Ring involutions and self-dual codes

Jay A. Wood

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

Algebra for Secure and Reliable Communications Modeling
Morelia, Michoacán, Mexico
October 9, 2012

MacWilliams identities

- For a left linear code $C \subset R^n$, where R is a finite Frobenius ring, the MacWilliams identities hold for the Hamming weight:

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

- Remember that $r(C) = \{b \in R^n : c \cdot b = 0, c \in C\}$.
- Also a version using $l(C)$ instead.

Case of finite fields

- When R is a finite field (or a commutative Frobenius ring, more generally), we do not need to distinguish between $r(C)$ and $l(C)$. We instead use the customary $C^{\perp}$.
- $|C||C^{\perp}| = |R^n|$, for R Frobenius.

Self-dual codes

- Assume R is a finite field (or a finite commutative Frobenius ring, more generally).
- A linear code $C \subset R^n$ is *self-orthogonal* if $C \subset C^\perp$.
- A linear code $C \subset R^n$ is *self-dual* if $C = C^\perp$.
- Since $|C||C^\perp| = |R^n|$, a self-dual code must satisfy $|C| = |R|^{n/2}$. (For fields, $\dim C = n/2$.)
- If $|R|$ is not a square, then a self-dual code must have even length. (For fields, also even length.)

MacWilliams identities for self-dual codes

- When $C \subset R^n$ is self-dual, the MacWilliams identities become

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

- W_C appears on both sides of the equation, so that W_C is invariant under a group action.
- More on this in a few moments.

Some examples over $\mathbb{F}_2$

- Because $c \cdot c \equiv \mathrm{wt}(c) \bmod 2$, all codewords of a binary self-dual code have even weight.
- A binary self-dual code is *doubly-even*, if all codewords have weight divisible by 4.
- $n = 2$, $C_2 = \{00, 11\}$.
  $W_2 := W_{C_2}(X, Y) = X^2 + Y^2$.
- $n = 8$, E_8 generated by

$$\begin{pmatrix} 11110000 \\ 00111100 \\ 00001111 \\ 10101010 \end{pmatrix}.$$

$W_8 := W_{E_8}(X, Y) = X^8 + 14X^4Y^4 + Y^8$.

Binary extended Golay code

- The famous extended Golay code G_{24} is a doubly-even self-dual code of length $n = 24$.
- $W_{G_{24}}(X, Y) = X^{24} + 759X^{16}Y^8 + 2576X^{12}Y^{12} + 759X^8Y^{16} + Y^{24}$
- The Golay code has minimum weight 8.

Substitution

- An invertible 2×2 matrix S acts on polynomials $f(X, Y) \in \mathbb{C}[X, Y]$ by substitution:

$$f^S(X, Y) := f((X, Y)S).$$

- For example, let

$$S = \frac{1}{\sqrt{|R|}} \begin{pmatrix} 1 & 1 \\ |R| - 1 & -1 \end{pmatrix}.$$

Invariance of W_C

- If $f \in \mathbb{C}[X, Y]$ is homogeneous of degree n, then

$$f^S(X, Y) = \frac{1}{|R|^{n/2}} f(X + (|R| - 1)Y, X - Y).$$

- If $f = W_C$ for a self-dual code, then the MacWilliams identities imply that $f^S = f$.

Binary examples

- A binary self-dual code (all weights even) will also be invariant under

$$D_1 := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

- A binary doubly-even self-dual code (all weights divisible by 4) will be invariant under

$$D_2 := \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{-1} \end{pmatrix}.$$

Gleason's theorem, 1970

- Let $\mathcal{G}_1$ be the group generated by S and D_1; let $\mathcal{G}_2$ be generated by S and D_2.
- W_C is invariant under $\mathcal{G}_1$, if C is binary self-dual; and under $\mathcal{G}_2$, if C is binary doubly-even self-dual.
- Let $\mathbb{C}[X,Y]^{\mathcal{G}} := \{f : f^P = f, P \in \mathcal{G}\}$.

Theorem

$\mathbb{C}[X,Y]^{\mathcal{G}_1} = \mathbb{C}[W_{C_2}, W_{E_8}]$; $\mathbb{C}[X,Y]^{\mathcal{G}_2} = \mathbb{C}[W_{E_8}, W_{G_{24}}]$.

- $W_{G_{24}}(X,Y) = W_8^3 + \frac{21}{8}(2W_2^8 W_8 - W_2^4 W_8^2 - W_2^{12})$.

Work of Nebe-Rains-Sloane

- Gleason's theorem was generalized greatly by Nebe-Rains-Sloane, 2006.
- Their work also applies over noncommutative rings.
- What are some of the obstacles they needed to overcome in order to study self-dual codes over noncommutative rings?
- We begin by recalling what happens over finite fields.

"Standard properties" of dual codes

- $C^\perp \subset \mathbb{F}_q^n$.
- $C^\perp$ 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:

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

"Standard properties" for additive codes

- Assume $C \subset A^n$ is an additive code.
- $(\widehat{A}^n : C) \subset \widehat{A}^n$.
- $(\widehat{A}^n : C)$ is an additive code.
- $|C||(\widehat{A}^n : C)| = |A^n|$.
- $(A^n : (\widehat{A}^n : C)) = C$.
- MacWilliams identities hold:

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

"Standard properties" for linear codes over modules

- Now assume R is a finite ring with 1, A is a finite left R-module, and $C \subset A^n$ is a left R-linear code.
- $(\widehat{A}^n : C) \subset \widehat{A}^n$.
- $(\widehat{A}^n : C)$ is a right R-linear code.
- $|C||(\widehat{A}^n : C)| = |A^n|$.
- $(A^n : (\widehat{A}^n : C)) = C$.
- MacWilliams identities hold:

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

Problems with self-duality

- We need to use the character-theoretic annihilator $(\widehat{A}^n : C)$ in order for the MacWilliams identities to hold.
- But $(\widehat{A}^n : C)$ lives in $\widehat{A}^n$, not in A^n.
- But $(\widehat{A}^n : C)$ is right linear when C is left linear.
- How can we legitimately have $C = (\widehat{A}^n : C)$, in order to have a self-dual code?
- Even if $A = R$ is a Frobenius ring, the left/right problem remains.

