The MacWilliams Identities

Jay A. Wood

Western Michigan University

Colloquium

March 1, 2012

The Coding Problem

- How to ensure the integrity of a message transmitted over a noisy channel?
- Cleverly add redundancy.
- Encode possible messages (information) as a string of elements in an alphabet.
- Transmit the string over the channel.
- Detect errors and decode.

Adding Algebraic Structure

- Assume the alphabet is a finite field $\mathbb{F}$.
- Assume the set of messages M is a finite dimensional vector space over F of dimension k.
- The encoding is a linear embedding $M \hookrightarrow \mathbb{F}^n$, for some n.
- The image is a linear code of *length* n.

Example: Hamming Code

- Alphabet is $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$.
- Let $E_7 \subset \mathbb{F}_2^7$ be spanned by the rows of

$$\begin{matrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{matrix}$$

- Messages M form a vector space of dimension 4 over $\mathbb{F}_2$, and E_7 corrects one error.

Hamming Code, Continued

- $x \in E_7$ if and only if $Hx^T = 0$, where

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

- If there is one error in x, then $Hx^T \neq 0$ and Hx^T gives the binary representation of the position where the error occurs.
- H is the generator matrix for the dual code $E_7^{\perp}$.

Objectives for this Talk

- Some of the language of algebraic coding theory.
- Basic properties of dual codes, including the MacWilliams identities.
- The MacWilliams identities and their proof.
- Generalizations over finite rings.

Definitions (a)

- Let $\mathbb{F}_q$ be a finite field, q a prime power. For example, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, the integers modulo a prime p. The case $p = 2$ is especially important.
- A *linear code* of length n is a vector subspace $C \subset \mathbb{F}_q^n$.
- Can generalize to left submodules $C \subset R^n$, for a finite ring R with 1. Or even $C \subset A^n$, for a finite left module A over R.

Definitions (b)

- For $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$, the *Hamming weight* $\mathrm{wt}(x)$ equals the number of nonzero entries of x.
- For a linear code $C \subset \mathbb{F}_q^n$, the *Hamming weight enumerator* is the polynomial

$$W_C(X, Y) = \sum_{x \in C} X^{n - \mathrm{wt}(x)} Y^{\mathrm{wt}(x)}.$$

- An estimate of the error-correcting capability of the code C is given by the *minimum weight* $d_C = \min\{\mathrm{wt}(x) : x \in C, x \neq 0\}$. ($d_{E_7} = 3$.)

Definitions (c)

- Define a *dot product* on $\mathbb{F}_q^n$ by

$$x \cdot y = \sum_{i=1}^{n} x_i y_i,$$

for $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$.

- For a linear code $C \subset \mathbb{F}^n$, define the *dual code* $C^\perp$ (also denoted $r(C)$, the *right annihilator*) by

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

"Standard Properties" of Dual Codes

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:

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

Proofs

- The first four items are obvious or follow from basic linear algebra of nondegenerate forms over fields.
- The proof of the MacWilliams identities given will be based on character theory and the Poisson summation formula.
- The proof is due to Gleason.

Florence Jessie MacWilliams

- 1917–1990
- Worked for many years at Bell Labs.
- 1962 doctoral dissertation under Andrew Gleason at Harvard. (Mackey, Stone, Ge. Birkhoff, EH Moore.)
- "Combinatorial Problems of Elementary Abelian Groups"
- The second section is the MacWilliams identities.

An Eye Towards Generalizations

- When $\mathbb{F}_q$ is replaced by a finite ring R, do the "standard properties," including the MacWilliams identities, still hold?
- For the double dual, need R to be quasi-Frobenius. For the size condition and the MacWilliams identities, need R to be Frobenius.
- Why Frobenius?
- There is a character-theoretic proof over $\mathbb{F}$ 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

- Let $(G, +)$ be a finite abelian group.
- A *character* π of G is a group homomorphism $\pi : (G, +) \to (\mathbb{C}^\times, \times)$, the nonzero complexes.
- The set $\widehat{G}$ of all characters of G is itself a finite abelian group called the *character group*.
- $|\widehat{G}| = |G|$.
- If M is a finite left R-module, then $\widehat{M}$ is a right R-module. (Thus, $\widehat{\mathbb{F}} \cong \mathbb{F}$, as vector spaces.)

Two Useful Formulas

$$\sum_{x \in G} \pi(x) = \begin{cases} |G|, & \pi = 1, \\ 0, & \pi \neq 1. \end{cases}$$

$$\sum_{\pi \in \widehat{G}} \pi(x) = \begin{cases} |G|, & x = 0, \\ 0, & x \neq 0. \end{cases}$$

Frobenius Rings

- 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

- Finite ring R with 1.
- (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 ρ of R such that $\ker \rho$ contains no nonzero left (right) ideal of R. This ρ is a *generating character*.

Examples of Finite Frobenius Rings

- Finite fields $\mathbb{F}_q$: $\chi(x) = \exp(2\pi i \operatorname{Tr}_{q,p}(x)/p)$.
- $\mathbb{Z}/n\mathbb{Z}$: $\chi(x) = \exp(2\pi i x/n)$.
- Galois rings (Galois extensions of $\mathbb{Z}/p^m\mathbb{Z}$). $\operatorname{Soc}(R) \cong \mathbb{F}_{p^m}$; use χ for $\mathbb{F}_{p^m}$ and extend.
- Finite chain rings (all ideals form a chain). Extend from $\operatorname{Soc}(R) \cong \mathbb{F}_q$.
- Products of Frobenius rings. Use product of the generating characters.
- Matrix rings over a Frobenius ring: $M_n(R)$. $\chi = \chi_R \circ \operatorname{Tr}$.
- Finite group rings over a Frobenius ring: $R[G]$. $\chi(\sum a_g g) = \chi_R(a_e)$, e is identity element.

