The MacWilliams Identities

Jay A. Wood

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

Huangshi Institute of Technology
Huangshi, Hubei
June 24, 2011

Acknowledgments

- I am pleased to be visiting the city of Huangshi, and I thank my host, Professor Xiusheng Liu, for the invitation and for his hospitality.

Error-Correcting Codes

- If one tries to send data (a "message") over a noisy channel (copper wires, fiber-optic cables, satellite or cell phone transmissions, even storing data on a hard drive or flash drive), it is possible that the message will be corrupted by noise.
- An error-correcting code adds redundancy to the data in such a way that the original message may be recovered after transmission over the noisy channel.

Repetition Code

- Suppose message is either 0 or 1.
- Transmit 000 or 111.
- If only one bit gets corrupted, the original can be recovered.
- Example: 000 is sent. Possible that 010 is received. More probable that 000 was the original.

Hamming Code (a)

- Define 4×7 matrix G:

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

- Take any 4-bit message x (of 0's and 1's) and transmit the 7-bit message xG.
- Calculate xG using matrix multiplication over the binary field $\mathbb{F}_2 = \{0, 1\}$ under mod2 arithmetic.

Hamming Code (b)

- Example: if $x = 1010$, then $xG = 1000011$. (Remember that $1 + 1 \equiv 0 \bmod 2$.)
- Suppose one bit is corrupted during transmission.
- Say $y = 100\underline{1}011$ is received. (The corrupted bit is underlined.)

Hamming Code (c)

- Define 3×7 matrix H:

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

- Calculate $Hy^T = 100^T$.
- Error occurred in position 4 (100 in binary), so 1000011 was sent.

Hamming Code (d)

- Note that $HG^T = 0$.
- If one bit is corrupted, then $y = xG + e_i$, where e_i is all 0's except for a 1 in position i.
- Then $Hy^T = H(xG + e_i)^T = HG^T x^T + He_i^T$.
- But $HG^T = 0$, so $Hy^T = He_i^T$, which equals the ith column of H.
- The columns of H are just $1, 2, \ldots, 7$ in binary.

Finite Fields

- Work over a finite field $\mathbb{F}_q$. It is known that q must be a prime power, $q = p^e$ for some prime p and positive integer e. If $q = p$, $\mathbb{F}_p$ is just $\mathbb{Z}/p\mathbb{Z}$ with mod p arithmetic.
- To get $\mathbb{F}_q$, $q = p^e$, form the field extension $\mathbb{F}_p[x]/(f(x))$, where $f(x)$ is an irreducible polynomial over $\mathbb{F}_p$ of degree e.
- Example: $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2 + x + 1)$. So $\mathbb{F}_4 = \{0, 1, \omega, 1 + \omega\}$, where $\omega^2 = 1 + \omega$.

Linear Codes

- A *linear code* C over $\mathbb{F}_q$ is a linear subspace $C \subset \mathbb{F}_q^n$, for some n. The number n is the *length* of C. Let $k = \dim C$ as a vector space over $\mathbb{F}_q$.
- Let C_G be the subspace of $\mathbb{F}_2^7$ spanned by the rows of G. Then $\dim C_G = 4$.
- Let C_H be the subspace of $\mathbb{F}_2^7$ spanned by the rows of H. Then $\dim C_H = 3$.

Hamming Weight

- For any vector $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n$, define the *Hamming weight* $\mathrm{wt}(x)$ to equal the number of nonzero components of x. That is,

$$\mathrm{wt}(x) = |\{i : x_i \neq 0\}|.$$

- The smallest nonzero weight of $x \in C$ is called the *minimum weight* of the code C. It is a measure of how many errors C can correct ($<$ half the minimum weight).

Hamming Weight Enumerator

- It is useful to keep track of all the weights of elements of a code C.
- Given a linear code $C \subset \mathbb{F}_q^n$, the *Hamming weight enumerator* of C is the two-variable polynomial (generating function):

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

- $W_C(X, Y) = \sum_{i=0}^{n} A_i X^{n-i} Y^i$, where A_i is the number of elements of C of weight i.

