The Extension Theorem for Lee Weight

Jay A. Wood

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

AMS meeting
University of St. Thomas
Minneapolis, MN
October 29, 2016

Co-authors

- This is a report on joint work with Sergey Dyshko and Philippe Langevin of the University of Toulon.

Monomial transformations

- Suppose $\mathbb{F}_q$ is a finite field.
- A *monomial transformation* $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ is determined by a permutation τ of $\{1, 2, \ldots, n\}$ and non-zero scalars (units) $u_i \in \mathbb{F}_q^\times$, $i = 1, 2, \ldots, n$:

$$T(x_1, x_2, \ldots, x_n) = (u_1 x_{\tau(1)}, \ldots, u_n x_{\tau(n)}),$$

  for all $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n$.
- If the u_i belong to a subgroup $G \subseteq \mathbb{F}_q^n$, we say that T is a *G-monomial transformation*.

Monomial transformations are isometries

- A monomial transformation preserves the Hamming weight wt:

$$\mathrm{wt}(T(x)) = \mathrm{wt}(x), \quad x \in \mathbb{F}_q^n.$$

The extension theorem of MacWilliams

- If $C \subseteq \mathbb{F}_q^n$ is a linear code and $f : C \to \mathbb{F}_q^n$ is a linear transformation that preserves the Hamming weight, then f extends to a monomial transformation T of $\mathbb{F}_q^n$. I.e., $f = T|_C$.
- This result was part of the 1962 doctoral dissertation of MacWilliams (as were the MacWilliams identities).

Lee weight on $\mathbb{Z}/N\mathbb{Z}$

- Represent elements of $\mathbb{Z}/N\mathbb{Z}$ by integers in $\{0, 1, \ldots, N-1\}$.
- The *Lee weight* w_L on $\mathbb{Z}/N\mathbb{Z}$ is

$$w_L(a) = \begin{cases} a, & 0 \leq a \leq \lfloor N/2 \rfloor, \\ N - a, & \lfloor N/2 \rfloor < a < N. \end{cases}$$

- The *Euclidean weight* w_E equals w_L^2.

Role of symmetry

- The Lee and Euclidean weights satisfy $w(-a) = w(a)$ for all $a \in \mathbb{Z}/N\mathbb{Z}$.
- The *symmetry group* of these weights is $G = \{\pm 1\}$.
- A G-monomial transformation (a “signed permutation”) of $(\mathbb{Z}/N\mathbb{Z})^n$ preserves the Lee and Euclidean weights.
- Is the extension theorem true for w_L and w_E?

Progression of results

- Numerical verification for $N \leq 2048$.
- (LW, dates from 2000) True for $N = 2^k$, $N = 3^k$ and $N = p = 2q + 1$, p, q primes.
- (Barra, 2012) True for $N = p = 4q + 1$, p, q primes.
- (DLW, 2016) True for $N = p$, p prime.
- (LW, 2016) True for $N = p^k$, p prime.
- (D, last month) True for any N.

Outline of plan of attack

- Extension theorem for symmetrized weight compositions.
- Invertibility of a matrix W.
- Factoring $\det(W)$.
- Showing that the factors of $\det(W)$ are nonzero.

Matrix W

- Let w be the Lee or Euclidean weight on $\mathbb{Z}/N\mathbb{Z}$.
- Let $r = \lfloor N/2 \rfloor$.
- Form an $r \times r$ matrix W with i, j entry equal to $w(ij)$, the value of w at the product ij in $\mathbb{Z}/N\mathbb{Z}$.
- If W is invertible (over $\mathbb{Q}$), then the extension theorem is true.
  - Fine print: Invertibility of W implies that any w-isometry preserves the symmetrized weight composition determined by $G = \{\pm 1\}$. Then apply the extension theorem for symmetrized weight compositions.

Factoring $\det(W)$

- When $N = p$, a prime, the matrix W represents, up to a permutation of columns, the regular representation in the group ring of $\mathbb{F}_p^\times/\{\pm 1\}$.
- (Dedekind-Frobenius) $\det(W)$ factors into a product of linear expressions, which are the Fourier coefficients of w with respect to the characters of $\mathbb{F}_p^\times/\{\pm 1\}$, i.e., of even multiplicative characters mod p.
- A generalization of this works for $N = p^k$, p prime.

A quadratic relation

- For Lee weight w_L and $a \in \mathbb{F}_p$, what is $w_L(2a)$?

$$w_L(2a) = \begin{cases} 2w_L(a), & 0 \leq a < p/4, \\ p - 2w_L(a), & p/4 < a < p/2. \end{cases}$$

- For any a, $0 \leq a < p/2$,

$$(w_L(2a) - 2w_L(a))(w_L(2a) - p + 2w_L(a)) = 0;$$
$$w_E(2a) - 4w_E(a) = p(w_L(2a) - 2w_L(a)).$$

Fourier coefficients

- Let χ be an even character mod p. Then the Fourier transform with respect to χ of the quadratic relation

$$w_E(2a) - 4w_E(a) = p(w_L(2a) - 2w_L(a))$$

yields

$$(\bar{\chi}(2) - 4)\hat{w}_E(\chi) = p(\bar{\chi}(2) - 2)\hat{w}_L(\chi).$$

- Thus: $\hat{w}_L(\chi) = 0$ if and only if $\hat{w}_E(\chi) = 0$.

Generalized Bernoulli numbers

- Given a character χ mod p, the first two generalized Bernoulli numbers are

$$B_1(\chi) = (1/p)\sum_{k=1}^{p} k\chi(k),$$

$$B_2(\chi) = (1/(2p))\sum_{k=1}^{p}(k^2 - pk)\chi(k).$$

If $\det(W) = 0$, then ...

- If $\det(W) = 0$ (for either w_L or w_E), then some Fourier coefficient $\hat{w}(\chi) = 0$, with χ a non-trivial even character mod p.
- Then both $\hat{w}_L(\chi) = 0$ and $\hat{w}_E(\chi) = 0$.
- One then computes that $B_1(\chi) = 0$ and $B_2(\chi) = 0$.

If $B_1(\chi) = B_2(\chi) = 0$, then ...

- Dirichlet L-function of χ:

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

- Fact: $L(-1,\chi) = -B_2(\chi)/2$.
- Fact: for a non-trivial even character χ and integers $n \geq 1$, $L(1-n,\chi) = 0$ if and only if n is odd.
- Let $n = 2$:
  $0 \neq L(1-2,\chi) = L(-1,\chi) = -B_2(\chi)/2 = 0$, contradiction!

Other cases

- A variant of the L-function argument works when $N = p^k$, p prime.
- Dyshko's proof for general N shows that $\det(W) \neq 0$ by showing that a related matrix is diagonally dominant with positive diagonal terms.