An Essay on Equivalence of Linear Codes, III

Jay A. Wood
Western Michigan University
jay.wood@wmich.edu
http://homepages.wmich.edu/∼jwood

AMS/SMM Special Session
Houston, Texas
May 14, 2004

I want to discuss equivalence of linear codes from a particular point of view.

Outline

- Definitions from a functional point of view
- Weights and symmetry
- MacWilliams extension theorem
- Codes over modules
- Examples of non-extension

Definitions

I use a functional point of view that goes back at least to Assmus and Mattson, 1961.

Fix a finite ring R with 1.

A *linear code* C consists of a finite (left) R-module M and a function $\eta : M^\sharp \to \mathbb{N}$. $M^\sharp = \mathrm{Hom}_R(M, R)$.

This is a coordinate-free point of view. There is no need to talk about permutations of coordinate positions. Questions of scaling will come later.

Virtual codes

It will be convenient to allow η to have values in $\mathbb{Q}$.

A *virtual linear code* C consists of a finite (left) R-module M and a function $\eta : M^\sharp \to \mathbb{Q}$.

Weights

Fix a weight function $w : R \to \mathbb{Q}$; $w(0) = 0$.

This allows us to define a weight mapping on the collection of all codes with underlying module M.

$$W : \mathsf{Map}(M^\sharp, \mathbb{Q}) \to \mathsf{Map}(M, \mathbb{Q}), \quad \eta \mapsto w_\eta,$$

where

$$w_\eta(x) = \sum_{\lambda \in M^\sharp} \eta(\lambda) w(\lambda(x)).$$

Notice that W is a linear transformation of $\mathbb{Q}$-vector spaces.

What can we say about W?

Degeneracies

Since $w(0) = 0$, we see that $w_\eta(0) = 0$, for any $\eta \in \mathrm{Map}(M^\sharp, \mathbb{Q})$.

Dually, the η defined by

$$\eta(\lambda) = \begin{cases} 1, & \lambda = 0; \\ 0, & \lambda \neq 0. \end{cases}$$

is in $\ker W$.

There is no loss of generality to study

$$W : \mathrm{Map}_0(M^\sharp, \mathbb{Q}) \to \mathrm{Map}_0(M, \mathbb{Q}),$$

where Map_0 indicates the maps taking 0 to 0.

Symmetry

The weight function $w : R \to \mathbb{Q}$ allows us to define two *symmetry groups*, which are subgroups of the group of units $\mathcal{U}(R)$:

$$\begin{aligned} G_l &= \{u \in \mathcal{U}(R) : w(ur) = w(r), r \in R\}, \\ G_r &= \{u \in \mathcal{U}(R) : w(ru) = w(r), r \in R\}. \end{aligned}$$

Proposition *The image of W lies in the G_l-invariant functions* $\mathsf{Map}_0(M, \mathbb{Q})^{G_l}$.

Proof. For $u \in G_l$, $x \in M$, $\eta \in \mathsf{Map}_0(M^\sharp, \mathbb{Q})$,

$$\begin{aligned} w_\eta(ux) &= \sum \eta(\lambda) w(\lambda(ux)) \\ &= \sum \eta(\lambda) w(u\lambda(x)) \\ &= \sum \eta(\lambda) w(\lambda(x)) = w_\eta(x). \quad \square \end{aligned}$$

More symmetry

Define a projection (averaging) map

$$P : \mathsf{Map}_0(M^\sharp, \mathbb{Q}) \to \mathsf{Map}_0(M^\sharp, \mathbb{Q})$$

by

$$(P\eta)(\lambda) = \frac{1}{|G_r|} \sum_{u \in G_r} \eta(\lambda \cdot u).$$

Proposition *P is a projection ($P^2 = P$), with image the G_r-invariant functions $\mathsf{Map}_0(M^\sharp, \mathbb{Q})^{G_r}$.*

Proposition *The weight mapping*

$$W : \mathsf{Map}_0(M^\sharp, \mathbb{Q}) \to \mathsf{Map}_0(M, \mathbb{Q})^{G_l}$$

factors through P:

$$\begin{array}{ccc} \mathsf{Map}_0(M^\sharp, \mathbb{Q}) & \xrightarrow{W} & \mathsf{Map}_0(M, \mathbb{Q})^{G_l}. \\ \downarrow P & \nearrow & \\ \mathsf{Map}_0(M^\sharp, \mathbb{Q})^{G_r} & & \end{array}$$

A canonical representative of an equivalence class of codes is the one where η is G_r-invariant.

