Applications of Finite Frobenius Rings to Algebraic Coding Theory — I. Two Theorems of MacWilliams over Finite Frobenius Rings

Jay A. Wood

Western Michigan University
http://homepages.wmich.edu/∼jwood

Symposium on Ring and Representation Theory,
Okayama University, September 25, 2011

Acknowledgments

- I am pleased to be visiting the city of Okayama, and I thank the symposium organizers, especially Professor Kunio Yamagata, for the invitation and for their hospitality.
- I thank the Japan Society for the Promotion of Science for its financial support of the symposium.

For Your Amusement

Table: Mathematical Genealogy of Two Speakers

Dan Zacharia	Jay Wood
Maurice Auslander	Shoshichi Kobayashi
Robert Taylor	Carl Allendoerfer
JHC Whitehead	Tracy Thomas
Oswald Veblen	
EH Moore	
⋮	
Simeon Poisson	
Pierre-Simon Laplace (and JL Lagrange)	
Jean Le Rond d'Alembert	

The Coding Problem

- How to ensure the integrity of a message transmitted over a noisy channel?
- Cleverly add redundancy.
- Encode possible messages (information) as a string of elements in an alphabet.
- Transmit the string over the channel.
- Detect errors and decode.

Adding Algebraic Structure

- Assume the alphabet is a finite field $\mathbb{F}$.
- Assume the set of messages M is a finite dimensional vector space over F of dimension k.
- The encoding is a linear embedding $M \hookrightarrow \mathbb{F}^n$, for some n.
- The image is a linear code of *length* n.

Objectives for this Talk

- Some of the language of algebraic coding theory.
- Two theorems of MacWilliams valid over finite fields.
- Finite Frobenius rings and their character modules.
- Generalize the two theorems.

Definitions (a)

- Let R be a finite associative ring with 1.
- Let A be a finite unital left R-module; A will be the *alphabet*.
- A left *linear code* over A of length n is a left R-submodule $C \subset A^n$.
- Special case: when $A = R$ as a left module.

Definitions (b)

- For $x = (x_1, \ldots, x_n) \in A^n$, the *Hamming weight* $\mathrm{wt}(x)$ equals the number of nonzero entries of x.
- For a linear code $C \subset A^n$, the *Hamming weight enumerator* is the polynomial

$$W_C(X, Y) = \sum_{x \in C} X^{n-\mathrm{wt}(x)} Y^{\mathrm{wt}(x)}.$$

Definitions (c)

- When $A = R$, define a *dot product* on R^n by

$$x \cdot y = \sum_{i=1}^{n} x_i y_i,$$

for $x = (x_1, \dots, x_n), y = (y_1, \dots, y_n) \in R^n$.
- When $A = R$, and $C \subset R^n$ is a left linear code, define the *right annihilator* $r(C)$ by

$$r(C) = \{y \in R^n : x \cdot y = 0, x \in C\}.$$

MacWilliams Identities (1962/63)

- Let $C \subset \mathbb{F}_q^n$ be a linear code over $\mathbb{F}_q$.
- The MacWilliams identities hold:

$$W_C(X, Y) = \frac{1}{|r(C)|} W_{r(C)}(X + (q-1)Y, X - Y).$$

Florence Jessie MacWilliams

- 1917–1990
- 1962 doctoral dissertation under Andrew Gleason at Harvard. (Mackey, Stone, Ge. Birkhoff, EH Moore.)
- "Combinatorial Problems of Elementary Abelian Groups"
- Three sections:
  - Extension theorem on isometries
  - The MacWilliams identities
  - Coverings

Monomial Transformations

- A *monomial transformation* $T : R^n \to R^n$ has the form
$$T(x_1, \ldots, x_n) = (x_{\sigma(1)}u_1, \ldots, x_{\sigma(n)}u_n),$$
where σ is a permutation of $\{1, \ldots, n\}$ and $u_1, \ldots, u_n$ are units of R.
- A monomial transformation preserves Hamming weight: $\mathrm{wt}(T(x)) = \mathrm{wt}(x)$, $x \in R^n$.

MacWilliams Extension Theorem (1961/62)

- Assume $R = \mathbb{F}$, a finite field.
- Assume $C_1, C_2 \subset \mathbb{F}^n$ are linear codes.
- If $f : C_1 \to C_2$ is a linear isomorphism that preserves Hamming weight, then f extends to a monomial transformation of $\mathbb{F}^n$.

