Character-Theoretic Tools for Studying Linear Codes over Rings and Modules

Jay A. Wood

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

Algebraic Methods in Coding Theory
CIMPA School
Ubatuba, Brazil
July 14, 2017

10. Extension Problem for general weights

- Report on work of Dyshko for Lee weight (2017)
- Generalized to weights over modules
- Fourier transforms and linear independence of characters
- Recursive argument involving posets

Dyshko's work

- Sergii Dyshko has proved EP for the Lee weight over any $\mathbb{Z}/N\mathbb{Z}$ (2017)
- Part of his proof was a general criterion for any weight over $Z/N\mathbb{Z}$ to have EP.
- Dyshko's ideas can be generalized to module alphabets.

Set up: the alphabet

- R finite ring, A finite left R-module
- Assume A is pseudo-injective and has cyclic socle.
- Pseudo-injective: for any submodule $B \subseteq A$ and injective homomorphism $f : B \to A$, f extends to isomorphism $A \to A$.
- Cyclic socle: implies that A injects into $\widehat{R}$ and that $\widehat{A}$ is a cyclic right R-module, with generating character χ.

Set up: the weight

- Let w be a weight on A; $w : A \to \mathbb{C}$, $w(0) = 0$.
- Symmetry groups

$$G_{\mathrm{lt}} = \{u \in \mathcal{U}(R) : w(ua) = w(a), a \in A\},$$
$$G_{\mathrm{rt}} = \{\phi \in \mathrm{GL}_R(A) : w(a\phi) = w(a), a \in A\}.$$

The problem

- Determine conditions on w that imply w has EP.
- EP: for $C \subseteq A^n$ and linear w-isometry $f : C \to A^n$, f extends to a G_{rt}-monomial transformation of A^n.

Some matrices

- For any submodule $B \subseteq A$, define a matrix $Q^B = (Q^B_{\phi,u})$:

$$Q^B_{\phi,u} = \sum_{b \in B} w(b\phi)\chi(ub),$$

where $\phi \in \mathrm{Stab}(B) \backslash \mathrm{GL}_R(A) / G_{\mathrm{rt}}$ and $u \in \mathrm{Stab}(\chi|_B) \backslash \mathcal{U}(R) / G_{\mathrm{lt}}$.

- Here, $\mathrm{Stab}(B) = \{\phi \in \mathrm{GL}_R(A) : b\phi = b, b \in B\}$ is the *point-wise* stabilizer of B.

Main result

- Condition: for each nonzero submodule $B \subseteq A$:

$$\text{the matrix } Q^B \text{ has zero left nullspace.} \tag{1}$$

Theorem

If (1) is satisfied, then w has EP.

Isometry condition

- Let $C \subseteq A^n$ be the image of $\Lambda : M \to A^n$, $\Lambda = (\lambda_1, \ldots, \lambda_n)$, with information module $M \cong C$.
- Set $N = \Lambda f : M \to A^n$, $N = (\nu_1, \ldots, \nu_n)$.
- f being a w-isometry means

$$\sum_{i=1}^{n} w(x\lambda_i) = \sum_{j=1}^{n} w(x\nu_j), \quad x \in M.$$

- Goal: show that the numbers of λ_i and ν_j in a given G_{rt}-orbit are equal.
- Method: take Fourier transform and set up linear equations in these numbers.

Fourier transform calculation

- Each $\lambda_i, \nu_j \in \mathrm{Hom}_R(M, A)$.
- For arbitrary $\sigma \in \mathrm{Hom}_R(M, A)$, what is the Fourier transform of $f_\sigma : M \to \mathbb{C}$, $x \mapsto w(x\sigma)$?
- For $\pi \in \widehat{M}$,

$$\hat{f}_\sigma(\pi) = \sum_{x \in M} \pi(x) f_\sigma(x) = \sum_{x \in M} \pi(x) w(x\sigma).$$

- Write in terms of sum over values $x\sigma \in \operatorname{im} \sigma$.

Re-write sum

- For $\pi \in \widehat{M}$,

$$\hat{f}_\sigma(\pi) = \sum_{a \in \operatorname{im}\sigma} \sum_{x : x\sigma = a} \pi(x) w(a) = \sum_{a \in \operatorname{im}\sigma} w(a) \sum_{x : x\sigma = a} \pi(x).$$

- Because σ is a homomorphism, $\sum_{x:x\sigma=a} \pi(x)$ is a sum over a coset of $\ker \sigma$.
- Let $x_a \in M$ be one element with $x_a\sigma = a$. Then every $x \in M$ with $x\sigma = a$ has the form $x = x_a + k$ with $k \in \ker \sigma$.

