}(C)) = \mathrm{Isom}(C) = G_2$.
- By using the explicit basis of $\ker W$, modify $\eta$ to obtain $\eta'$ such that $\eta' - \eta \in \ker W$, but $\eta'$ is invariant only under $G_1$ (and no larger).
- Then $\mathrm{restr}(\mathrm{Monom}(C')) = G_1$ and $\mathrm{Isom}(C') = \mathrm{Isom}(C) = G_2$.

# Corollaries

- Can choose $G_1 = \mathbb{F}_q^\times \cdot \mathrm{id}_M$ (minimal) and $G_2 = GL_K(M)$ (maximal).
- Such an example over $K = \mathbb{F}_2$ and $L = \mathbb{F}_4$ has length $n = 24$.
- Examples can then be found over any non-Frobenius ring $R$, since the socle contains a matrix module with $k < \ell$.