Characterizing Finite Frobenius Rings Via Coding Theory

Jay A. Wood

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

Algebra and Communications Seminar
University College Dublin
November 7, 2011

Florence Jessie MacWilliams

- 1917–1990
- Bell Labs
- 1962 Harvard dissertation under Andrew Gleason: "Combinatorial Problems of Elementary Abelian Groups"
- Three sections:
  - Extension theorem on isometries
  - The MacWilliams identities
  - Coverings

Linear Codes Defined over Finite Rings

- Let R be a finite ring with 1. A *linear code* of length n defined over R is a left R-submodule $C \subset R^n$.
- There were some results on codes over rings in the 1970s, but the real breakthrough came in 1994. Hammons, Kumar, Calderbank, Sloane, and Solé showed that important duality properties of certain non-linear binary codes could be explained by linear codes defined over $\mathbb{Z}/4\mathbb{Z}$.
- Are the fundamental results of MacWilliams valid over finite rings?

Code Equivalence

- When should two linear codes be considered the same?
- Monomial equivalence (external)
- Linear isometries (internal)
- These notions are the same over finite fields: the MacWilliams extension theorem.

Monomial equivalence

- Work over a finite ring R.
- A permutation σ of $\{1, \ldots, n\}$ and invertible elements (units) $u_1, \ldots, u_n$ in R determine a *monomial transformation* $T : R^n \longrightarrow R^n$ by

$$T(x_1, \ldots, x_n) = (x_{\sigma(1)}u_1, \ldots, x_{\sigma(n)}u_n).$$

- Two linear codes $C_1, C_2 \subset R^n$ are *monomially equivalent* if there exists a monomial transformation T such that $C_2 = T(C_1)$.

Linear Isometries

- The *Hamming weight* $\mathrm{wt}(x)$ of a vector $x = (x_1, \ldots, x_n) \in R^n$ is the number of nonzero entries in x.
- A linear isomorphism $f : C_1 \longrightarrow C_2$ between linear codes $C_1, C_2 \subset R^n$ is an *isometry* if it preserves Hamming weight: $\mathrm{wt}(f(x)) = \mathrm{wt}(x)$, for all $x \in C_1$.
- If T is a monomial transformation with $C_2 = T(C_1)$, then the restriction of T to C_1 is an isometry.
- Is the converse true? Does every linear isometry come from a monomial transformation?

MacWilliams Extension Theorem over Finite Fields

Assume C_1, C_2 are linear codes in $\mathbb{F}_q^n$. If a linear isomorphism $f : C_1 \longrightarrow C_2$ preserves Hamming weight, then f extends to a monomial transformation of $\mathbb{F}_q^n$.

- MacWilliams (1961); Bogart, Goldberg, Gordon (1978)
- Ward, Wood (1996)

Generalizing the Work of MacWilliams

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

Characters of Finite Abelian Groups

- Let $(G, +)$ be a finite abelian group.
- A *character* π of G is a group homomorphism $\pi : (G, +) \to (\mathbb{C}^\times, \times)$, where $(\mathbb{C}^\times, \times)$ is the multiplicative group of nonzero complex numbers.
- Example: let $G = \mathbb{Z}/n\mathbb{Z}$ be the integers modulo n. For any $a \in \mathbb{Z}/n\mathbb{Z}$, $\pi_a(x) = \exp(2\pi iax/n)$, $x \in G$, is a character of G.
- Example: let $G = \mathbb{F}_q$. For any $a \in \mathbb{F}_q$, $\pi_a(x) = \exp(2\pi i \operatorname{Tr}(ax)/p)$, $x \in \mathbb{F}_q$, is a character of $\mathbb{F}_q$. ($\operatorname{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ is the absolute trace to the prime subfield.)

Character Groups

- 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 (Hirano, 1997; indep. 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*.