Fourier Transform

- Given a function $f : G \longrightarrow V$, with V a complex vector space, its *Fourier transform* is a function $\hat{f} : \widehat{G} \longrightarrow V$ defined by

$$\hat{f}(\pi) = \sum_{x \in G} \pi(x) f(x), \quad \pi \in \widehat{G}.$$

- Fourier inversion:

$$f(x) = \frac{1}{|G|} \sum_{\pi \in \widehat{G}} \pi(-x) \hat{f}(\pi), \quad x \in G.$$

Poisson Summation Formula

- For a subgroup $H \subset G$, define its *annihilator* $(\widehat{G} : H) = \{\pi \in \widehat{G} : \pi(H) = 1\}$.
- $|(\widehat{G} : H)| = |G|/|H|$.
- For a subgroup $H \subset G$ and any $a \in G$,

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

- In particular, for a subgroup $H \subset G$,

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

MacWilliams Identities over Finite Frobenius Rings

Theorem (1999)

Let R be a finite Frobenius ring. If $C \subset R^n$ is a left linear code, then the MacWilliams identities hold:

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

Proof of the MacWilliams Identities (a)

- The proof follows a proof due to Gleason (1970).
- Let R be Frobenius with generating character ρ.
- Let $G = R^n$, an abelian group under addition.
- Let $H = C$, a left linear code.
- Let $V = \mathbb{C}[X, Y]$, a complex vector space.
- Let $f : G \longrightarrow V$ be

$$f(x) = X^{n-\mathrm{wt}(x)} Y^{\mathrm{wt}(x)}.$$

Proof of the MacWilliams Identities (b)

- By Frobenius hypothesis, every character of $G = R^n$ has the form π_a, for some $a \in R^n$, with

$$\pi_a(x) = \rho(x \cdot a), \quad x \in R^n.$$

- $\pi_a \in (\widehat{G} : H)$ if and only if $a \in r(C)$.
- $|(\widehat{G} : H)| = |r(C)|$.

Proof of the MacWilliams Identities (c)

- For $f(x) = X^{n-\mathrm{wt}(x)} Y^{\mathrm{wt}(x)}$,

$$\hat{f}(\pi_a) = (X + (|R| - 1)Y)^{n-\mathrm{wt}(a)}(X - Y)^{\mathrm{wt}(a)}.$$

- This requires some manipulations and use of $\sum \pi(x)$ formulas. (Next slide.)
- Recognize $\hat{f}(\pi_a)$ as summand of $W_{r(C)}(X + (|R| - 1)Y, X - Y)$.

Idea of Manipulation

- Let $n = 1$, $f(x) = X^{1-\mathrm{wt}(x)} Y^{\mathrm{wt}(x)}$.

$$\begin{aligned}
\hat{f}(\pi_a) &= \sum_{x \in R} \pi_a(x) X^{1-\mathrm{wt}(x)} Y^{\mathrm{wt}(x)} \\
&= X + \sum_{x \neq 0} \pi_a(x) Y \\
&= \begin{cases} X + (|R| - 1)Y, & a = 0, \\ X - Y, & a \neq 0, \end{cases} \\
&= (X + (|R| - 1)Y)^{1-\mathrm{wt}(a)} (X - Y)^{\mathrm{wt}(a)}
\end{aligned}$$

Example, $n = 2$

- Let $C_2 \subset \mathbb{F}_2^2$ be

$$C_2 = \{00, 11\}.$$

- C_2 is *self-dual*; i.e., $C_2^{\perp} = C_2$.
- $W_{C_2}(X, Y) = X^2 + Y^2$. Call this S.
- In a binary self-dual code, all elements have even weight.

Example, $n = 8$

- Let $E_8 \subset \mathbb{F}_2^8$ be spanned by the rows of

$$\begin{array}{cccccccc} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{array}$$

- E_8 is self-dual. Also, all elements x of E_8 satisfy $\mathrm{wt}(x) \equiv 0 \bmod 4$. E_8 is *doubly-even*.
- $W_{E_8}(X, Y) = X^8 + 14X^4Y^4 + Y^8$. Call this T.

Extended Golay Code (1949)

- There is a famous binary code G_{24} of length 24, dimension 12, which is self-dual, doubly-even, with minimum weight 8.
- Weight enumerator:

$$W_{G_{24}}(X, Y) = X^{24} + 759X^{16}Y^8 + 2576X^{12}Y^{12} + 759X^8Y^{16} + Y^{24}.$$

Gleason's Theorem (1970)

- The weight enumerator of any binary self-dual code is a polynomial expression in the weight enumerators S and T of C_2 and E_8.
- $W_{G_{24}}(X, Y) = T^3 + \frac{21}{8}(2S^8T - S^4T^2 - S^{12})$.
- The weight enumerator of any binary self-dual, doubly-even code is a polynomial expression in the weight enumerators of E_8 and G_{24}. So, $n \equiv 0 \bmod 8$.
- Greatly generalized by Nebe, Rains, and Sloane in 2006.

Self-Dual Codes in the Non-Commutative Setting

- 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.

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?
- There are some partial results (2010), but the area is wide open.