The use of Frobenius rings in coding theory: a personal view

Jay A. Wood

Department of Mathematics
Western Michigan University
jay.wood@wmich.edu

AMS meeting, Kalamazoo, Michigan
October 18, 2008

Linear codes over a module

- Let R be a finite ring with 1.
- Let A (for *alphabet*) be a finite left R-module.
- A *linear code* of length n over A is a left R-submodule $C \subset A^n$.
- Special case when $A = R$ itself: linear codes over a ring.

Equivalence

- When should two linear codes over A be equivalent?
  - ('extrinsic') Existence of a monomial transformation of A^n taking one code to the other.
  - ('intrinsic') Existence of a linear isomorphism between the codes that preserves Hamming weight.
- When are these two notions of equivalence the same?

Easy direction

- Extrinsic equivalence implies intrinsic equivalence.
- A monomial transformation $T : A^n \to A^n$ has the form

$$T(x_1, \dots, x_n) = (x_{\sigma(1)}\tau_1, \dots, x_{\sigma(n)}\tau_n),$$

  where σ is a permutation of $\{1, 2, \dots, n\}$ and the τ_i are R-automorphisms of A.
- If $T : A^n \to A^n$ is a monomial transformation with $T(C_1) = C_2$, then the restriction $T : C_1 \to C_2$ is a linear isomorphism that preserves Hamming weight.

Hard direction

- The converse, intrinsic equivalence implying extrinsic equivalence, requires solving an extension problem.
- Given: $f : C_1 \longrightarrow C_2$, a linear isomorphism that preserves Hamming weight, with $C_1, C_2 \subset A^n$.
- Problem: extend f to a monomial transformation of A^n.

Solutions

- MacWilliams, 1961, over finite fields.
- Bogart, Goldberg, Gordon, 1978, also over finite fields.
- Ward, W., 1996, over finite fields, using characters.
- W., 1999, over finite Frobenius rings, using characters.
- Greferath, Schmidt, 2000, over finite Frobenius rings, using poset of principal ideals.
- Greferath, 2002, over finite Frobenius rings, generalizing Bogart, et al.

Solutions, continued

- Greferath, Nechaev, Wisbauer, 2004, for A a Frobenius bimodule.
- W., submitted, for certain submodules of a Frobenius bimodule (pseudo-injective submodules of $\widehat{R}$).

Why does Frobenius work?

- The proof with Ward using characters relies on the fact that the group of characters of the additive group of a finite field is itself a vector space over the finite field, necessarily of dimension 1. That is, $\widehat{R} \cong R$ as vector spaces.
- Which finite rings have the same property, that $\widehat{R} \cong R$ as one-sided modules over R?
- Answer: finite Frobenius rings. And the property is if and only if.

Frobenius bimodules

- More generally, a Frobenius bimodule is a bimodule A with $A \cong \widehat{R}$ as one-sided modules. Then $\widehat{A} \cong R$ as one-sided modules.
- These isomorphisms allow one to make identifications.

Is Frobenius necessary?

- If the extension problem can always be solved, i.e., if the extrinsic and intrinsic notions of equivalence are the same, must the ring be Frobenius?
- For $A = R$, Dinh, López-Permouth, 2004, two papers prove special cases, as well as provide a strategy to prove the general case.
- For $A = R$, W., 2008, general case—yes, the ring must be Frobenius.
- For module alphabets, W., submitted, the sufficient conditions are also necessary (pseudo-injective submodule of $\widehat{R}$).

Why is Frobenius necessary?

- Dinh, López-Permouth: if R is not Frobenius, then the socle of R contains an R-submodule that is a pullback of the matrix module $M_{m,k}(\mathbb{F}_q)$ over the ring $M_m(\mathbb{F}_q)$, with $k > m$.
- W.: there exist counter-examples to the extension problem over such matrix modules that can be pulled back to give counter-examples over R itself.
- Same idea works for pseudo-injective submodules of $\widehat{R}$.

Summary

- For linear codes over finite rings, the extension problem is always solvable if and only if the ring is Frobenius.
- For linear codes over finite modules, the extension problem is always solvable if and only if the module alphabet is a pseudo-injective submodule of $\widehat{R}$.

Duality and the MacWilliams identities

- The notion of dual code becomes somewhat subtle when working with linear codes over finite rings (or modules).
- When the ground ring is Frobenius, the situation is about as good as it can get.

Features of the classical case

- $C^{\perp} \subset \mathbb{F}_q^n$.
- $C^{\perp}$ is a linear code.
- $\dim C + \dim C^{\perp} = n$; or $|C||C^{\perp}| = |\mathbb{F}_q^n|$.
- $(C^{\perp})^{\perp} = C$.
- The MacWilliams identities hold.

