Exotic Automorphisms of Additive Codes

Jay A. Wood

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

AMS meeting, Louisville, Kentucky
October 5, 2013

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^e, where $e = \dim_K L$.
- Can generalize to finite rings K and finite module alphabets L.

Additive Codes

- Let $L = \mathbb{F}_q$, $q = p^e$, 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).

The Example

- Let $L = \mathbb{F}_4 = \mathbb{F}_2[\omega]/(\omega^2 + \omega + 1)$, $K = \mathbb{F}_2$.
- 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 the code automorphisms of C?

Warmup (a)

- Cyclic code C_1 of length 7 over $\mathbb{F}_2$:

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

- $|\mathrm{Aut}(C_1)| = 168$
- Magma calculation (later)

Warmup (b)

- Additive code C_2 over $\mathbb{F}_4$ ($\omega^2 = 1 + \omega$):

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

- Permutation group of C_2 has order 2.
- 'Monomial' group has order 18.
- Magma calculation (later)

The Example

- Additive code C over $\mathbb{F}_4$:

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

- Permutation group of C has order 1.
- 'Monomial' group has order 2 (P generates).
- Magma calculation (next)

Magma computations

- See other files for Magma output that confirms $\mathrm{Aut}(C)$ calculations.
- Run on September 30, 2013.

Another Code Automorphism

- Same additive code C over $\mathbb{F}_4$:

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

- Define $f : C \longrightarrow C$ by fixing the first generator and interchanging the other two generators.
- This f is an additive isomorphism that preserves Hamming weight over $\mathbb{F}_4$ (next slide).

Weight Preservation

- List of codewords and their images under f:

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

Non-extendability of f

- This f does not extend to a 'monomial' transformation over $\mathbb{F}_4$; f is 'exotic.'
- 'Monomial' means permutations and $\mathbb{F}_2$-linear isomorphisms of $\mathbb{F}_4$ (not field automorphisms, just vector space isomorphisms: $GL(2, \mathbb{F}_2)$, of order 6).
- Why not a 'monomial' transformation? The zeros do not transform properly.

What is a Code Automorphism?

- One meaning: A 'monomial' transformation $T : L^n \longrightarrow L^n$ that preserves the code C, i.e., $T(C) = C$. Let $\mathrm{Aut}(C)$ be the group of all such transformations. Then $\mathrm{Aut}(C) \subset \mathrm{Aut}(L^n)$.
- Second meaning: A K-linear isomorphism $f : C \longrightarrow C$ that preserves the Hamming weight; i.e., $\mathrm{wt}(f(x)) = \mathrm{wt}(x)$, for all $x \in C$. Let $\mathrm{Isom}(C)$ be the group of all such *linear isometries*.
- Fact: $\mathrm{Aut}(L^n) = \mathrm{Isom}(L^n)$.

Restriction Homomorphism

- By restricting an automorphism $T \in \mathrm{Aut}(C)$ to C, we get an isometry $f = T|_C \in \mathrm{Isom}(C)$.
- The kernel $\mathcal{K}$ of $\mathrm{Aut}(C) \longrightarrow \mathrm{Isom}(C)$ arises from repeated columns (up to action of K-isomorphisms of L) in a generator matrix.
- The Example shows that the exact sequence

$$0 \longrightarrow \mathcal{K} \longrightarrow \mathrm{Aut}(C) \longrightarrow \mathrm{Isom}(C)$$

need not be right exact.

Linear Codes via Functionals (a)

- Assmus-Mattson (1963). Let K be a finite field and L, M be finite dimensional K-vector spaces; 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 $M \longrightarrow L^n$, $x \mapsto (\lambda_1(x), \ldots, \lambda_n(x))$, 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 $\lambda_j(x_i)$ is a generator matrix for this K-linear code.

Linear Codes via Functionals (b)

- $G = GL(L, K)$, 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

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

- This defines an additive map of function spaces

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

- For additive codes and the Hamming weight, W has a nonzero kernel.

Producing the Example

- The K-linear isomorphisms $GL(M, K)$ also act on $M^\sharp = \mathrm{Hom}_K(M, L)$ and on $M^{\sharp G}$.
- For some non-trivial $\varphi \in GL(M, K)$, find a multiplicity function $\eta \in F(M^{\sharp G}, \mathbb{N})$ such that $\varphi^*(\eta) - \eta \in \ker W$, but $\varphi^*(\eta) - \eta \neq 0$.
- This reduces to solving a system of linear equations.

Research Questions

- Are there families of examples that are easy to construct?
- Can examples be found for matrix module alphabets $A = M_{m\times k}(\mathbb{F}_q)$ over $R = M_{m\times m}(\mathbb{F}_q)$, with $m < k$?
- How prevalent are exotic automorphisms?