Simplify character sum

$$\begin{aligned}
\sum_{x : x\sigma = a} \pi(x) &= \sum_{k \in \ker\sigma} \pi(x_a + k) \\
&= \pi(x_a) \sum_{k \in \ker\sigma} \pi(k) \\
&= \begin{cases} |\ker\sigma|\pi(x_a), & \pi \in (\widehat{M} : \ker\sigma), \\ 0, & \pi \notin (\widehat{M} : \ker\sigma). \end{cases}
\end{aligned}$$

Summary of calculation

- For $\pi \in \widehat{M}$,

$$\hat{f}_\sigma(\pi) = \begin{cases} |\ker\sigma| \sum_{a \in \operatorname{im}\sigma} w(a)\pi(x_a), & \pi \in (\widehat{M} : \ker\sigma), \\ 0, & \pi \notin (\widehat{M} : \ker\sigma). \end{cases}$$

- When $\pi \in (\widehat{M} : \ker\sigma)$, the value of $\pi(x_a)$ depends only on a: π descends to well-defined character on $M/\ker\sigma \cong \operatorname{im}\sigma$.
- When $\pi \in (\widehat{M} : \ker\sigma)$, write $(\mathcal{F}_{\operatorname{im}\sigma} w)(\pi) = \sum_{a \in \operatorname{im}\sigma} w(a)\pi(x_a) = \sum_{x \in M/\ker\sigma} w(x\sigma)\pi(x)$.

Dual maps

- For $\sigma \in \mathrm{Hom}_R(M, A)$, $\sigma : M \to A$, there is the dual map $\hat{\sigma} : \widehat{A} \to \widehat{M}$ with image $\operatorname{im} \hat{\sigma}$.
- Remember that $\widehat{A}$ is a cyclic right R-module, so $\operatorname{im} \hat{\sigma}$ is also cyclic.
- $\operatorname{im} \hat{\sigma} = (\widehat{M} : \ker \sigma)$.
- If $\psi \in \widehat{A}$, $x \in \ker \sigma$, $\hat{\sigma}(\psi)(x) = \psi(x\sigma) = \psi(0) = 1$.
- If $\pi \in (\widehat{M} : \ker \sigma)$, π descends to well-defined character on $M/\ker \sigma \cong \operatorname{im} \sigma \subseteq A$. Any lift $\tilde{\pi}$ of π under $\widehat{A} \twoheadrightarrow (\operatorname{im} \sigma)\widehat{}$ has $\hat{\sigma}(\tilde{\pi}) = \pi$.

Fourier transform of isometry condition

- Let the indicator function of a subset $S \subseteq \widehat{M}$ be δ_S: value 1 on S, value 0 elsewhere.
- Isometry condition: $\sum_{i=1}^n w(x\lambda_i) = \sum_{j=1}^n w(x\nu_j)$.
- Fourier transform: an equation of functions on $\widehat{M}$:

$$\sum_{i=1}^n |\ker \lambda_i| (\mathcal{F}_{\operatorname{im}\lambda_i} w) \delta_{\operatorname{im}\hat{\lambda}_i} = \sum_{j=1}^n |\ker \nu_j| (\mathcal{F}_{\operatorname{im}\nu_j} w) \delta_{\operatorname{im}\hat{\nu}_j}.$$

Picking a maximal submodule

- The character module $\widehat{M}$ is partially ordered by set inclusion.
- Among the submodules $\operatorname{im}\hat{\lambda}_i, \operatorname{im}\hat{\nu}_j \subseteq \widehat{M}$, choose one that is maximal under set inclusion. Refer to it as $\operatorname{im}\hat{\sigma}$, with $\sigma \in \operatorname{Hom}_R(M, A)$.
- Recall that $\operatorname{im}\hat{\sigma}$ is a cyclic right R-module. Denote by $\mathcal{U}(\operatorname{im}\hat{\sigma})$ the set of all generators of $\operatorname{im}\hat{\sigma}$. We restrict the Fourier transform equation to $\mathcal{U}(\operatorname{im}\hat{\sigma}) \subseteq \widehat{M}$.

Exploiting the Fourier transform

- If $\pi \in \mathcal{U}(\operatorname{im}\hat{\sigma})$, evaluating the Fourier transform equation at π yields nonzero terms only when $\pi \in \operatorname{im}\hat{\lambda}_i$ or $\pi \in \operatorname{im}\hat{\nu}_j$.
- Because π generates $\operatorname{im}\hat{\sigma}$, this means $\operatorname{im}\hat{\sigma} \subseteq \operatorname{im}\hat{\lambda}_i$ or $\operatorname{im}\hat{\sigma} \subseteq \operatorname{im}\hat{\nu}_j$.
- But $\operatorname{im}\hat{\sigma}$ was chosen to be maximal, so $\operatorname{im}\hat{\sigma} = \operatorname{im}\hat{\lambda}_i$ or $\operatorname{im}\hat{\sigma} = \operatorname{im}\hat{\nu}_j$.
- Thus $(\widehat{M} : \ker\sigma) = (\widehat{M} : \ker\lambda_i)$ or $(\widehat{M} : \ker\sigma) = (\widehat{M} : \ker\nu_j)$; $\ker\sigma = \ker\lambda_i$ or $\ker\sigma = \ker\nu_j$.