Examples of Finite Frobenius Rings

- Finite fields $\mathbb{F}_q$: $\pi(x) = \exp(2\pi i \operatorname{Tr}(x)/p)$.
- $\mathbb{Z}/n\mathbb{Z}$: $\pi(x) = \exp(2\pi i x/n)$.
- Galois rings (Galois extensions of $\mathbb{Z}/p^m\mathbb{Z}$).
- Finite chain rings (all ideals form a chain).
- Products of Frobenius rings.
- Matrix rings over a Frobenius ring: $M_n(R)$.
- Finite group rings over a Frobenius ring: $R[G]$.
- $\mathbb{F}_2[X, Y]/(X^2, XY, Y^2)$ is not Frobenius (Klemm, 1989).

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.

- Also, Greferath and Schmidt (2000), using poset techniques.
- Greferath (2002), generalizing Bogart, et al.

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 $\Lambda_i : M \longrightarrow R^n$, 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.

Re-Write the Extension Problem

- The character-theoretic proof just given generalized the Ward-Wood proof over finite fields.
- Now we will generalize an approach due to MacWilliams; Bogart, Goldberg, and Gordon; and Greferath in order to re-formulate the extension problem.
- Will use R-linear codes over an alphabet A, an idea of Nechaev and his collaborators.

Monomial Transformations

- R finite ring, A finite left R-module (an *alphabet*).
- A *linear code* over A is a left R-submodule $C \subset A^n$.
- A *monomial transformation* $T : A^n \longrightarrow A^n$ has the form

$$T(x_1, \ldots, x_n) = (x_{\sigma(1)}\phi_1, \ldots, x_{\sigma(n)}\phi_n),$$

for $(x_1, \ldots, x_n) \in A^n$, where σ is a permutation of $\{1, \ldots, n\}$ and $\phi_1, \ldots, \phi_n \in \mathrm{Aut}(A)$.

Re-Formulation of Extension Problem (a)

- View a left R-linear code $C \subset A^n$ as the image of an R-linear homomorphism $\Lambda : M \longrightarrow A^n$, where $\Lambda = (\lambda_1, \ldots, \lambda_n)$ and $\lambda_i : M \longrightarrow A$ are R-linear.
- Up to monomial equivalence, what matters is the number of λ_i's in a given scale class (under right action by automorphisms of A).
- The group $\mathrm{Aut}(A)$ of R-automorphisms of A acts on the right on the group $\mathrm{Hom}_R(M, A)$ of R-linear homomorphisms from M to A.

Re-Formulation of Extension Problem (b)

- Let $\mathcal{O}^\sharp$ be the set of nonzero orbits of the action of $\mathrm{Aut}(A)$ on $\mathrm{Hom}_R(M, A)$.
- Let $\eta : \mathcal{O}^\sharp \longrightarrow \mathbb{N}$ be the *multiplicity function* that counts how many of the λ_i belong to each scale class.
- Functions equivalent to η have appeared elsewhere under various names (value function, multiset, etc.).

Re-Formulation of Extension Problem (c)

- Summary, so far: the monomial equivalence class of $\Lambda : M \longrightarrow A^n$ is encoded by its multiplicity function $\eta : \mathcal{O}^\sharp \longrightarrow \mathbb{N}$.

Re-Formulation of Extension Problem (d)

- Now, turn to Hamming weights.
- Note that the Hamming weight depends only on the left scale class of $x \in M$ via units of R:

$$\mathrm{wt}(\Lambda(ux)) = \mathrm{wt}(u\Lambda(x)) = \mathrm{wt}(\Lambda(x)), x \in M, u \in \mathcal{U}.$$

- Let $\mathcal{O}$ be the set of nonzero orbits of the left action of the group of units $\mathcal{U}$ on M.