Approach of Nebe-Rains-Sloane

- Work in the context of R-linear codes with alphabet A, a finite left R-module.
- Suppose R admits an anti-isomorphism ε, which will allow us to turn a left R-module M into a right R-module $\varepsilon(M)$.
- Suppose there is an isomorphism $\widehat{A} \cong \varepsilon(A)$, which will allow us to treat the annihilator $(\widehat{A}^n : C)$ as a submodule of A^n.
- Plus one more technical condition (suppressed).

Anti-isomorphisms

- Let R be any finite ring with 1.
- A map $\varepsilon : R \longrightarrow R$ is an *anti-isomorphism* is ε is an additive isomorphism and $\varepsilon(rs) = \varepsilon(s)\varepsilon(r)$ for all $r, s \in R$.
- An anti-isomorphism ε is an *involution* if $\varepsilon^2 = 1$.
- If M is a left R-module, define $\varepsilon(M)$ to be the same additive group as M, equipped with the right R-module structure $mr := \varepsilon(r)m$, for $m \in M$, $r \in R$; $\varepsilon(M)$ is a right R-module. (And vice versa.)

Examples

- Commutative rings: use $\varepsilon = 1$.
- $M_n(\mathbb{F}_q)$: use $\varepsilon = \mathrm{Tr}$, the matrix transpose.
- If R has anti-isomorphism ϵ, then $M_n(R)$ has anti-isomorphism $\varepsilon = \mathrm{Tr} \circ \epsilon$.
- For a finite group G and R with ϵ, the group ring $R[G]$ has $\varepsilon(\sum a_g g) = \sum \epsilon(a_g) g^{-1}$.
- The upper-triangular matrices $U_n(\mathbb{F}_q)$ over $\mathbb{F}_q$ (not Frobenius) admit an involution (exercise).

Questions

- When does a finite ring admit an anti-isomorphism? an involution?
- Which Frobenius rings admit anti-isomorphisms?
- Are there large classes of examples?

Identifications

- Suppose the ring R admits an anti-isomorphism ε.
- Characters: assume A admits an isomorphism $\psi : \varepsilon(A) \to \widehat{A}$ of right R-modules.
- If $A = R$, this happens if and only if 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.

Self-dual codes

- The dual code $C^{\perp}$ satisfies all the standard properties.
- A left linear code $C \subset A^n$ is *self-dual* if $C = C^{\perp}$.
- (Nebe-Rains-Sloane) Every "type" of self-dual code defines an invariance group $\mathcal{G}$ for the complete weight enumerators of self-dual codes of that type.
- (NRS) The space of all $\mathcal{G}$-invariant polynomials is spanned by the complete weight enumerators of self-dual codes of that type, generalizing Gleason.

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 (a)

- Define $\mathcal{A}(1)$ to be the algebra over $\mathbb{F}_2$ generated by 1, s_1, s_2, subject to $s_1^2 = 0$ and $s_2^2 = s_1 s_2 s_1$.
- $\mathcal{A}(1)$ has dimension 8 as an $\mathbb{F}_2$-vector space, with basis $1, s_1, s_2, s_1 s_2, s_2 s_1, s_2^2 (= s_1 s_2 s_1), s_2 s_1 s_2, s_2^3$.
- Involution determined by $\varepsilon(s_1) = s_1$ and $\varepsilon(s_2) = s_2$. Then $\varepsilon(s_1 s_2) = s_2 s_1$, and $\varepsilon(s_2 s_1) = s_1 s_2$.
- $\mathcal{A}(1)$ is Frobenius.

Another example (b)

- Let $A_n = \mathbb{F}_2[X]/(X^{n+1})$ be a truncated polynomial algebra over $\mathbb{F}_2$; $\dim A_n = n + 1$.
- A_n is a left $\mathcal{A}(1)$-module (coefficients in $\mathbb{F}_2$, remember) via:

$$s_1 X^j = \begin{cases} j\, X^{j+1}, & j+1 \leq n, \\ 0, & j+1 > n; \end{cases}$$

$$s_2 X^j = \begin{cases} j(j-1)/2\, X^{j+2}, & j+2 \leq n, \\ 0, & j+2 > n. \end{cases}$$

Another example (c)

- It turns out that A_n admits an isomorphism $\psi : \varepsilon(A_n) \to \widehat{A}_n$ iff $n = 4k + 3$.
- For $n = 7$, the subspace spanned by $\{X^4, X^5, X^6, X^7\}$ inside A_7 is a left $\mathcal{A}(1)$-submodule and a self-dual code (of length 1).

Huh?

- $\mathcal{A}(1)$ is a subalgebra of the mod 2 Steenrod algebra from algebraic topology.
- The ring A_n is $H^*(\mathbb{R}P^n; \mathbb{F}_2)$, the mod 2 cohomology of real projective n-space.
- Are there other interesting examples?