Dual Codes over Finite Rings—Cautions and Compromises

Jay A. Wood

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

AMS meeting, Bloomington, Indiana
April 5, 2008

Acknowledgments

Much of the material in this talk has become part of the fabric of coding theory and was developed by Delsarte, Gleason, MacWilliams, Sloane, ... Later influences include Dinh and López-Permouth; Greferath, Nechaev, and Wisbauer; Nebe, Rains, and Sloane.

The classical case—finite fields

- On $\mathbb{F}_q^n$, the standard $\mathbb{F}_q$-valued dot product is a nondegenerate, symmetric bilinear form.
- If $C \subset \mathbb{F}_q^n$ is a linear code of dimension k, then the *dual code* is

$$C^{\perp} = \{y \in \mathbb{F}_q^n : x \cdot y = 0, \text{ all } x \in C\}.$$

- We work with Hamming weights throughout.

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.

More structure—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.*

Example—Klemm

- A finite ring is *quasi-Frobenius* if it is self-injective.
- Let $R = \mathbb{F}_2[X, Y]/(X^2, XY, Y^2)$. R is not QF.
- $l(r((X))) = (X, Y)$ violates equality of double annihilators.

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.)*