Examples

- For $C_G \subset \mathbb{F}_2^7$, $\dim C_G = 4$, $|C_G| = 2^4 = 16$,

$$W_{C_G}(X, Y) = X^7 + 7X^4Y^3 + 7X^3Y^4 + Y^7.$$

- For $C_H \subset \mathbb{F}_2^7$, $\dim C_H = 3$, $|C_H| = 2^3 = 8$,

$$W_{C_H}(X, Y) = X^7 + 7X^3Y^4.$$

Dual Codes

- Dot product on $\mathbb{F}_q^n$ (all operations in $\mathbb{F}_q$):

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

  for $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$.
- It is a nondegenerate, symmetric bilinear form.
- If $C \subset \mathbb{F}_q^n$ is a linear code, then the *dual code* is

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

- Example: $C_H = C_G^\perp$ (and $C_G = C_H^\perp$).

"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 (a nice relationship between $W_{C^{\perp}}$ and W_C).

Florence Jessie MacWilliams

- 1917–1990
- 1962 doctoral dissertation under Andrew Gleason at Harvard University
- "Combinatorial Problems of Elementary Abelian Groups"
- Three sections, the second being the MacWilliams identities

Statement of the MacWilliams Identities

- For any linear code $C \subset \mathbb{F}_q^n$,

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

- Exercise: verify for C_G and C_H, where $q = 2$.

Proofs of Standard Properties

- 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.

Characters of Finite Abelian Groups

- Let $(G, +)$ be a finite abelian group.
- A *character* π of G is a group homomorphism $\pi : (G, +) \to (\mathbb{C}^\times, \times)$, where $(\mathbb{C}^\times, \times)$ is the multiplicative group of nonzero complex numbers.
- Example: let $G = \mathbb{Z}/n\mathbb{Z}$ be the integers modulo n.
  - For any integer a, $\pi_a(x) = \exp(2\pi iax/n)$, $x \in G$, is a character of G.
  - $\pi_a = \pi_b$ if and only if $a \equiv b \bmod n$.

Character Group

- The set $\widehat{G}$ of all characters of G is itself a finite abelian group under pointwise multiplication of functions.
- $\widehat{G}$ is called the *character group*.
- $\widehat{G} \cong G$ (not naturally); in particular, $|\widehat{G}| = |G|$.
- $\widehat{\widehat{G}} \cong G$ (naturally).

Two Useful Formulas

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

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

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 $H \subset G$,

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

Application to MacWilliams Identities (a)

- Let $G = \mathbb{F}_q^n$, an abelian group under addition.
- Let $H = C$, a linear code.
- Let $V = \mathbb{C}[X, Y]$, a complex vector space.
- Let $f : G \to V$ be

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

Application to MacWilliams Identities (b)

- Every character of $G = \mathbb{F}_q^n$ has the form π_a, for some $a \in \mathbb{F}_q^n$, with

$$\pi_a(x) = \exp(2\pi i \,\mathrm{Tr}(a \cdot x)/p), \quad x \in \mathbb{F}_q^n,$$

  where $\mathrm{Tr} : \mathbb{F}_q \longrightarrow \mathbb{F}_p$ is the absolute trace map to the prime field. View $\mathbb{F}_p$ as $\mathbb{Z}/p\mathbb{Z}$.
- $\pi_a \in (\widehat{G} : H)$ if and only if $a \in C^{\perp}$.
- $|(\widehat{G} : H)| = |C^{\perp}|$.

Application to MacWilliams Identities (c)

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

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

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

Idea of Manipulation

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

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

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.

Extended Hamming Code

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

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

- 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, $n \equiv 0 \bmod 8$.

Thank you

- I again thank Professor Xiusheng Liu for the invitation.
- I also thank you, the audience, for your kind attention.