Two Fundamental Theorems of MacWilliams: MacWilliams Identities over Finite Rings

Jay A. Wood

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

Huazhong Normal University, Wuhan, Hubei
June 28, 2011

Wanted: MacWilliams Identities in the Context of Linear Codes Defined over Finite Rings

- Review what is known over finite fields.
- Linear codes over finite rings.
- What can be proved without restrictions.
- What can go wrong.
- Frobenius rings as a way to make identifications.
- Self-dual codes in the non-commutative setting.

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, 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

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

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

Some Notation

- Finite ring R, with 1, possibly non-commutative.
- A left *linear code* over R of length n is a left R-submodule $C \subset R^n$.
- Hamming weight is defined as for fields: count the number of nonzero entries in an element of R^n.
- If M is a finite left R-module, then the character group $\widehat{M}$ is a right R-module (*character module*):

$$(\pi r)(m) := \pi(rm), \quad \pi \in \widehat{M}, r \in R, m \in M.$$

MacWilliams Identities—How Are They Proved?

- Gleason's proof uses characters and the Poisson summation formula:

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

- If $C \subset R^n$ is a left linear code, then its "dual" will be the character-theoretic annihilator $(\widehat{R}^n : C)$, a right submodule of the right character module $\widehat{R}^n$.
- $(\widehat{R}^n : C) = \{\pi \in \widehat{R}^n : \pi(C) = 1\}$.

"Standard Properties" Using Characters

1. $(\widehat{R}^n : C) \subset \widehat{R}^n$.
2. $(\widehat{R}^n : C)$ is a right R-submodule.
3. $|C||(\widehat{R}^n : C)| = |\widehat{R}^n| = |R^n|$.
4. $(R^n : ((\widehat{R}^n : C)) = C$.
5. The MacWilliams identities hold:

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

Some Obstacles

- We want the dual code to be a submodule of R^n, not $\widehat{R}^n$. (Next topic, after an interlude.)
- In order to have self-dual codes, we need to have the dual code be a left submodule, not a right submodule. (Later.)

Interlude: Why Not Just Use the Dot Product?

- Dot product on R^n (all operations in R):

$$x \cdot y = \sum x_i y_i,$$

  for $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in R^n$.
- Non-degenerate, but not usually symmetric when R is non-commutative.
- Two annihilators of left submodule $C \subset R^n$:
  - $l(C) = \{y \in R^n : y \cdot x = 0, x \in C\}$ (left)
  - $r(C) = \{y \in R^n : x \cdot y = 0, x \in C\}$ (right)

Interlude: Problems

- Always have $C \subset I(r(C))$ and $D \subset r(I(D))$.
- Equality may not hold, even when R is commutative.
- Equality always holding is equivalent to R being quasi-Frobenius (QF).
- QF is also equivalent to R being self-injective (injective as a module over itself).

Interlude: More Problems

- Even when R is QF, one may not have $|C||r(C)|$ equal to $|R^n|$.
- Which would mean that the MacWilliams identities also fail: just set $X = Y = 1$.
- Need R to be Frobenius.
- End of interlude.

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) *socle* $\mathrm{Soc}(R)$ of R is the ideal of R generated by all the simple left ideals of R.
- R is *Frobenius* if $R/\mathrm{Rad}(R) \cong \mathrm{Soc}(R)$ as one-sided modules.

Two Useful Theorems About Finite Frobenius Rings

- (Honold, 2001) $R/\operatorname{Rad}(R) \cong \operatorname{Soc}(R)$ as left modules iff $R/\operatorname{Rad}(R) \cong \operatorname{Soc}(R)$ 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*.

Examples of Finite Frobenius Rings

- Finite fields $\mathbb{F}_q$: $\pi(x) = \exp(2\pi i \,\mathrm{Tr}(x)/p)$.
- $\mathbb{Z}/n\mathbb{Z}$: $\pi(x) = \exp(2\pi i x/n)$.
- 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).

