An Essay on Equivalence of Linear Codes

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

AMS Special Session
Boulder
October 4, 2003

Outline

Definition(s) of linear codes

Equivalence of linear codes: When should two linear codes be considered to be the same?

- Extrinsic: permute columns, scale entries in a column.

- Intrinsic: linear isomorphism that preserves weight.

MacWilliams, 1961: these are the same, for Hamming weight over fields.

Generalizations of the MacWilliams extension theorem

Matrix treatment

Definition 1 *A* linear code C *over a field* F *is a* k*-dimensional subspace of the* n*-dimensional vector space* F^n*.*

A linear code can be presented by a generator matrix G of size $k \times n$. The rows of G form a basis for the linear code.

Allowing for a different basis leads to a left action of $GL(k, F)$.

Allowing for equivalence (scaling and permutations) leads to a right action of Monom$(n, F^\times)$, the group of $n \times n$ *monomial matrices* with non-zero entries from $F^\times$.

MacWilliams Extension Theorem

Work over a finite field F, using Hamming weight.

Theorem (MacWilliams, 1961) *Two linear codes C_1, C_2 in F^n are equivalent if and only if there exists a linear isomorphism from C_1 to C_2 that preserves Hamming weight.*

This result links the extrinsic and intrinsic notions of equivalence. It is a coding theory counterpart of theorems of Witt, 1937, and Arf, 1941, for bilinear and quadratic forms.

I'll sketch some proofs later.

Functional treatment

Definition 2 *A* linear code C *over a field* F *is a* k*-dimensional vector space* M *together with a linear embedding* $M \to F^n$*.*

By composing with the various coordinate projections $F^n \to F$, the linear embedding is given by n linear functionals $\lambda_1, \ldots, \lambda_n : M \to F$.

One can pre-compose with an element of

$$\mathrm{Aut}(M) \cong GL(k, F),$$

and post-compose with an element of

$$\mathrm{Monom}(n, F^\times).$$

The functional viewpoint was introduced by Assmus and Mattson, 1963.

Coordinate-free approach

In fact, Assmus and Mattson advocated a coordinate free approach, using linear functionals. Namely,

Definition 3 *A* linear code C *over a field* F *is a* k*-dimensional vector space* M *together with a multiset* S *of linear functionals on* M*.*

By not ordering the linear functionals, one can avoid the use of permutations in describing equivalence.

Multiplicity function approach

Let $M^\sharp$ denote the space of all linear functionals on a vector space M. Then $F^\times$ acts on $M^\sharp \setminus \{0\}$. The orbits form a projective space, which I will choose to denote by $\mathcal{O}^\sharp$.

Definition 4 *A* linear code C *over a field* F *is a* k*-dimensional vector space* M *together with a* multiplicity function $\eta : \mathcal{O}^\sharp \to \mathbb{N}$*.*

The monomial (scaling and permutation) aspects of equivalence are encapsulated in the multiplicity function η. There is still the action of Aut(M).

Weights

Let $w : F \to \mathbb{N}$ be a *weight function*, with $w(0) = 0$. The Hamming weight is one example.

Given a linear code $C = (M, \eta)$, the *weight* of a vector $x \in M$ is given by

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

For Hamming weight, this sum does not depend on the representative λ. In addition,

$$w_\eta(x) = w_\eta(ax)$$

for any non-zero $a \in F^\times$.

MacWilliams extension theorem, again

We work with Hamming weight over a field F.

Theorem *Given two linear codes* $C_1 = (M, \eta_1)$, $C_2 = (M, \eta_2)$ *with the same underlying space* M, *then* $\eta_1 = \eta_2$ *if and only if* $w_{\eta_1} = w_{\eta_2}$.

Let $\mathcal{O}$ denote the projective space obtained from the action of $F^\times$ on $M \setminus \{0\}$, and let $\mathbb{N}[\mathcal{O}]$, resp. $\mathbb{N}[\mathcal{O}^\sharp]$, be the spaces of functions $\mathcal{O} \to \mathbb{N}$, resp. $\mathcal{O}^\sharp \to \mathbb{N}$, then the forming of weights gives a well-defined map

$$T : \mathbb{N}[\mathcal{O}^\sharp] \to \mathbb{N}[\mathcal{O}], \quad \eta \mapsto w_\eta.$$

The extension theorem says that T is injective.

Sketch of proof

Let $\chi : F \to \mathbb{C}^\times$ be a non-trivial character of the additive group of F. Then every other character of F has the form $\pi(a) = \chi(ba)$, for some $b \in F$.

For the Hamming weight w, note that

$$w(a) = 1 - \frac{1}{|F|} \sum_{b \in F} \chi(ba),$$

is the expansion of w as a linear combination of characters on F.

Sketch, continued

Then, on M,

$$\begin{aligned} w_\eta(x) &= \sum_{\lambda\in\mathcal{O}^\sharp} \eta(\lambda) w(\lambda(x)) \\ &= \sum_{\lambda\in\mathcal{O}^\sharp} \eta(\lambda) - \frac{1}{|F|} \sum_{\lambda\in\mathcal{O}^\sharp} \sum_{b\in F} \eta(\lambda)\chi(b\lambda(x)) \end{aligned}$$

is the expansion of w_η as a linear combination of characters on M. Now, match up coefficients. (Ward, Wood, 1996)

MacWilliams, 1961; Bogart, Goldberg, Gordon, 1978, view as matrix equation for η. Greferath, Schmidt, 2000; Greferath, 2002.

Codes over rings

Given a finite ring R with a weight function $w : R \to \mathbb{N}$, let

$$G = \{u \in \mathcal{U}(R) : w(ur) = w(ru) = w(r), r \in R\}$$

be the *symmetry group* of the weight function w. $\mathcal{U}(R)$ is the group of units in R.

By taking M to be an R-module, and letting G play the role played by $F^{\times}$ in forming $\mathcal{O}$ and $\mathcal{O}^{\sharp}$, the whole apparatus carries over.

One major problem is to determine for which rings R and weight functions w the weight map T is injective.