Code Equivalence and Finite Frobenius Rings

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

OSU-Denison Conference
Columbus, Ohio
May 19, 2006

Acknowledgments

My thinking about equivalence of linear codes has been influenced greatly by recent work of a number of authors (Dinh, Greferath, Honold, López-Permouth, Nechaev, Schmidt, Wisbauer, ...). I wish to express my gratitude to them all.

Classical coding theory

Let $\mathbb{F} = \mathbb{F}_q$ be a finite field. A *linear code* C of *length* n and *dimension* k is a k-dimensional linear subspace $C \subset \mathbb{F}^n$.

A linear code C is often presented as the image of a linear transformation $G : \mathbb{F}^k \to \mathbb{F}^n$ represented by a $k \times n$ *generator matrix*, also denoted by G. The code C is then the row space of G.

Equivalence

Two linear codes C, C' of length n and dimension k are *equivalent* (with respect to Hamming weight) if there is an invertible transformation P of $\mathbb{F}^k$ and a monomial transformation T of $\mathbb{F}^n$ so that the generator matrices satisfy

$$G' = PGT.$$

The *Hamming weight* wt(x) of $x \in \mathbb{F}^n$ is the number of nonzero entries of x.

The monomial transformation $T : C \to C'$ preserves Hamming weight.

Theorem of MacWilliams

Theorem (MacWilliams, 1961) *Let* C, C' *be two linear codes in* $\mathbb{F}^n$*. If* $T : C \to C'$ *is a linear isomorphism preserving Hamming weight, then* T *extends to a monomial transformation of* $\mathbb{F}^n$*.*

Definition of linear codes over a ring

Let R be a finite ring with 1, with $\mathcal{U}$ denoting the group of units of R. A *linear code* C of length n is a left submodule of R^n.

Denote the underlying (finite) module of the code C by M. Then the linear code C is a linear embedding $M \to R^n$, given by a list $(\lambda_1, \ldots, \lambda_n)$ of linear functionals on M.

Up to monomial transformations, it is enough to keep track of the multiplicities of $\mathcal{U}$-scale classes of linear functionals.

Functional point of view

Let $\mathcal{O}^\sharp$ denote the $\mathcal{U}$-scale classes of nonzero linear functionals on M and $\mathcal{O}$ the $\mathcal{U}$-scale classes of nonzero elements of M.

Linear codes with underlying module M are parameterized, up to monomial equivalence, by multiplicity functions $\eta : \mathcal{O}^\sharp \to \mathbb{N}$. Denote by $\mathbb{N}[\mathcal{O}^\sharp]$ the set of all such multiplicity functions.

Associated to every linear code $C = (M, \eta)$ is the function of weights of elements of M:

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

where w is the Hamming weight. Note that $w_\eta(ux) = w_\eta(x)$, $x \in M$, $u \in \mathcal{U}$. This induces a map

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

Virtual linear codes

This is a Grothendieck-type construction.

A *virtual linear code* $C = (M, \eta)$ consists of a module M and a $\mathbb{Q}$-valued multiplicity function $\eta \in \mathbb{Q}[\mathcal{O}^\sharp]$.

Then W extends naturally to a $\mathbb{Q}$-linear transformation

$$W : \mathbb{Q}[\mathcal{O}^\sharp] \to \mathbb{Q}[\mathcal{O}].$$

In the case of $R = \mathbb{F}$, a finite field, the theorem of MacWilliams says that W is injective for any M.

Two main theorems

Theorem *If R is a finite Frobenius ring, then W is injective for any finite module M.*

The original proof of this in 1999 was character-theoretic. Greferath and Schmidt have also provided a combinatorial proof.

Theorem *If R is a finite ring and W is injective for any finite module M, then R is Frobenius.*

This is today's main topic, and we follow a strategy of Dinh and López-Permouth

Finite Frobenius rings

Suppose R is a finite ring with 1.

As rings, $R/\text{Rad}(R) \cong \bigoplus M_{\mu_i}(\mathbb{F}_{q_i})$.

Principal decomposition: ${}_R R \cong \bigoplus \mu_i R e_i$.

Top quotients: $T(Re_i) = Re_i/\text{Rad}(R)e_i$, the pull-back of the birth-certificate representation of $M_{\mu_i}(\mathbb{F}_{q_i})$.

