The Extension Theorem for Lee Weight Using Dirichlet L-functions

Jay A. Wood

Department of Mathematics
Western Michigan University
http://sites.google.com/a/wmich.edu/jaywood

University of São Paulo
July 17, 2017

In memoriam:
Maryam Mirzakhani,
May 3, 1977–July 15, 2017

Joint work

- This is joint work with Sergii Dyshko and Philippe Langevin.

Linear codes

- Let R be a finite commutative ring with 1.
- A **linear code** of length n over R is a submodule $C \subseteq R^n$.
- Classically, R was a finite field $\mathbb{F}_q$.
- Our interest today will be $R = \mathbb{Z}/N\mathbb{Z}$, especially the case where $N = p^k$, p prime.

Presenting a linear code

- Linear codes are often presented via a **generator matrix** G of size $k \times n$ over R.
- The linear code is the submodule of R^n generated by the rows of G.
- The generator matrix defines a homomorphism $R^k \to R^n$ via $x \mapsto xG$. If this map has a kernel, we may instead write the map as $M = R/\ker \to R^n$.
- We will call M an **information module**.

Errors in transmission

- Error-correcting codes are designed to detect and correct errors in transmission in communication channels.

$$M \xrightarrow[\text{encode}]{} R^n \xrightarrow[\text{transmit}]{+\text{noise}} R^n \xrightarrow[\text{decode}]{} R^n \xrightarrow[\text{unencode}]{} M$$

- The code adds redundancy which, if done properly, may allow errors to be corrected ("decoding").

Weights and distances

- When an element of R is transmitted, a different element might be received (a 'noisy channel').
- Weights and distances are often defined on R and R^n as a proxy for probabilities of errors.
- A **weight** w on R is any function $w : R \to \mathbb{C}$ with $w(0) = 0$. Extend to R^n by $w(\vec{x}) = \sum_{i=1}^{n} w(x_i)$.
- The **distance** on R^n determined by w is $d_w(\vec{x}, \vec{y}) = w(\vec{x} - \vec{y})$, where we assume $w(-r) = w(r)$ for all $r \in R$.

Three important examples

- For any R, the **Hamming weight** is $\mathrm{H}(0) = 0$ and $\mathrm{H}(r) = 1$ for $r \neq 0$.
- For $R = \mathbb{Z}/N\mathbb{Z}$, the **Lee** and **Euclidean** weights are

$$\mathrm{L}(r) = \min\{r, N - r\},$$
$$\mathrm{E}(r) = \min\{r^2, (N - r)^2\},$$

where $r \in R$ is represented by $r \in \{0, 1, \ldots, N - 1\}$.

Weight-preserving maps

- What are the invertible homomorphisms $R^n \to R^n$ that preserve one of these weights?
- A **monomial transformation** $T : R^n \to R^n$ is determined by a permutation σ of $\{1, 2, \ldots, n\}$ and units $u_1, \ldots, u_n$ of R. Define

$$T(\vec{x}) = (u_1 x_{\sigma(1)}, \ldots, u_n x_{\sigma(n)}).$$

- Hamming weight: all monomial transformations.
- Lee or Euclidean: need all $u_i = \pm 1$; 'signed permutations'.

Extension problem

- If $C \subseteq R^n$ is a linear code and T is a monomial transformation or signed permutation, then the restriction of T to C is an isomorphism from C to $C' = T(C)$ that preserves the weight (an 'isometry').
- Is the converse true?
- Extension problem: determine conditions on R and the weight w so that every isometry $C \to R^n$ extends to an isometry $R^n \to R^n$.
- Say: 'R and w have the extension property' (EP).

Some of what is known

- Hamming weight has EP: over finite fields (MacWilliams, 1961–62); over finite Frobenius rings (W, 1999); only over Frobenius rings (W, 2008).
- Lee weight has EP over $\mathbb{Z}/N\mathbb{Z}$ when N is: 2^k, 3^k, prime $p = 2q + 1$, q prime (Langevin, W, 2000); prime $p = 4q + 1$, q prime (Barra, 2012); any prime p (Dyskho, L, W, 2016); any prime power p^k (L, W, 2016); any positive integer (D, 2017).
- Euclidean: prime powers p^k (L, W).

