Characters and the MacWilliams identities

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 8, 2012

Characters

- Let G be a finite abelian group (usually additive).
- A *character* of G is a group homomorphism $\pi : G \to \mathbb{C}^\times$, where $\mathbb{C}^\times$ is the multiplicative group of nonzero complex numbers.
- Example. Let $G = \mathbb{Z}/m\mathbb{Z}$ and let $a \in \mathbb{Z}/m\mathbb{Z}$. Then $\pi_a : \mathbb{Z}/m\mathbb{Z} \to \mathbb{C}^\times$, $\pi_a(g) = \exp(2\pi iag/m)$ is a character. Every character of $\mathbb{Z}/m\mathbb{Z}$ is of this form.

Character group

- Let $\widehat{G}$ be the set of all characters of G.
- Then $\widehat{G}$ is itself a finite abelian group under pointwise multiplication of characters. That is, $(\pi_1\pi_2)(g) := \pi_1(g)\pi_2(g)$ for $g \in G$.
- $\widehat{G}$ is the *character group* of G.
- $|\widehat{G}| = |G|$; in fact, $\widehat{G} \cong G$ (but not naturally).
- $\widehat{\widehat{G}} \cong G$, naturally: $g \mapsto [\pi \mapsto \pi(g)]$.

Products

- If G_1 and G_2 are two finite abelian groups, then $(G_1 \times G_2)\widehat{\ } \cong \widehat{G_1} \times \widehat{G_2}$.
- $(\pi_1, \pi_2)(g_1, g_2) := \pi_1(g_1)\pi_2(g_2)$.

Vanishing formulas

- The character sending every $g \in G$ to $1 \in \mathbb{C}^\times$ is written 1, the *principal character*.

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

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

Linear independence of characters

- Let $F(G, \mathbb{C}) = \{f : G \to \mathbb{C}\}$ be the set of all functions from G to $\mathbb{C}$.
- $F(G, \mathbb{C})$ is a vector space over $\mathbb{C}$ of dimension $|G|$.
- The characters of G are linearly independent in $F(G, \mathbb{C})$; in fact, they form a basis.
- The characters are orthonormal under

$$\langle f_1, f_2 \rangle = \frac{1}{|G|} \sum_{g \in G} f_1(g) \overline{f_2(g)}.$$

Fourier transform

- Let V be a complex vector space.
- The *Fourier transform* $\widehat{\ } : F(G, V) \to F(\widehat{G}, V)$ is a linear transformation defined for $f \in F(G, V)$ by:

$$\hat{f}(\pi) := \sum_{g \in G} \pi(g) f(g).$$

- *Fourier inversion*: $\widehat{\ }$ is invertible

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

Annihilators

- For H a subgroup of G, define the *annihilator*

$$(\widehat{G} : H) := \{\pi \in \widehat{G} : \pi(H) = 1\}.$$

- $(\widehat{G} : H)$ is a subgroup of $\widehat{G}$.
- $(\widehat{G} : H) \cong (G/H)\widehat{\ }$, so $|(\widehat{G} : H)| = |G|/|H|$.
- $0 \to H \to G \to G/H \to 0$ induces
  $1 \to (\widehat{G} : H) \to \widehat{G} \to \widehat{H} \to 1$.
- Double annihilator: $(G : (\widehat{G} : H)) = H$.

Poisson summation formula

- For H a subgroup of G and $f : G \to V$,

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

Additive codes

- Let the alphabet A be a finite abelian group.
- An *additive code* of length n over A is a subgroup $C \subset A^n$.
- The *Hamming weight* $\mathrm{wt}(a) = 1$ for $a \neq 0$ in A.
- Extend to vectors $a \in A^n$ by $\mathrm{wt}(a) = \sum \mathrm{wt}(a_i)$.

Hamming weight enumerator

- For an additive code $C \subset A^n$, the *Hamming weight enumerator* is the generating function

$$W_C(X,Y) := \sum_{c \in C} X^{n-\mathrm{wt}(c)} Y^{\mathrm{wt}(c)} = \sum_{i=0}^{n} A_i X^{n-i} Y^i,$$

where A_i equals the number of codewords in C of Hamming weight i.