Re-Formulation of Extension Problem (e)

- The Hamming weight $\mathrm{wt}(\Lambda(x))$ depends only on the scale classes of the λ_i ($\phi_i \in \mathrm{Aut}(A)$):

$$\mathrm{wt}(\Lambda(x)) = \sum_{i=1}^{n} \mathrm{wt}(\lambda_i(x)) = \sum_{i=1}^{n} \mathrm{wt}(\lambda_i(x)\phi_i).$$

- The Hamming weight does not depend on the order of the λ_i.

Re-Formulation of Extension Problem (f)

- Let $F(\mathcal{O}^\sharp, \mathbb{N})$ denote the set of all functions from $\mathcal{O}^\sharp$ to $\mathbb{N}$. Similarly for $F(\mathcal{O}, \mathbb{N})$.
- The Hamming weight gives a well-defined map $W : F(\mathcal{O}^\sharp, \mathbb{N}) \to F(\mathcal{O}, \mathbb{N})$:

$$W(\eta)(x) = \sum_{\lambda \in \mathcal{O}^\sharp} \eta(\lambda)\, \mathrm{wt}(\lambda(x)).$$

- Summary: the Extension Theorem for Hamming weight holds iff the map W is injective for every finite module M.

Re-Formulation of Extension Problem (g)

- By formally allowing rational coefficients, we get

$$W : F(\mathcal{O}^{\sharp}, \mathbb{Q}) \to F(\mathcal{O}, \mathbb{Q}).$$

- W is a linear transformation of $\mathbb{Q}$-vector spaces.
- The Extension Theorem for Hamming weight holds iff the map W is injective for every finite module M.

A Counter-Example to Extension (a)

- For R-linear codes defined over a module A, the extension theorem might not hold.
- Let $R = M_m(\mathbb{F}_q)$, the ring of $m \times m$ matrices over $\mathbb{F}_q$. The group of units is $\mathcal{U} = GL(m, \mathbb{F}_q)$.
- Let $A = M_{m,k}(\mathbb{F}_q)$, the space of all $m \times k$ matrices. A is a left R-module. $\mathrm{Aut}(A) = GL(k, \mathbb{F}_q)$.
- Assume $m < k$.

A Counter-Example to Extension (b)

- A general left R-module has the form $M = M_{m,j}(\mathbb{F}_q)$. Then $Hom_R(M, A) = M_{j,k}(\mathbb{F}_q)$ (via right matrix multiplication).
- Left action of $\mathcal{U} = GL(m, \mathbb{F}_q)$ on $M = M_{m,j}(\mathbb{F}_q)$: orbits $\mathcal{O}$ consist of row reduced echelon matrices of size $m \times j$.
- Right action of $\mathrm{Aut}(A) = GL(k, \mathbb{F}_q)$ on $Hom_R(M, A) = M_{j,k}(\mathbb{F}_q)$: orbits $\mathcal{O}^\sharp$ consist of column reduced echelon matrices of size $j \times k$.

A Counter-Example to Extension (c)

- In $W : F(\mathcal{O}^\sharp, \mathbb{Q}) \to F(\mathcal{O}, \mathbb{Q})$, the dimensions over $\mathbb{Q}$ of the domain and range equal the number of elements in $\mathcal{O}^\sharp$ and $\mathcal{O}$, respectively.
- $\dim_{\mathbb{Q}} F(\mathcal{O}^\sharp, \mathbb{Q})$ equals the number of column reduced echelon matrices of size $j \times k$.
- $\dim_{\mathbb{Q}} F(\mathcal{O}, \mathbb{Q})$ equals the number of row reduced echelon matrices of size $m \times j$.
- Since $k > m$, $\dim_{\mathbb{Q}} F(\mathcal{O}^\sharp, \mathbb{Q}) > \dim_{\mathbb{Q}} F(\mathcal{O}, \mathbb{Q})$, and W is not injective.

