Character-theoretic proofs of equivalence theorems

in honor of Thann Ward

Jay A. Wood

Department of Mathematics
Department of Statistics
Western Michigan University
jay.wood@wmich.edu

AMS meeting, Chicago
October 6, 2007

Thanks

I thank Thann Ward for ideas (characters), advice, and inspiration.

Linear codes over modules

- Let R be a finite ring with 1, and let A (for *alphabet*) be a finite left R-module.
- An *R-linear code of length n over A* is a submodule $C \subset A^n$.
- Equip A with the Hamming weight.

Equivalence of linear codes

- Two linear codes $C_1, C_2 \subset A^n$ are *equivalent* if there exists a monomial transformation $T : A^n \longrightarrow A^n$ taking C_1 to C_2.
- A monomial transformation is made up of a permutation and n linear automorphisms of A.

Monomial transformations preserve Hamming weight

Theorem

The restriction of a monomial transformation $T : C_1 \longrightarrow C_2$ is a linear isomorphism between C_1 and C_2 that preserves Hamming weight.

Theorem of MacWilliams

MacWilliams proved the converse over finite fields in 1961. Also Bogart, et al., 1978.

Theorem

Over $R = A = GF(q)$, if $T : C_1 \longrightarrow C_2$ is a linear isomorphism between linear codes $C_1, C_2 \subset A^n$ that preserves Hamming weight, then T extends to a monomial transformation of A^n.

Character-theoretic proof

In 1996 Ward & W. published a character-theoretic proof of the MacWilliams theorem (over $GF(q)$).

- View the codes as images: $\lambda, \mu : V \longrightarrow A^n$.
- Express weight preservation as an equation of characters:

$$\sum_{i=1}^{n} \sum_{\pi \in \widehat{A}} \pi(\lambda_i(v)) = \sum_{i=1}^{n} \sum_{\pi \in \widehat{A}} \pi(\mu_i(v))$$

- Use linear independence of characters to match up terms and build monomial transformation.

Generalizations to rings and modules

- To what extent does the theorem of MacWilliams extend to linear codes over finite rings ($A = R$) or finite modules (A over R)?
- At issue is: if a linear isomorphism T between linear codes preserves Hamming weight, does T extend to a monomial transformation?
- If the answer is always 'yes,' we say that the alphabet A has the *extension property*.

Case of rings

Theorem

Let $A = R$, a finite ring. Then R has the extension property if and only if R is a Frobenius ring.

- One characterization of finite Frobenius rings: $\widehat{R} \cong R$ as one-sided R-modules.

Case of modules

Theorem

Let A be a finite module over R, a finite ring. Then A has the extension property if and only if

1. *A is isomorphic to a submodule of $\widehat{R}$, and*
2. *A is a pseudo-injective R-module.*

- Condition 2 means that any injective homomorphism of a submodule $B \subset A$ to A extends to a homomorphism from A to A.

The conditions are sufficient

- First step: $A = \widehat{R}$ has the extension property (Greferath, Nechaev, and Wisbauer, 2004).
- There is also a character-theoretic proof, using that $\widehat{A} \cong R$.
- General case: use condition 1 and the result for $\widehat{R}$ to reduce to the case of length $n = 1$.
- The length $n = 1$ case is equivalent to condition 2 (Dinh and López-Permouth, 2004).

The conditions are necessary

- The length $n = 1$ case implies condition 2.
- Following a strategy of Dinh and López-Permouth, 2004, condition 1 follows from a non-extension result for linear codes defined over certain matrix modules.

Matrix modules

- Let $\mathbb{F} = GF(q)$, $R = M_k(\mathbb{F})$ ($k \times k$ matrices over $\mathbb{F}$), and $A = M_{k,l}(\mathbb{F})$ ($k \times l$ matrices over $\mathbb{F}$).

Theorem

If $k < l$, then there exist linear codes $C_1, C_2 \subset A^n$ (some large n) with $T : C_1 \longrightarrow C_2$ a linear isomorphism that preserves Hamming weight, yet T does not extend to a monomial transformation.

Example

- $\mathbb{F} = GF(2)$, $k = 1$, $l = 2$.

$$\begin{pmatrix} 00 & 00 & 00 \\ 10 & 10 & 00 \\ 01 & 01 & 00 \\ 11 & 11 & 00 \end{pmatrix} \qquad \begin{pmatrix} 00 & 00 & 00 \\ 10 & 10 & 00 \\ 00 & 10 & 10 \\ 10 & 00 & 10 \end{pmatrix}$$

- These are additive $GF(4)$ codes, self-orthogonal under the trace-Hermitian (symplectic) form.

Application to module case

If condition 1 is not satisfied, i.e., A is not a submodule of $\widehat{R}$, then one can find a copy of $M_{k,l}(\mathbb{F})$, with $k < l$, inside the socle of A. One can build a counter-example to the extension property from this.

Parameterized codes

- A *linear code* is a submodule of A^n.
- A linear code *parameterized* by a module M is a homomorphism $\lambda : M \longrightarrow A^n$.
- Two linear codes parameterized by the same M can be *concatenated*.

Parameterized codes under concatenation

Theorem

The collection of all linear codes (any length) parameterized by a module M, up to monomial transformations, forms a commutative semi-group under concatenation. This semigroup is isomorphic to the function space $\mathrm{Map}(\mathrm{Hom}_R(M, A)/G; \mathbb{N})$ *under addition.*

- $G = \mathrm{Aut}_R(A)$.

Weight map

- Weight map W sending η to w_η: $\mathrm{Map}(\mathrm{Hom}_R(M,A)/G;\mathbb{N}) \to \mathrm{Map}(R^\times\backslash M;\mathbb{N})$
- $w_\eta(x) = \sum_\lambda \eta(\lambda)\,\mathrm{wt}(\lambda(x))$
- Tensor over $\mathbb{Q}$ to get $\mathbb{Q}$-vector spaces, written $W : \mathbb{Q}[\mathrm{Hom}_R(M,A)/G] \to \mathbb{Q}[R^\times\backslash M]$ ('virtual codes').
- When $A = M_{k,l}(\mathbb{F})$, $k < l$, one calculates dimensions, and there is a non-zero $\ker W$.

Thanks

Thanks again, Thann. Happy retirement!