In Honor of Vera Pless

—

Equivalence of Linear Codes over Finite Rings

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

AMS Special Session
Cincinnati, Ohio
October 22, 2006

1. Introduction

On April 28, 1992, I gave a talk at the University of Illinois at Chicago. At the end of the talk, Vera Pless suggested that I re-examine the theorem of MacWilliams on code equivalence.

This talk is a summary of progress made.

2. Equivalence Theorem of MacWilliams

Let $\mathbb{F}$ be a finite field.

Two linear codes C, C' over $\mathbb{F}$ of length n are *equivalent* if there is a monomial transformation T of $\mathbb{F}^n$ such that $T(C) = C'$. In terms of generator matrices G, G', this means that

$$G' = PGM,$$

where P is invertible and M is monomial.

Theorem (MacWilliams, 1961) *Two linear codes $C, C' \subset \mathbb{F}^n$ are equivalent if and only if there exists a linear isomorphism $T : C \to C'$ that preserves Hamming weight,* $\mathrm{wt}(T(x)) = \mathrm{wt}(x)$, *all $x \in C$.*

3. Character-theoretic proof

Thann Ward observed that the weight preservation condition

$$\mathrm{wt}(T(x)) = \mathrm{wt}(x), \quad x \in C,$$

could be expressed in terms of the characters of $\mathbb{F}$. This led to a simple character-theoretic proof of the Equivalence Theorem of MacWilliams in H. N. Ward, J. A. Wood, Characters and the equivalence of codes, J. Combin. Theory Ser. A **73** (1996), 348–352.

4. Generalizations to codes over rings

In 1993–1994 the famous $\mathbb{Z}/4\mathbb{Z}$-paper of Hammons, et al. appeared. That work inspired the problem of generalizing the Equivalence Theorem to linear codes over rings.

Problem *Determine conditions on a finite ring R so that two (left) linear codes $C, C' \subset R^n$ are monomially equivalent if and only if there is an R-linear isomorphism $f : C \to C'$ preserving Hamming weight.*

Note that monomial equivalence implies the existence of a Hamming weight preserving isomorphism, namely the monomial transformation restricted to C. So, the problem is an extension problem: when can a Hamming weight preserving isomorphism $f : C \to C'$ be extended to a monomial transformation $R^n \to R^n$?

5. Main Theorem

The answer is that R must be a finite Frobenius ring.

Theorem *Let R be a finite ring with* 1*. Every Hamming weight preserving isomorphism $C \to C'$ extends to a monomial transformation $R^n \to R^n$ if and only if R is a Frobenius ring.*

The 'if' portion dates from Duality for modules over finite rings and applications to coding theory, Amer. J. Math. **121** (1999), 555-575.

The 'only if' portion is new: A coding-theoretic characterization of finite Frobenius rings, submitted to Amer. J. Math., 2006.

6. Finite Frobenius rings

Every finite ring R with 1 admits decompositions

$$R/\mathrm{Rad}R \cong \bigoplus_{i=1}^{l} M_{\mu_i}(\mathbb{F}_{q_i}),$$
$$_RR \cong \bigoplus_{i=1}^{l} \mu_i Re_i,$$

where the Re_i, $i = 1, 2, \ldots, l$, represent the distinct isomorphism classes of principal indecomposable modules. Each Re_i has a top quotient $T(Re_i) = Re_i/(\mathrm{Rad}R)e_i$ and a socle $\mathrm{Soc}(Re_i)$.

The ring R is *quasi-Frobenius* if there exists a permutation σ of $\{1, 2, \ldots, l\}$ with $T(Re_i) \cong \mathrm{Soc}(Re_{\sigma(i)})$. The ring is *Frobenius* if, in addition, $\mu_{\sigma(i)} = \mu_i$.

7. Equivalencies for finite rings

- R Frobenius
- ${}_R(R/\mathrm{Rad}R) \cong \mathrm{Soc}({}_RR)$ (Honold)
- ${}_R\widehat{R} \cong {}_RR$

where $\widehat{R}$ is the character module of R.

The character isomorphism $\widehat{R} \cong R$ allows the character-theoretic proof of Ward-Wood to be applied over finite Frobenius rings.

8. Counter-examples for non-Frobenius rings

The following strategy is due to H. Q. Dinh, S. R. López-Permouth, On the equivalence of codes over rings and modules, Finite Fields Appl. **10** (2004), 615–625.

If R is not Frobenius, then there is an index i, $1 \leq i \leq l$, and $k > \mu_i$ such that $kT(Re_i) \subset \mathrm{Soc}(R)$.

The module $T(Re_i)$ is just the standard birth-certificate module $M_{\mu_i,1}(\mathbb{F}_{q_i})$ of $M_{\mu_i}(\mathbb{F}_{q_i})$ pulled back to R. Then $kT(Re_i) \cong M_{\mu_i,k}(\mathbb{F}_{q_i})$, with $k > \mu_i$.

We now build linear codes over the alphabet $M_{\mu_i,k}(\mathbb{F}_{q_i})$. By pulling back, we build a counter-example to extension over a non-Frobenius ring.

Codes over modules—work of Greferath, Nechaev, Wisbauer.

9. Construction

Let $m = \mu_i$, $q = q_i$, $A = M_{m,k}(\mathbb{F}_q)$, $k > m$.

Build two vectors $v_+, v_- \in M_k(\mathbb{F}_q)^N$:

Entries of v_+ consist of all the column echelon matrices of size $k \times k$ over $\mathbb{F}_q$ of even rank, with multiplicity $q^{\binom{r}{2}}$, r denoting rank. Entries of v_- are similar, but with odd rank.

Two codes $C_+, C_- \subset A^N$ are the images of $g_\pm : A \to A^N$, $X \mapsto Xv_\pm$ (entry-wise matrix multiplication).

Theorem/Exercise *There is a Hamming weight preserving isomorphism $C_+ \to C_-$ that does not extend to a monomial transformation.*

10. Example

This is a re-casting of an example first found in M. Greferath, S. Schmidt, Finite ring combinatorics and MacWilliams's equivalence theorem, J. Combin. Theory Ser. A **92** (2000), 17–28.

$A = M_{1,2}(\mathbb{F}_2)$

$$
\begin{aligned}
v_+ &= \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix} \\
v_- &= \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}
\end{aligned}
$$

$$
\begin{aligned}
(xy)v_+ &= \begin{pmatrix} 0 & 0 & x & y & x & y \end{pmatrix} \\
(xy)v_- &= \begin{pmatrix} x & 0 & z & 0 & y & 0 \end{pmatrix}
\end{aligned}
$$

where $z = x + y$.