MacWilliams extension theorem

We have reduced the situation to

$$W : \mathrm{Map}_0(M^\sharp, \mathbb{Q})^{G_r} \to \mathrm{Map}_0(M, \mathbb{Q})^{G_l}.$$

Theorem (MacWilliams) *If $R = GF(q)$, and w is the Hamming weight, then W is an isomorphism. In particular, W is injective.*

In general, when w is the Hamming weight, $G_l = G_r = \mathcal{U}(R)$.

Theorem *For R Frobenius, w Hamming weight, W is injective.*

There are similar results for other weight functions (Lee, Euclidean) over certain finite rings ($\mathbb{Z}/N\mathbb{Z}$). Especially, homogenous weights (Heise, et al.; Greferath, et al.).

Linear codes over modules

Nechaev and collaborators, especially Greferath, Nechaev, Wisbauer

R, S finite rings, "alphabet" (bi-)module ${}_R A_S$, weight function $w : A \to \mathbb{Q}$, $w(0) = 0$.

A *virtual linear code* over A consists of a module ${}_R M$ and a function $\eta : \mathrm{Hom}_R({}_R M, {}_R A) \to \mathbb{Q}$.

The weight mapping is then

$$W : \mathrm{Map}_0(\mathrm{Hom}_R(M, A), \mathbb{Q}) \to \mathrm{Map}_0(M, \mathbb{Q}),$$

with

$$w_\eta(x) = \sum_{\lambda \in \mathrm{Hom}_R(M,A)} \eta(\lambda) w(\lambda(x)).$$

Symmetry

Now the symmetry groups are slightly different

$$\begin{aligned} G_l &= \{u \in \mathcal{U}(R) : w(ua) = w(a), a \in A\}, \\ G_r &= \{v \in \mathcal{U}(S) : w(av) = w(a), a \in A\}. \end{aligned}$$

As before, we have

$W : \mathsf{Map}_0(\mathsf{Hom}_R(M, A), \mathbb{Q})^{G_r} \to \mathsf{Map}_0(M, \mathbb{Q})^{G_l}$.

When is W injective? "Friendly" modules, i.e., cyclic socle, for Hamming and homogenous weights (Greferath, Nechaev, Wisbauer).

Conversely, if W is injective, what does that say about R, A, w? (Dinh, López-Permouth)

Examples of non-extension

Greferath and Schmidt, Dinh and López-Permouth

$R = F = GF(q)$ is any finite field, $S = M_2(F)$, and $A = M_{1,2}(F)$. A is a non-friendly module over R.

$$G_1 = \begin{pmatrix} 10 & 00 & 10 & \dots & a0 \\ 00 & 10 & 10 & \dots & 10 \end{pmatrix},$$

$$G_2 = \begin{pmatrix} 00 & 10 & 10 & \dots & 10 \\ 00 & 01 & 01 & \dots & 01 \end{pmatrix},$$

where, in G_1, a varies over the elements of F, and G_2 has q identity blocks. Both G_1 and G_2 have $q + 1$ columns (viewed over A).

Both G_1 and G_2 generate one-weight linear codes over A. The one non-zero weight is q. The codes are not equivalent because of the zero column in G_2.

Generalize

Let F be any finite field, $R = M_n(F)$ the matrix algebra, $S = M_{n+1}(F)$, and $A = M_{n,n+1}(F)$. Over R, A is a non-friendly module.

Question: for $n > 1$, can one find similar examples of non-extension?

If yes, one should be able to show that, for any finite QF ring that is not Frobenius, there is a counter-example to the extension theorem for Hamming weight (Dinh, López-Permouth).