Quasi-Frobenius (QF): there is a permutation σ with $T(Re_i) \cong \text{Soc}(Re_{\sigma(i)})$ and $\text{Soc}(e_i R) \cong T(e_{\sigma(i)} R)$.

Frobenius: QF, plus $\mu_{\sigma(i)} = \mu_i$. $R/\text{Rad}(R) \cong \text{Soc}(R)$, as one-sided modules.

Strategy of Dinh and López-Permouth

1. If R is not Frobenius, then there exists $kT(Re_i) \subset \text{Soc}(R) \subset R$, for some index i and multiplicity $k > \mu_i$.

2. Build counter-examples over the alphabet $M_{\mu_i,k}(\mathbb{F}_{q_i})$, when $k > \mu_i$. The alphabet is a left module over $M_{\mu_i}(\mathbb{F}_{q_i})$. (New)

3. Pull back the counter-examples to R.

Linear codes over modules

Important work was done by Greferath, Nechaev, and Wisbauer.

Start with two finite rings R and S and a finite (R, S)-bimodule A (for *alphabet*).

An *R-linear code over A* is a left R-submodule $C \subset A^n$ for some n.

View the linear code C as the image of an R-linear map $M \to A^n$ composed from n R-linear maps $M \to A$.

Functional point of view

Let $\mathcal{O}$ denote the $\mathcal{U}(R)$-scale classes of nonzero elements of M and $\mathcal{O}^\sharp$ the $\mathcal{U}(S)$-scale classes of nonzero elements of $\mathrm{Hom}_R(M, A)$.

Up to monomial transformations, a linear code with underlying module M is determined by a multiplicity function $\eta \in \mathbb{N}[\mathcal{O}^\sharp]$.

By generalizing to virtual codes, we again get a linear transformation

$$W : \mathbb{Q}[\mathcal{O}^\sharp] \to \mathbb{Q}[\mathcal{O}].$$

Counter-examples

Let $R = M_{\mu_i}(\mathbb{F}_{q_i})$, $S = M_k(\mathbb{F}_{q_i})$, and $A = M_{\mu_i,k}(\mathbb{F}_{q_i})$. Then $\mathcal{U}(R) = GL(\mu_i, \mathbb{F}_{q_i})$ and $\mathcal{U}(S) = GL(k, \mathbb{F}_{q_i})$.

Theorem *If $k > \mu_i$, then there exists a finite left R-module M such that W is not injective.*

Analysis of W

Let $M = M_{\mu_i,t}(\mathbb{F}_{q_i})$, with $t > \mu_i$. M is a left R-module. The set $\mathcal{O}$ consists of the nonzero row echelon classes of $\mu_i \times t$ matrices over $\mathbb{F}_{q_i}$. The vector space $\mathbb{Q}[\mathcal{O}]$ has dimension equal to the number of these row echelon classes.

The space $\mathrm{Hom}_R(M, A) = M_{t,k}(\mathbb{F}_{q_i})$. The set $\mathcal{O}^\sharp$ consists of the column echelon classes of $t \times k$ matrices over $\mathbb{F}_{q_i}$. The dimension of the vector space $\mathbb{Q}[\mathcal{O}^\sharp]$ is equal to the number of such column echelon classes.

Since $k > \mu_i$, $\dim(\mathbb{Q}[\mathcal{O}^\sharp]) > \dim(\mathbb{Q}[\mathcal{O}])$, so that W cannot be injective.

Example

Suppose $k = t = \mu_i + 1$. In this case, $\dim(\mathbb{Q}[\mathcal{O}^\sharp]) = 1 + \dim(\mathbb{Q}[\mathcal{O}])$, so that $\dim \ker W \geq 1$.

With $t = k$, $M = A$. We build two linear maps $g_+, g_- : A \to A^N$ by constructing two vectors v_+, v_- in $M_k(\mathbb{F}_{q_i})^N$ and multiplying componentwise, denoted as $g_\pm(x) = xv_\pm$, for $x \in A$.

The vector v_+ (resp., v_-) consists of all nonzero column echelon matrices of size $k \times k$ over $\mathbb{F}_{q_i}$ of even (resp., odd) rank, with multiplicity $q^{\binom{r}{2}}$ (where r is the rank of the matrix).

Homework: show that $\mathrm{wt}(g_+(x)) = \mathrm{wt}(g_-(x))$, for all $x \in A$.

There is no monomial transformation taking the image of g_+ to the image of g_-.