Symmetrized weight compositions

- The Lee and Euclidean weights are invariant under the action of $U = \{\pm 1\}$: $\mathrm{L}(-x) = \mathrm{L}(x)$ and $\mathrm{E}(-x) = \mathrm{E}(x)$.
- Denote the set of nonzero orbits of U on $R = \mathbb{Z}/N\mathbb{Z}$ by $\mathcal{O}$. Orbit of r is $[r] = \{\pm r\}$.
- For $[r] \in \mathcal{O}$ and $x \in R^n$, define

$$\mathrm{swc}_{[r]}(x) = |\{i : x_i \in [r]\}|.$$

swc has EP

Theorem

Suppose $R = \mathbb{Z}/N\mathbb{Z}$ and $U = \{\pm 1\}$. If $f : C \to R^n$ preserves swc, *i.e.,* $\mathrm{swc}_{[r]}(f(x)) = \mathrm{swc}_{[r]}(x)$ *for all $x \in C$ and $[r] \in \mathcal{O}$, then f extends to a signed permutation.*

- Finite field case: Goldberg (1980)
- Finite Frobenius rings: W (1997)
- Improved proof: Barra, Gluesing-Luerssen (2015)

Proof

- For fixed $x \in C$, there exists a permutation σ_x and units $u_{i,x} \in U$ such that $f_i(x) = u_{i,x} x_{\sigma_x(i)}$.
- Special character on R: $\rho(r) = \exp(2\pi\sqrt{-1}r/N)$.
- Multiply by $u \in U$, plug into ρ, and sum:

$$\begin{aligned}\sum_{i=1}^{n}\sum_{u\in U}\rho(uf_i(x)) &= \sum_{i=1}^{n}\sum_{u\in U}\rho(uu_{i,x}x_{\sigma_x(i)}) \\ &= \sum_{i=1}^{n}\sum_{u\in U}\rho(ux_{\sigma_x(i)}) = \sum_{i=1}^{n}\sum_{u\in U}\rho(ux_i)\end{aligned}$$

Proof, continued

- Equation of characters: for all $x \in C$,

$$\sum_{i=1}^{n} \sum_{u \in U} \rho(uf_i(x)) = \sum_{j=1}^{n} \sum_{v \in U} \rho(vx_j)$$

- Linear independence of characters: for each i and $u = 1$ in the left, there exists $j = \sigma(i)$ and $v_i \in U$ on the right, with $\rho(f_i(x)) = \rho(v_i x_{\sigma(i)})$.
- ρ is injective: $f_i(x) = v_i x_{\sigma(i)}$. Signed permutation!

Expressing w in terms of swc

- Suppose weight w satisfies $w(-r) = w(r)$, $r \in R$.
- Then, for $x \in R^n$ and $[t] \in \mathcal{O}$:

$$w(x) = \sum_{[r]\in\mathcal{O}} w(r)\,\mathrm{swc}_{[r]}(x)$$

$$w(tx) = \sum_{[r]\in\mathcal{O}} w(tr)\,\mathrm{swc}_{[r]}(x)$$

Criterion

- Set $W_w = (w(tr))_{[t],[r]}$, a $|\mathcal{O}| \times |\mathcal{O}|$ matrix.

Theorem (W, 1999)

If the matrix W_w is invertible, then w has EP.

- Use $w(tx) = \sum_{[r]\in\mathcal{O}} w(tr)\,\mathrm{swc}_{[r]}(x)$ to show that swc is preserved.

Factoring det W_w

- When $N = p$ prime, $R = \mathbb{Z}/p\mathbb{Z}$ is a field, and $\mathcal{O}$ is a cyclic group.
- Dedekind-Frobenius (1896): det W_w factors into linear expressions in w given by the Fourier transforms of w with respect to the characters of $\mathcal{O}$ (even Dirichlet characters mod p).
- When $N = p^k$, p prime, there is a similar factorization in terms of even Dirichlet characters mod p^k and their conductors (W, 2000).

Fourier transforms

- From here on, assume $N = p$, an odd prime. The case of $N = p^k$ is similar, but more intricate.
- The factors of det W_w are $\hat{w}(\chi) = \sum_{r \in \mathcal{O}} w(r)\chi(r)$, where χ is a character of $\mathcal{O}$ (homomorphism $\chi : \mathcal{O} \to \mathbb{C}^\times$).
- $\mathcal{O} \leftrightarrow \{j : 1 \leq j < p/2\}$: $\hat{w}(\chi) = \sum_{j<p/2} w(j)\chi(j)$.
- If $f(x) = w(2x)$, then $\hat{f}(\chi) = \bar{\chi}(2)\hat{w}(\chi)$.
- $\sum_{j<p/2} w(2j)\chi(j) = \sum_{j<p/2} w(j)\chi(2^{-1}j) = \sum_{j<p/2} w(j)\bar{\chi}(2)\chi(j)$.

Special feature of Lee weight

- Remember that $\mathrm{L}(r) = \min\{r, N - r\}$.
- If $0 \le r < p/4$, then $\mathrm{L}(2r) = 2\mathrm{L}(r)$.
- If $p/4 < r < p/2$, then $\mathrm{L}(2r) = p - 2\mathrm{L}(r)$.
- For any r, $0 \le r < p/2$,
  $(\mathrm{L}(2r) - 2\mathrm{L}(r))(\mathrm{L}(2r) - p + 2\mathrm{L}(r)) = 0$.

