Linear Codes over Finite Rings and Modules

Jay A. Wood

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

Central China Normal University
Wuhan, Hubei
May 11, 2018
9. Extension theorem for Lee and Euclidean weights

- Work over $\mathbb{Z}/p\mathbb{Z}$ or $\mathbb{Z}/p^k\mathbb{Z}$, $p$ prime
- Factoring the determinant of $A$
- Fourier transforms
- Relation between Lee and Euclidean determinants
- Dirichlet $L$-functions and generalized Bernoulli numbers
Joint work

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

- A **weight** \( w \) on \( R \) is any function \( w : R \to \mathbb{C} \) with \( w(0) = 0 \). Extend to \( R^n \) by \( w(\vec{x}) = \sum_{i=1}^n w(x_i) \).

- For \( R = \mathbb{Z}/N\mathbb{Z} \), the **Lee** and **Euclidean** weights are

  \[
  L(r) = \min\{r, N - r\}, \\
  E(r) = \min\{r^2, (N - r)^2\},
  \]

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

- Our primary focus will be \( N = p \) or \( p^k \), \( p \) prime.
Symmetry groups

- The ring $\mathbb{Z}/N\mathbb{Z}$ is commutative, so the two symmetry groups are equal.
- Both Lee weight and Euclidean weight have symmetry group $G = \{\pm 1\}$. 
Extension problem

- \( R = \mathbb{Z}/N\mathbb{Z}, \ G = \{\pm 1\}. \)
- Given a linear code \( C \subseteq R^n \) and an injective homomorphism \( f : C \to R^n \), if \( f \) preserves the Lee weight \( L \) or the Euclidean weight \( E \), does \( f \) extend to a \( G \)-monomial transformation?
- Yes!
Progression of knowledge

- Minimal polynomial approach gives 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).

- This talk’s approach: any prime (Dyskho, L, W, 2016); any prime power (L, W, 2016).

Recall (Lecture 8): Form matrix $\mathcal{A}$ with rows indexed by nonzero $[r] \in G_{lt} \setminus R$ and columns indexed by nonzero $[a] \in A/G_{rt}$:

$$\mathcal{A}_{[r],[a]} = w(ra).$$

This lecture: $A = R$, so set $\mathcal{O} = R^\times / \{\pm 1\}$ (nonzero classes).

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

**Theorem (W, 1999)**

*If the matrix $\mathcal{A}_w$ is invertible, then $w$ has EP.*
Factoring $\det A_w$

- When $N = p$ prime, $R = \mathbb{Z}/p\mathbb{Z}$ is a field, and $\mathcal{O}$ is a cyclic group.
- Dedekind-Frobenius (1896): $\det A_w$ factors into linear expressions in $w$ given by the Fourier transforms of $w$ with respect to the characters of $\mathcal{O}$ (known as ‘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).
- The next several slides explain the Dedekind-Frobenius factorization.
Examples

- For $p = 5$ and $p = 7$, here are the $A_w$ matrices.

\[
A_5 = \begin{bmatrix} w_1 & w_2 \\ w_2 & w_1 \end{bmatrix}, \quad A_7 = \begin{bmatrix} w_1 & w_2 & w_3 \\ w_2 & w_3 & w_1 \\ w_3 & w_1 & w_2 \end{bmatrix}.
\]

- $\det A_5 = w_1^2 - w_2^2 = (w_1 + w_2)(w_1 - w_2)$.
- $\det A_7 = 3w_1w_2w_3 - (w_1^3 + w_2^3 + w_3^3) = - (w_1 + w_2 + w_3)(w_1 + \zeta w_2 + \zeta^2 w_3)(w_1 + \zeta^2 w_2 + \zeta w_3)$, where $\zeta$ is a primitive third root of unity.
More representation theory

Let $G$ be any finite (multiplicative) group.
The complex group algebra $\mathbb{C}G = \{\alpha : G \to \mathbb{C}\}$ is a $\mathbb{C}$-algebra under pointwise addition and scalar multiplication of functions, with

$$(\alpha\beta)(g) = \sum_{xy=g} \alpha(x)\beta(y)$$

$$= \sum_{y \in G} \alpha(gy^{-1})\beta(y).$$
Left multiplication

- Fix element $\alpha \in \mathbb{C}G$.
- Left multiplication by $\alpha$ is a linear transformation $\mathbb{C}G \rightarrow \mathbb{C}G$.
- What is the matrix representing left multiplication by $\alpha$?
Basis of group elements

