Ring Involutions and Self-Dual Codes

Jay A. Wood

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

AMS meeting, Lexington, Kentucky
March 27, 2010

Acknowledgments

- Much of the material in this talk is my interpretation of work previously done by Nebe, Rains, and Sloane, *Self-Dual Codes and Invariant Theory*, Springer, 2006.
- Results to appear in special issue dedicated to Vera Pless of Int. J. of Information and Coding Theory.

Wanted: a good notion of self-dual codes over non-commutative rings

- In general, the dual code to a left linear code will be a right linear code.
- In general, left submodules are not right submodules.
- How can we get a linear code to be self-dual?
- Will "standard properties" hold?

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.

"Standard properties" in 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.

Some notation

- Finite ring R, usually non-commutative.
- Alphabet A, a finite left R-module.
- A left *linear code* over A of length n is a left R-submodule $C \subset A^n$.

MacWilliams identities—how are they proved?

- Gleason's proof uses characters and the Poisson summation formula.
- If $C \subset A^n$ is a left linear code, then its "dual" will be the character-theoretic annihilator $(\widehat{A}^n : C)$, a right submodule of the right character module $\widehat{A}^n$.
- $(\widehat{A}^n : C) = \{\pi \in \widehat{A}^n : \pi(C) = 1\}$.
- Make identifications (e.g., when $A = R$, Frobenius).

Obstacles

- We want the dual code to be a submodule of A^n, not $\widehat{A}^n$.
- In order to have self-dual codes, we need to have the dual code be a left submodule, not a right submodule.

Making identifications, I

- Left-right identifications: assume the ring R admits an anti-isomorphism.
  - *Anti-isomorphism* $\varepsilon : R \to R$, additive isomorphism, with $\varepsilon(rs) = \varepsilon(s)\varepsilon(r)$, for all $r, s \in R$.
  - *Involution*: if $\varepsilon^2 = 1$.
- Given a left R-module M, define a right R-module $\varepsilon(M)$ to be the same additive group, but with right scalar multiplication $mr := \varepsilon(r)m$, for $m \in M$, $r \in R$.

Making identifications, II

- Characters: assume the alphabet A admits an isomorphism $\psi : \varepsilon(A) \to \widehat{A}$ of right R-modules.
- Dual code: for a left linear code $C \subset A^n$, define the *dual code* $C^\perp = \varepsilon^{-1}\psi^{-1}(\widehat{A}^n : C)$.
- The dual code is now a left submodule of A^n.

Which standard properties hold?

- $C^{\perp} \subset A^n$.
- $C^{\perp}$ is a left linear code, if C is.
- $|C||C^{\perp}| = |A^n|$, from general character results.
- Double dual?—not clear. Need an extra assumption on ψ.
- MacWilliams identities hold.

Recasting in terms of biadditive form

- View characters as having values in $\mathbb{Q}/\mathbb{Z}$ ("additive form").
- Define $\beta : A^n \times A^n \to \mathbb{Q}/\mathbb{Z}$ by

$$\beta(x, y) = \sum \psi(y_i)(x_i), \quad x, y \in A^n.$$

Properties of β

- β is biadditive.
- β is non-degenerate.
- $\beta(rx, y) = \beta(x, \varepsilon(r)y)$, all $r \in R$, $x, y \in A^n$.
- (Extra) The exists unit $e \in R$ such that $\beta(x, y) = \beta(ey, x)$, all $x, y \in A^n$.
- $C^{\perp} = \{y \in A^n : \beta(C, y) = 0\}$.

An example

- G finite group. $R = F[G]$, the group algebra.
- Involution $\varepsilon(\sum a_g g) = \sum a_g g^{-1}$.
- $G = \Sigma_3$, symmetric group: $\sigma^3 = e$, $\tau^2 = e$, $\sigma\tau = \tau\sigma^2$.
- $C = R(e + \tau)(e + \sigma + \sigma^2) + R(e + \sigma + \tau\sigma + \tau\sigma^2)$ is a self-dual code of length 1 in $A = R$.

Questions

- Which finite rings admit anti-isomorphisms?
- Which finite modules admit isomorphisms $\psi : \varepsilon(A) \to \widehat{A}$?
- Are there interesting examples?
- Some partial results in paper in Pless issue.
- Some examples from algebraic topology: cohomology as modules over the Steenrod algebra.