Explicit Counter-Examples (a)

- $R = M_1(\mathbb{F}_q) = \mathbb{F}_q$, $A = M_{1,2}(\mathbb{F}_q)$. Remember that Hamming weight depends on elements being nonzero in A (nonzero as a pair).
- For $q = 2$, $n = 3$:

C_+	C_-
$(00, 00, 00)$	$(00, 00, 00)$
$(00, 10, 10)$	$(10, 10, 00)$
$(00, 01, 01)$	$(00, 10, 10)$
$(00, 11, 11)$	$(10, 00, 10)$

Explicit Counter-Examples (b)

- For $q = 3$, $n = 4$:

C_+	C_-
$(00, 00, 00, 00)$	$(00, 00, 00, 00)$
$(00, 01, 01, 01)$	$(00, 10, 20, 10)$
$(00, 02, 02, 02)$	$(00, 20, 10, 20)$
$(00, 10, 10, 10)$	$(10, 10, 10, 00)$
$(00, 11, 11, 11)$	$(10, 20, 00, 10)$
$(00, 12, 12, 12)$	$(10, 00, 20, 20)$
$(00, 20, 20, 20)$	$(20, 20, 20, 00)$
$(00, 21, 21, 21)$	$(20, 00, 10, 10)$
$(00, 22, 22, 22)$	$(20, 10, 00, 20)$

Characterizing Finite Frobenius Rings

- Theorem (2008). Suppose R is a finite ring, and set $A = R$. If the extension theorem for Hamming weight holds for linear codes over R, then R is a Frobenius ring.
- Dinh and López-Permouth (2004–2005) proved some special cases and developed a strategy to prove the general result.

The Strategy of Dinh and López-Permouth

- Every non-Frobenius ring has a copy of some $M_{m,k}(\mathbb{F}_q) \subset \mathrm{Soc}(R)$, with $m < k$.
- The extension theorem fails for $M_{m,k}(\mathbb{F}_q) \subset \mathrm{Soc}(R)$, with $m < k$ (as a module over $M_m(\mathbb{F}_q)$).
- View the $M_{m,k}(\mathbb{F}_q)$ counter-examples as modules (and hence counter-examples) over R itself.

Structure of a Finite Ring

- Let R be a finite ring with 1.
- $R/\operatorname{Rad}(R)$ is a sum of simple rings, which must be matrix rings over finite fields:

$$R/\operatorname{Rad}(R) \cong \bigoplus M_{m_i}(\mathbb{F}_{q_i}).$$

- $\operatorname{Soc}({}_R R)$ is a left module over $R/\operatorname{Rad}(R)$, so

$$\operatorname{Soc}({}_R R) \cong \bigoplus M_{m_i,k_i}(\mathbb{F}_{q_i}).$$

Frobenius Rings

- Remember that a finite ring is Frobenius if $R/\operatorname{Rad}(R)$ is isomorphic to $\operatorname{Soc}(R)$ as one-sided modules (so $k_i = m_i$).
- In a non-Frobenius ring, there exist $k_i \neq m_i$, with some larger and some smaller.
- These provide the counter-examples to the extension theorem.

Additional Comments (a)

- One can characterize alphabets A for which the extension theorem holds: $A \subset \widehat{R}$ plus one more condition.
- In particular, $A = \widehat{R}$ always satisfies the extension theorem for Hamming weight (for any finite ring R, Frobenius or not). This is a theorem of Greferath, Nechaev, Wisbauer (2004) that extends the original Frobenius result.

Additional Comments (b)

- Some results are known for other weight functions, especially the "homogeneous weight" (again, by Greferath, Nechaev, Wisbauer).
- But, there is much that is not known about other weight functions. For example, it is not known if the extension theorem is always true for the Lee weight over $R = \mathbb{Z}/n\mathbb{Z}$ for all n.
- Are there other uses of $W : F(\mathcal{O}^\sharp, \mathbb{Q}) \to F(\mathcal{O}, \mathbb{Q})$?

References

- These slides and other papers are available on the web: `http://homepages.wmich.edu/~jwood`
- Many references in the paper "Foundations of Linear Codes ... "