- Given a group element $g \in G$, define $\delta_g \in \mathbb{C}G$ by
  \[
  \delta_g(x) = \begin{cases} 
  1, & x = g, \\
  0, & x \neq g.
  \end{cases}
  \]

- The $\delta_g$, $g \in G$, form a basis of $\mathbb{C}G$.
- Then $(\alpha \delta_h)(g) = \sum_{y \in G} \alpha(gy^{-1})\delta_h(y) = \alpha(gh^{-1})$.
- Left multiplication by $\alpha$ is given by a matrix whose $(g, h)$-entry is $\alpha(gh^{-1})$.
- Note that $\delta_{1_G} = 1_{\mathbb{C}G}$. 
Group determinant

- If we view the values of $\alpha$ as indeterminates, $\alpha(g) = x_g$, $g \in G$, then $\det(x_{gh^{-1}})$ is called the **group determinant** of $G$.
- Then $\det(x_{gh}) = \pm \det(x_{gh^{-1}})$.
- Dedekind and Frobenius factored the group determinant, 1896.
Abelian case: characters give idempotents

- Suppose $G$ is abelian.
- For any character $\pi \in \hat{G}$, set $e_\pi = \pi/|G| \in \mathbb{C}G$.
- Then $e_\pi$ is idempotent: $e_\pi^2 = e_\pi$ in $\mathbb{C}G$.

\[
\pi^2(g) = \sum_{y \in G} \pi(gy^{-1})\pi(y) = \sum_{y \in G} \pi(g)\pi(y^{-1})\pi(y) = |G|\pi(g).
\]

- Thus $e_\pi^2 = \frac{\pi^2(g)}{|G|^2} = \frac{\pi(g)}{|G|} = e_\pi$. 
Characters are orthogonal

- Suppose $\pi, \theta \in \hat{G}$ are different: $\pi \neq \theta$.
- Claim: $e_\pi e_\theta = 0$.

\[
(\pi \theta)(g) = \sum_{y \in G} \pi(gy^{-1})\theta(y)
\]

\[
= \sum_{y \in G} \pi(g)\pi(y^{-1})\theta(y)
\]

\[
= \pi(g) \sum_{y \in G} (\pi^{-1} \theta)(y) = 0
\]

(by summation formulas in Lecture 3)
Hermitian inner product on \( \mathbb{C}G \)

- Hermitian inner product on \( \mathbb{C}G \):
  \[
  \langle \alpha, \beta \rangle = \left( \sum_{y \in G} \alpha(y) \overline{\beta(y)} \right) / |G|,
  \]

  where \( \overline{\cdot} \) is complex conjugation.

- For characters, define \( \overline{\pi}(y) = \pi(y) \). Then
  \[
  \pi(y) = (\pi(y))^{-1} = \pi(y^{-1}) = \pi^{-1}(y), \text{ so } \overline{\pi} = \pi^{-1}.
  \]

- Characters are orthonormal: \( \langle \pi, \theta \rangle = 0 \) for \( \pi \neq \theta \) and \( \langle \pi, \pi \rangle = 1 \). So characters are linearly independent (as promised in Lecture 6).
Use idempotents as a basis of $\mathbb{C}G$

- $\sum_{\pi \in \hat{G}} e_{\pi} = \delta_{1_G} = 1_{\mathbb{C}G}$.
- Using the $e_{\pi}$, $\pi \in \hat{G}$, as a basis of $\mathbb{C}G$ yields
  $$\mathbb{C}G \cong \mathbb{C} \oplus \cdots \oplus \mathbb{C}$$
  as $\mathbb{C}$-algebras. There are $|G|$ summands.
- In this basis, $\alpha = \sum_{\pi \in \hat{G}} c_{\pi} e_{\pi}$, where
  $c_{\pi} = |G| \langle \alpha, \pi \rangle = \sum_{y \in G} \alpha(y) \overline{\pi}(y) = \hat{\alpha}(\pi)$.
- Bad joke: despite appearances, $\pi \neq ¥ = \text{CNY}$. 
Factoring $\text{det } A_w$

▶ The determinant of a linear transformation is independent of the basis chosen.