Identifying $\widehat{R}^n$ with R^n (a)

- "Dual" of $C \subset R^n$ was $(\widehat{R}^n : C) \subset \widehat{R}^n$.
- Use R Frobenius to make identifications.
- Compose the dot product with a generating character π of R:

$$R^n \times R^n \xrightarrow{\cdot} R \xrightarrow{\pi} \mathbb{C}.$$

Identifying $\widehat{R}^n$ with R^n (b)

- The pairing is non-degenerate:

$$R^n \times R^n \xrightarrow{\cdot} R \xrightarrow{\pi} \mathbb{C}.$$

- Suppose $\pi(x \cdot R^n) = 1$. Then $x \cdot R^n$ is a right ideal contained in $\ker(\pi)$.
- But π is a generating character, so $x \cdot R^n = 0$.
- The dot product is non-degenerate, so $x = 0$.

Identifying $\widehat{R}^n$ with R^n (c)

- The non-degenerate pairing

$$R^n \times R^n \xrightarrow{\cdot} R \xrightarrow{\pi} \mathbb{C}$$

  defines two isomorphisms of R^n with $\widehat{R}^n$.
- When C is a left linear code, $r(C)$ equals the pullback of $(\widehat{R}^n : C)$ under one of these isomorphisms.

MacWilliams Identities over Finite Frobenius Rings

- For a left linear code $C \subset R^n$, R Frobenius:
- $r(C) \subset R^n$.
- $r(C)$ is a right R-submodule.
- $|C||r(C)| = |R^n|$.
- $l(r(C)) = C$.
- The MacWilliams identities hold:

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

Generalizations to Linear Codes Defined over Finite Modules

- Use an alphabet different from the ring itself.
- Let R be a finite ring with 1 (no extra assumptions).
- Let A be a finite left R-module (the *alphabet*).
- An *R-linear code over A of length n* is a left R-submodule $C \subset A^n$.

MacWilliams Identities over Finite Modules

- For a left R-linear code $C \subset A^n$:
- $(\widehat{A}^n : C) \subset \widehat{A}^n$.
- $(\widehat{A}^n : C)$ is a right R-submodule of $\widehat{A}^n$.
- $|C||(\widehat{A}^n : C)| = |A^n|$.
- $(A^n : (\widehat{A}^n : C)) = C$.
- The MacWilliams identities hold:

$$W_{(\widehat{A}^n:C)}(X, Y) = \frac{1}{|C|} W_C(X + (|A| - 1)Y, X - Y).$$

Self-Dual Codes in the Non-Commutative Setting

- We have seen that for a left linear code $C \subset R^n$, R Frobenius, the right linear code $r(C)$ is the proper choice for the dual code to C.
- There is no guarantee that a right code will also be a left code.
- The same for $C \subset A^n$ and $(\widehat{A}^n : C) \subset \widehat{A}^n$.
- How to make sense of self-duality?
- Follow ideas of Nebe, Rains, and Sloane.

Making Identifications (a)

- 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 (b)

- Characters: assume the alphabet A admits an isomorphism $\psi : \varepsilon(A) \longrightarrow \widehat{A}$ of right R-modules. (If $A = R$, this happens iff R is Frobenius.)
- 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?

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

$$W_{C^{\perp}}(X, Y) = \frac{1}{|C|} W_C(X + (|A| - 1)Y, X - Y).$$

Recasting in Terms of Biadditive Form

- View characters as having values in $\mathbb{Q}/\mathbb{Z}$ ("additive form"). Use $\exp(2\pi i(-))$ to get values in $\mathbb{C}^\times$.
- 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) There exists a unit $e \in R$ such that $\beta(x, y) = \beta(ey, x)$, all $x, y \in A^n$.
- $C^{\perp} = \{y \in A^n : \beta(C, y) = 0\}$.
- Then all the standard properties will hold.

An Example: Group Algebras

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

Another Example: Subalgebras of the Steenrod Algebra

- The Steenrod algebra is an (infinite) Frobenius $\mathbb{F}_p$-algebra that arises in algebraic topology. The $\mathbb{F}_p$-cohomology of any CW-complex is a module over the Steenrod algebra.
- For finite examples, use some subHopf algebras. For example, when $p = 2$, use $\mathcal{A}(1)$, the subalgebra generated by 1, Sq^1, and Sq^2.
- Then $A = H^*(\mathbb{R}P^{4k+3}; \mathbb{F}_2)$ admits an appropriate ψ.

Questions

- Which finite rings admit anti-isomorphisms?
- Which finite modules admit isomorphisms $\psi : \varepsilon(A) \to \widehat{A}$?
- Are there interesting examples of self-dual codes?
- I have some partial results (2010), but the area is wide open.