Relation between Lee and Euclidean weights

- For any r, $0 \leq r < p/2$, $(\mathrm{L}(2r) - 2\mathrm{L}(r))(\mathrm{L}(2r) - p + 2\mathrm{L}(r)) = 0$.
- $\mathrm{L}(2r)^2 - 4\mathrm{L}(r)^2 = p(\mathrm{L}(2r) - 2\mathrm{L}(r))$
- $\mathrm{E}(2r) - 4\mathrm{E}(r) = p(\mathrm{L}(2r) - 2\mathrm{L}(r))$
- FT: $(\bar{\chi}(2) - 4)\hat{\mathrm{E}}(\chi) = p(\bar{\chi}(2) - 2)\hat{\mathrm{L}}(\chi)$.
- Thus: $\hat{\mathrm{E}}(\chi) = 0$ if and only if $\hat{\mathrm{L}}(\chi) = 0$.

Relation between determinants

- Suppose 2 has order r in $\mathcal{O}$, then

$$(2^r + 1)^{(p-1)/(2r)} \det W_{\mathrm{E}} = p^{(p-1)/2} \det W_{\mathrm{L}}.$$

- Take the product of $(\bar{\chi}(2) - 4)\hat{\mathrm{E}}(\chi) = p(\bar{\chi}(2) - 2)\hat{\mathrm{L}}(\chi)$ over all χ.
- Make use of factorization $t^r - 1 = \prod_{j=0}^{r-1}(t - \zeta^j)$, and homomorphism $\chi \mapsto \zeta = \bar{\chi}(2)$.

Dirichlet characters

- Given a character χ of $\mathbb{F}_p^\times$, set $\chi(0) = 0$ and extend χ to be periodic of period p: a **Dirichlet character** mod p.
- The **Dirichlet L-function** associated to χ:

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

- Converges absolutely for $\Re(s) > 1$.
- Functional equation allows analytic continuation to entire function of s ($\chi \neq 1$).

Generalized Bernoulli numbers

- For $\chi \neq 1$, define $B_n(\chi)$ via:

$$\sum_{a=1}^{p} \frac{\chi(a)te^{at}}{e^{pt}-1} = \sum_{n=0}^{\infty} B_n(\chi)\frac{t^n}{n!}.$$

- $B_1(\chi) = (1/p)\sum_{a=1}^{p} a\chi(a)$.
- $B_2(\chi) = (1/p)\sum_{a=1}^{p}(a^2 - ap)\chi(a)$.

Facts about Dirichlet L-functions

- For $n \geq 1$, $L(1-n,\chi) = -B_n(\chi)/n$.
- For $n \geq 1$, if χ is even, $\chi \neq 1$, then $L(1-n,\chi) = 0$ if and only if n is odd.

Outline

- We want to show that $\det W_w \neq 0$ for $w = \mathrm{L}$ or $w = \mathrm{E}$.
- To the contrary, assume $\det W_w = 0$, so that $\hat{w}(\chi) = 0$ for some even character $\chi \neq 1$.
- Remember that $\hat{\mathrm{L}}(\chi) = 0$ iff $\hat{\mathrm{E}}(\chi) = 0$.
- Calculate B_1 and B_2.
- Contradict information about $L(1-n, \chi) = 0$.

Preliminary calculation

- In all that follows, χ is even and $\chi \neq 1$.

$$2\hat{1}(\chi) = 2 \sum_{j<p/2} \chi(j) = \sum_{j=1}^{p} \chi(j) = 0.$$

- The sum of any nontrivial character over its group vanishes.

B_1 calculation

- $pB_1(\chi) = \sum_{j=1}^{p} j\chi(j)$.
- Split in two and re-index, using χ even:

$$pB_1(\chi) = \sum_{j<p/2} j\chi(j) + \sum_{j<p/2} (p-j)\chi(j)$$
$$= \sum_{j<p/2} p\chi(j) = p\hat{1}(\chi) = 0.$$

B_2 calculation

- $pB_2(\chi) = \sum_{j=1}^{p}(j^2 - jp)\chi(j) = \sum_{j=1}^{p} j^2\chi(j)$.
- Split in two, re-index, use $\hat{\mathrm{L}}(\chi) = \hat{\mathrm{E}}(\chi) = 0$:

$$pB_2(\chi) = \sum_{j<p/2} j^2\chi(j) + \sum_{j<p/2}(p-j)^2\chi(j)$$
$$= p^2\hat{1}(\chi) - 2p\hat{\mathrm{L}}(\chi) + 2\hat{\mathrm{E}}(\chi) = 0$$

Contradict $L(-1, \chi)$

- Under the hypothesis that $\hat{\mathrm{L}}(\chi) = \hat{\mathrm{E}}(\chi) = 0$ for even $\chi \neq 1$:
- $L(-1, \chi) = L(1-2, \chi) = -B_2(\chi)/2 = 0.$
- But, for even $\chi \neq 1$, $L(1-n, \chi) = 0$ if and only if n is odd.
- Thus L and E have EP over $\mathbb{Z}/p\mathbb{Z}$.

Thank you

- Thank you for the opportunity to speak to you.
- Thank you for your kind attention and your warm hospitality.