The MacWilliams identities

Theorem

For an additive code $C \subset A^n$, with annihilator $(\widehat{A}^n : C)$,

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

- Because $|\widehat{A}| = |A|$ and $(A^n : (\widehat{A}^n : C)) = C$, roles of C and $(\widehat{A}^n : C)$ can be reversed.
- This version is due to Delsarte, 1972.

Strategy of proof

- The idea of the proof is due to Gleason.
- Apply the Poisson summation formula

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

with $G = A^n$, $H = C$, $(\widehat{G} : H) = (\widehat{A}^n : C)$, and $f(h) = X^{n - \mathrm{wt}(c)} Y^{\mathrm{wt}(c)}$.

Form of $\hat{f}$, $n = 1$

- For $f(c) = X^{n-\mathrm{wt}(c)} Y^{\mathrm{wt}(c)}$, what is $\hat{f}$? Case $n = 1$:

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

Form of $\hat{f}$, general n

- For general n, we take the product of 1-dimensional results.
- For $\pi = (\pi_1, \pi_2, \ldots, \pi_n) \in \widehat{A}^n$,

$$\begin{aligned}\hat{f}(\pi) &= \hat{f}(\pi_1)\hat{f}(\pi_2)\cdots\hat{f}(\pi_n) \\ &= (X + (|A| - 1)Y)^{n-\mathrm{wt}(\pi)}(X - Y)^{\mathrm{wt}(\pi)}.\end{aligned}$$

- Here, $\mathrm{wt}(\pi)$ counts the number of $\pi_i \neq 1$.

Comments

- The format of the MacWilliams identities for additive codes was

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

- Can we identify $(\widehat{A}^n : C)$ with a subgroup of A^n? In a natural way?
- What about additional structure: if A is a field, a ring, or a module?

Finite fields (a)

- Prime fields: for $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$, then $\theta_p(a) = \exp(2\pi i a/p)$ is a character of $\mathbb{F}_p$.
- Every character of $\mathbb{F}_p$ is of the form $a \mapsto \theta_p(ba)$, for some $b \in \mathbb{F}_p$.
- In general, consider $\mathbb{F}_q$, $q = p^\ell$, with trace function $\mathrm{Tr}_{q/p} : \mathbb{F}_q \longrightarrow \mathbb{F}_p$, $\mathrm{Tr}_{q/p}(a) = a + a^p + a^{p^2} + \cdots + a^{p^{\ell-1}}$. Define $\theta_q = \theta_p \circ \mathrm{Tr}_{q/p}$, a character of $\mathbb{F}_q$.
- Every character of $\mathbb{F}_q$ is of the form $a \mapsto \theta_q(ba)$, for some $b \in \mathbb{F}_q$.

Finite fields (b)

- $\widehat{\mathbb{F}_q} \cong \mathbb{F}_q$ as vector spaces, and $\widehat{\mathbb{F}_q^n} \cong \mathbb{F}_q^n$ as vector spaces: $y \in \mathbb{F}_q^n \mapsto (a \mapsto \theta_q(a \cdot y))$, where $\cdot$ is the dot product on $\mathbb{F}_q^n$.
- Under this isomorphism, $(\widehat{\mathbb{F}_q^n} : C)$ corresponds to

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

MacWilliams identities for finite fields

- This leads to the original version of the MacWilliams identities, due to MacWilliams, 1961–1962, for $A = \mathbb{F}_q$:

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

Finite rings

- Suppose $A = R$, a finite ring. The same identifications that worked for finite fields will work here, provided $\widehat{R} \cong R$ as one-sided R-modules.
- Then $\widehat{R}^n \cong R^n$, and $(\widehat{R}^n : C)$ can be identified with

$$l(C) := \{b \in R^n : b \cdot c = 0, c \in C\},$$
$$r(C) := \{b \in R^n : c \cdot b = 0, c \in C\}.$$

MacWilliams identities for finite rings

- Assume R is a finite ring satisfying $\widehat{R} \cong R$ as one-sided R-modules. Then:

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

- Similarly for $r(C)$ in place of $l(C)$.
- In the next lecture we discuss rings satisfying $\widehat{R} \cong R$: the finite Frobenius rings.