An Essay on Equivalence of Linear Codes, II

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

AMS Special Session
Athens, Ohio
March 26, 2004

I want to explore several ideas concerning equivalence of linear codes from a particular point of view.

Outline

- Definitions from a functional point of view
- The weight mapping
- The role of symmetry
- MacWilliams extension theorem
- Generalizations

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 (right) 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 (right) 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_r-invariant functions* $\mathsf{Map}_0(M, \mathbb{Q})^{G_r}$.

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

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

More symmetry

Define a projection (averaging) map

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

by

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

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

Proposition *The weight mapping*

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

factors through P:

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

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

MacWilliams extension theorem

We have reduced the situation to

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

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.*

Example 1 (Klemm)

Let $R = \mathbb{F}_2[X,Y]/(X^2, XY, Y^2)$, w Hamming weight.

For M free of rank 1, both $\mathrm{Map}_0(M^\sharp, \mathbb{Q})^G$ and $\mathrm{Map}_0(M, \mathbb{Q})^G$ are 4-dimensional. (Orbits $\{X\}$, $\{Y\}$, $\{X+Y\}$, and $\mathcal{U}(R)$, under $G = \mathcal{U}(R)$.)

You will find that the image of W is further restricted to have the same values on X, Y, and $X+Y$. This forces a 2-dimensional kernel ($\eta(X^{\smile}) + \eta(Y^{\smile}) + \eta((X+Y)^{\smile}) = 0$).

Example 2

Let $R = \mathbb{Z}/5\mathbb{Z}$, written as $\{0, 1, 2, 3, 4\}$, with $w(r) = r$.

For M free of rank 1, the vector spaces are again of dimension 4, with $G = \{1\}$. One relation on the image,

$$w_\eta(1) + w_\eta(4) = w_\eta(2) + w_\eta(3),$$

forces a 1-dimensional kernel $\eta = (1, -1, -1, 1)$.

Some generalizations

Nechaev and collaborators, especially Greferath, Nechaev, Wisbauer

Linear codes over modules

R finite ring, "alphabet" (bi-)module ${}_S A_R$, weight function $w : A \to \mathbb{Q}$, $w(0) = 0$.

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

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

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

As before, we have

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

When is W injective?

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