Generalizing the Theorems of MacWilliams

- When $A = R$, are the MacWilliams identities and the MacWilliams extension theorem still valid?
- Yes, if R is a finite Frobenius ring.
- Why Frobenius?
- There are character-theoretic proofs over finite fields that use the crucial property $\widehat{\mathbb{F}} \cong \mathbb{F}$.
- Frobenius rings satisfy $\widehat{R} \cong R$, and the same proofs will work.

Characters

- Let $(G, +)$ be a finite abelian group.
- A *character* π of G is a group homomorphism $\pi : (G, +) \to (\mathbb{C}^\times, \times)$, the nonzero complexes.
- The set $\widehat{G}$ of all characters of G is itself a finite abelian group called the *character group*.
- $|\widehat{G}| = |G|$.
- As elements of the vector space of all functions from G to $\mathbb{C}$, the characters are linearly independent.
- If M is a finite left R-module, then $\widehat{M}$ is a right R-module.

Two Useful Formulas

$$\sum_{x \in G} \pi(x) = \begin{cases} |G|, & \pi = 1, \\ 0, & \pi \neq 1. \end{cases}$$

$$\sum_{\pi \in \widehat{G}} \pi(x) = \begin{cases} |G|, & x = 0, \\ 0, & x \neq 0. \end{cases}$$

Finite Frobenius Rings

- Finite ring R with 1.
- The (Jacobson) *radical* $\mathrm{Rad}(R)$ of R is the intersection of all maximal left ideals of R; $\mathrm{Rad}(R)$ is a two-sided ideal of R.
- The (left/right) *socle* $\mathrm{Soc}(R)$ of R is the ideal of R generated by all the simple left/right ideals of R.
- R is *Frobenius* if $R/\mathrm{Rad}(R) \cong \mathrm{Soc}(R)$ as one-sided modules (both left and right).

Two Useful Theorems About Finite Frobenius Rings

- (Honold, 2001) $R/\operatorname{Rad}(R) \cong \operatorname{Soc}({}_R R)$ as left modules iff $R/\operatorname{Rad}(R) \cong \operatorname{Soc}(R_R)$ as right modules.
- R is Frobenius iff $R \cong \widehat{R}$ as left modules iff $R \cong \widehat{R}$ as right modules (1999).
- Corollary: R is Frobenius iff there exists a character π of R such that $\ker \pi$ contains no nonzero left (right) ideal of R. This π is a *generating character*.

Fourier Transform

- Given a function $f : G \to V$, with V a complex vector space, its *Fourier transform* is a function $\hat{f} : \widehat{G} \to V$ defined by

$$\hat{f}(\pi) = \sum_{x \in G} \pi(x) f(x), \quad \pi \in \widehat{G}.$$

- Fourier inversion:

$$f(x) = \frac{1}{|G|} \sum_{\pi \in \widehat{G}} \pi(-x) \hat{f}(\pi), \quad x \in G.$$

Poisson Summation Formula

- For a subgroup $H \subset G$, define its *annihilator* $(\widehat{G} : H) = \{\pi \in \widehat{G} : \pi(H) = 1\}$.
- $|(\widehat{G} : H)| = |G|/|H|$.
- For a subgroup $H \subset G$ and any $a \in G$,

$$\sum_{h \in H} f(a+h) = \frac{1}{|(\widehat{G} : H)|} \sum_{\pi \in (\widehat{G}:H)} \pi(-a)\hat{f}(\pi).$$

- In particular, for a subgroup $H \subset G$,

$$\sum_{h \in H} f(h) = \frac{1}{|(\widehat{G} : H)|} \sum_{\pi \in (\widehat{G}:H)} \hat{f}(\pi).$$

MacWilliams Identities over Finite Frobenius Rings

Theorem (1999)

Let R be a finite Frobenius ring. If $C \subset R^n$ is a left linear code, then the MacWilliams identities hold:

$$W_C(X,Y) = \frac{1}{|r(C)|} W_{r(C)}(X + (|R|-1)Y, X - Y).$$

Proof of the MacWilliams Identities (a)

- The proof follows a proof due to Gleason (1970).
- Let R be Frobenius with generating character ρ.
- Let $G = R^n$, an abelian group under addition.
- Let $H = C$, a left linear code.
- Let $V = \mathbb{C}[X, Y]$, a complex vector space.
- Let $f : G \to V$ be

$$f(x) = X^{n-\mathrm{wt}(x)} Y^{\mathrm{wt}(x)}.$$

Proof of the MacWilliams Identities (b)

- By Frobenius hypothesis, every character of $G = R^n$ has the form π_a, for some $a \in R^n$, with

$$\pi_a(x) = \rho(x \cdot a), \quad x \in R^n.$$

- $\pi_a \in (\widehat{G} : H)$ if and only if $a \in r(C)$.
- $|(\widehat{G} : H)| = |r(C)|$.