▶ In the abelian case, $\text{det}(\alpha(gh^{-1})) = \prod_{\pi \in \hat{G}} \hat{\alpha}(\pi)$.

▶ Thus for $N = p$,

$$\text{det } A_w = \det(w(tr)) = \pm \prod_{\pi \in \hat{O}} \hat{w}(\pi).$$

▶ There is a similar factorization when $N = p^k$ that involves the conductors of the characters $\pi$. 
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 $\det A_w$ are $\widehat{w}(\chi) = \sum_{r \in \mathcal{O}} w(r) \chi(r)$, where $\chi$ is a character of $\mathcal{O}$.
- $\mathcal{O} \leftrightarrow \{j : 1 \leq j < p/2\}$: $\widehat{w}(\chi) = \sum_{j < p/2} w(j) \chi(j)$.
- If $f(x) = w(2x)$, then $\hat{f}(\chi) = \bar{\chi}(2) \hat{w}(\chi)$.
- $\sum_{j < p/2} w(2j) \chi(j) = \sum_{i < p/2} w(i) \chi(2^{-1}i) = \sum_{i < p/2} w(i) \bar{\chi}(2) \chi(i)$. (Reindex the sum via $i = 2j$.)
Special feature of Lee weight

- Remember that $N = p$, so $L(r) = \min\{r, p - r\}$.
- If $0 \leq r < p/4$, then $L(2r) = 2L(r)$.
- If $p/4 < r < p/2$, then $L(2r) = p - 2L(r)$.
- For any $r$, $0 \leq r < p/2$,
  \[(L(2r) - 2L(r))(L(2r) - p + 2L(r)) = 0.\]
Relation between Lee and Euclidean weights

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

- Suppose $2$ has order $r$ in $\mathcal{O}$, then
  \[(2^r + 1)^{(p-1)/(2r)} \det A_E = p^{(p-1)/2} \det A_L.\]

- Take the product of
  \[(\bar{\chi}(2) - 4)\hat{E}(\chi) = p(\bar{\chi}(2) - 2)\hat{L}(\chi)\]
  over all $\chi$.

- 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 $\chi$ of $\mathbb{F}_p^\times$, set $\chi(0) = 0$ and extend $\chi$ to be periodic of period $p$: a **Dirichlet character** mod $p$. If $\chi(-1) = 1$, i.e., $\chi \in \hat{O}$, $\chi$ is **even**.

- The **Dirichlet $L$-function** associated to $\chi$:

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

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

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

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

- $B_1(\chi) = \frac{1}{p} \sum_{a=1}^{p} a\chi(a)$.
- $B_2(\chi) = \frac{1}{p} \sum_{a=1}^{p} (a^2 - ap)\chi(a)$. 
Facts about Dirichlet $L$-functions

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

- We want to show that $\det A_w \neq 0$ for $w = L$ or $w = E$.
- To the contrary, assume $\det A_w = 0$, so that $\hat{w}(\chi) = 0$ for some even character $\chi \neq 1$. (When $\chi = 1$, $\hat{w}(\chi) = \sum_{j < p/2} w(j) > 0$.)
- Remember that $\hat{L}(\chi) = 0$ iff $\hat{E}(\chi) = 0$.
- Calculate $B_1$ and $B_2$.
- Contradict information about $L(1 - n, \chi) = 0$. 
Preliminary calculation

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

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

- 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 $\chi$ even:

\[
pB_1(\chi) = \sum_{j<p/2} j\chi(j) + \sum_{j<p/2} (p-j)\chi(j)
= \sum_{j<p/2} p\chi(j) = p \cdot \hat{1}(\chi) = 0.
\]
$B_2$ 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 $\hat{L}(\chi) = \hat{E}(\chi) = 0$:

$$pB_2(\chi) = \sum_{j < p/2} j^2 \chi(j) + \sum_{j < p/2} (p - j)^2 \chi(j)$$

$$= p^2 \cdot \hat{1}(\chi) - 2p\hat{L}(\chi) + 2\hat{E}(\chi) = 0$$
Contradict $L(-1, \chi)$

- Under the hypothesis that $\hat{L}(\chi) = \hat{E}(\chi) = 0$ 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 $\mathbb{Z}/p\mathbb{Z}$. 