What happens when we use other alphabets, such as finite rings or finite modules over a finite ring?

Less structure—Additive codes

- Let G be a finite abelian group.
- An *additive code of length n over G* is a subgroup $C \subset G^n$.
- Let $\beta : G \times G \to \mathbb{Q}/\mathbb{Z}$ be a nondegenerate biadditive form, and extend β to $\beta : G^n \times G^n \to \mathbb{Q}/\mathbb{Z}$.
- For $C \subset G^n$, define

$$\begin{aligned} l(C) &= \{y \in G^n : \beta(y, x) = 0, \text{ for all } x \in C\}, \\ r(C) &= \{y \in G^n : \beta(x, y) = 0, \text{ for all } x \in C\}. \end{aligned}$$

Features of additive case

- $l(C), r(C) \subset G^n$.
- $l(C), r(C)$ are additive codes.
- $|C||l(C)| = |C||r(C)| = |G^n|$.
- $l(r(C)) = r(l(C)) = C$.
- The MacWilliams identities hold.
- If β is symmetric, then $l(C) = r(C)$. Such a β exists for any finite G.

Codes over modules

- Let R be finite ring with 1.
- Let A be a finite left R-module, B a finite right R-module, and E a finite (R, R)-bimodule.
- Let $\beta : A \times B \to E$ be a nondegenerate bilinear form. Extend to $\beta : A^n \times B^n \to E$.
- For a left linear code (submodule) $C \subset A^n$, define

$$r(C) = \{y \in B^n : \beta(x, y) = 0, \text{ for all } x \in C\}.$$

- For a right linear code (submodule) $D \subset B^n$, define

$$l(D) = \{y \in A^n : \beta(y, x) = 0, \text{ for all } x \in D\}.$$

(Questionable) Features of the module case

- $r(C) \subset B^n$; $l(D) \subset A^n$.
- $r(C)$ is a right linear code; $l(D)$ is a left linear code.
- Question: Sizes?
- $C \subset l(r(C))$; $D \subset r(l(D))$. Question: Equality of double annihilators?
- Question: MacWilliams identities?

Linear codes over rings—double annihilators

- Suppose $A = B = E = R$, with β the R-valued dot product.

Theorem (M. Hall)

There is equality of double annihilators, i.e., $l(r(C)) = C$ and $r(l(D)) = D$ for all left linear codes C and right linear codes D, if and only if the finite ring R is quasi-Frobenius.

Sizes of annihilators

Theorem

Let R be a finite quasi-Frobenius ring. Then $|C||r(C)| = |D||l(D)| = |R^n|$, for all left linear codes C and right linear codes D, if and only if R is a Frobenius ring.

- R *Frobenius* if $R/\operatorname{Rad} R \cong \operatorname{Soc} R$ as one-sided modules.

Example—matrix module

- Every non-Frobenius ring contains in its socle a matrix submodule of the form $M_{k,l}(\mathbb{F}_q)$, with $k < l$.
- Let
$$x = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & & & \\ 0 & 0 & \dots & 0 \end{pmatrix} \in M_{k,l}(\mathbb{F}_q).$$
- One can show that $|Rx||r(Rx)| < |R|$.

Case of modules—MacWilliams identities

- MacWilliams identities will hold if we can relate $\beta : A \times B \to E$ to a nondegenerate $\beta' : A \times B \to \mathbb{Q}/\mathbb{Z}$. (Which will force A and B to be isomorphic as abelian groups.)
- If $\chi : E \to \mathbb{Q}/\mathbb{Z}$ is a homomorphism, define $\beta' = \chi \circ \beta$.

Case of modules—special character

Theorem

Suppose that $\chi : E \to \mathbb{Q}/\mathbb{Z}$ *has the property that* $\ker \chi$ *contains no nonzero left or right* R*-submodules of* E*. If* $\beta : A \times B \to E$ *is nondegenerate, then so is* $\beta' = \chi \circ \beta : A \times B \to \mathbb{Q}/\mathbb{Z}$.

- β-annihilators for submodules agree with β'-annihilators.
- The MacWilliams identities hold in this situation.

Case of rings—MacWilliams identities

- Again, let $A = B = E = R$, with β equal to the R-valued dot product.

Theorem

There exists $\chi : R \to \mathbb{Q}/\mathbb{Z}$ *with the property that* $\ker \chi$ *contains no nonzero one-sided ideals of* R *if and only if* R *is a Frobenius ring. (*χ *is a generating character.)*