Proof of the MacWilliams Identities (c)

- For $f(x) = X^{n-\mathrm{wt}(x)}Y^{\mathrm{wt}(x)}$,
$$\hat{f}(\pi_a) = (X + (|R|-1)Y)^{n-\mathrm{wt}(a)}(X-Y)^{\mathrm{wt}(a)}.$$
- This requires some manipulations and use of $\sum \pi(x)$ formulas. (Next slide.)
- Recognize $\hat{f}(\pi_a)$ as summand of $W_{r(C)}(X + (|R|-1)Y, X-Y)$.

Idea of Manipulation

- Let $n = 1$, $f(x) = X^{1-\mathrm{wt}(x)} Y^{\mathrm{wt}(x)}$.

$$
\begin{aligned}
\hat{f}(\pi_a) &= \sum_{x \in R} \pi_a(x) X^{1-\mathrm{wt}(x)} Y^{\mathrm{wt}(x)} \\
&= X + \sum_{x \neq 0} \pi_a(x) Y \\
&= \begin{cases} X + (|R| - 1)Y, & a = 0, \\ X - Y, & a \neq 0, \end{cases} \\
&= (X + (|R| - 1)Y)^{1-\mathrm{wt}(a)} (X - Y)^{\mathrm{wt}(a)}
\end{aligned}
$$

MacWilliams Extension Theorem over Finite Frobenius Rings

Theorem (1999)

Let R be a finite Frobenius ring, and suppose $C_1, C_2 \subset R^n$ are left linear codes. If $f : C_1 \longrightarrow C_2$ is an R-linear isomorphism that preserves Hamming weight, then f extends to a monomial transformation of R^n.

Character-Theoretic Proof (a)

- The proof follows a proof of Ward and Wood in the finite field case (1996).
- View C_i as the image of $\lambda_i : M \to R^n$, with $\lambda_i = (\lambda_{i,1}, \ldots, \lambda_{i,n})$ and $\lambda_2 = f \circ \lambda_1$.
- Using character sums, express Hamming weight as:

$$\mathrm{wt}(\lambda_i(x)) = n - \sum_{j=1}^{n} \frac{1}{|R|} \sum_{\pi \in \widehat{R}} \pi(\lambda_{i,j}(x)), x \in M.$$

Character-Theoretic Proof (b)

- Because f preserves Hamming weight, we get

$$\sum_{j=1}^{n} \sum_{\pi \in \widehat{R}} \pi(\lambda_{1,j}(x)) = \sum_{k=1}^{n} \sum_{\psi \in \widehat{R}} \psi(\lambda_{2,k}(x)), x \in M.$$

- In a Frobenius ring, there is a generating character ρ. Every character of R has the form $a\rho$, $a \in R$.
- $(a\rho)(r) := \rho(ra)$, $r \in R$.

Character-Theoretic Proof (c)

- Re-write weight-preservation equation as

$$\sum_{j=1}^{n}\sum_{a\in R}(a\rho)(\lambda_{1,j}(x)) = \sum_{k=1}^{n}\sum_{b\in R}(b\rho)(\lambda_{2,k}(x)), x \in M.$$

- Or as

$$\sum_{j=1}^{n}\sum_{a\in R}\rho(\lambda_{1,j}(x)a) = \sum_{k=1}^{n}\sum_{b\in R}\rho(\lambda_{2,k}(x)b), x \in M.$$

Character-Theoretic Proof (d)

- The last equation is an equation of characters on M.
- Characters are linearly independent, so one can match up terms (carefully).
- A technical argument involving a preordering given by divisibility in R shows how to match up terms with units as multipliers.
- This produces a permutation σ and units u_i in R such that $\lambda_{2,k} = \lambda_{1,\sigma(k)} u_k$, as desired.