When are kernels equal?

- Let A be pseudo-injective. For $\sigma, \tau \in \mathrm{Hom}_R(M, A)$, $\ker \sigma = \ker \tau$ if and only if $\sigma = \tau\phi$ for some $\phi \in \mathrm{GL}_R(A)$.
- If $\sigma = \tau\phi$, then $x\sigma = 0$ iff $x\tau = 0$, as ϕ is invertible.
- If $\ker \sigma = \ker \tau$, σ, τ descend to well-defined injective maps $\bar{\sigma}, \bar{\tau} : M/\ker \tau \to A$. Set $B = \operatorname{im} \bar{\tau} \subseteq A$. Then $\bar{\tau}^{-1}\bar{\sigma} : B \to A$ is injective.
- By pseudo-injectivity, $\bar{\tau}^{-1}\bar{\sigma}$ extends to $\phi \in \mathrm{GL}_R(A)$; then $\bar{\sigma} = \bar{\tau}\phi$ and $\sigma = \tau\phi$.

Summary of exploitation

- Evaluating the Fourier transform equation at $\pi \in \mathcal{U}(\operatorname{im} \hat{\sigma})$ yields

$$\sum_{\lambda_i \in \sigma \, \mathrm{GL}_R(A)} (\mathcal{F}_{\operatorname{im} \lambda_i} w)(\pi) = \sum_{\nu_j \in \sigma \, \mathrm{GL}_R(A)} (\mathcal{F}_{\operatorname{im} \nu_i} w)(\pi).$$

- The factors of $|\ker \lambda_i| = |\ker \sigma| = |\ker \nu_j|$ cancel.

Next steps

- Write equations in terms of G_{rt}-orbits, not just $\mathrm{GL}_R(A)$-orbits.
- Vary $\pi \in \mathcal{U}(\operatorname{im} \hat{\sigma})$: get different equations for different G_{lt}-orbits.
- How does the Fourier transform equation depend on these orbits?

Dependency on orbits

- Remember that for each $\pi \in \mathcal{U}(\operatorname{im}\hat{\sigma})$, we have
$$\sum_{\lambda_i \in \sigma \operatorname{GL}_R(A)} (\mathcal{F}_{\operatorname{im}\lambda_i} w)(\pi) = \sum_{\nu_j \in \sigma \operatorname{GL}_R(A)} (\mathcal{F}_{\operatorname{im}\nu_i} w)(\pi).$$
- The right $\operatorname{GL}_R(A)$-orbit of σ is a disjoint unit of G_{rt}-orbits, parametrized by elements of $\operatorname{Stab}(\sigma)\backslash \operatorname{GL}_R(A)/G_{\mathrm{rt}}$.
- The generators $\mathcal{U}(\operatorname{im}\hat{\sigma})$ equal the right $\mathcal{U}$-orbit of π, which is a disjoint union of G_{lt}-orbits, parametrized by elements of $\operatorname{Stab}(\pi)\backslash\mathcal{U}/G_{\mathrm{lt}}$.

What does $(\mathcal{F}_{\operatorname{im}\lambda_i} w)(\pi^u)$ depend on?

- Fix σ and $\pi \in \mathcal{U}(\operatorname{im}\hat{\sigma})$. Let $\xi \in \mathrm{Stab}(\sigma)$, $\phi \in \mathrm{GL}_R(A)$, $\psi \in G_{\mathrm{rt}}$, $s \in \mathrm{Stab}(\pi)$, $u \in \mathcal{U}$, and $v \in G_{\mathrm{lt}}$. Then (with $y = vx$),

$$\begin{aligned}
(\mathcal{F}_{\operatorname{im}\sigma\xi\phi\psi} w)(\pi^{suv}) &= \sum_{x \in M/\ker\sigma} w(x\sigma\xi\phi\psi)\pi^{suv}(x) \\
&= \sum_{x \in M/\ker\sigma} w(x\sigma\phi)\pi^{u}(vx) \\
&= \sum_{y \in M/\ker\sigma} w(v^{-1}y\sigma\phi)\pi^{u}(y) \\
&= (\mathcal{F}_{\operatorname{im}\sigma\phi} w)(\pi^u).
\end{aligned}$$

Re-write the Fourier transform equation

- Remember that for each $\pi \in \mathcal{U}(\operatorname{im}\hat{\sigma})$, we have

$$\sum_{\lambda_i \in \sigma\,\mathrm{GL}_R(A)} (\mathcal{F}_{\operatorname{im}\lambda_i} w)(\pi) = \sum_{\nu_j \in \sigma\,\mathrm{GL}_R(A)} (\mathcal{F}_{\operatorname{im}\nu_i} w)(\pi).$$

- Break up sum into pieces that depend on the G_{rt}-orbits of σ.
- Get an equation for each generator of the form π^u, as π^u varies over different G_{lt}-orbits of π.

Counting functions

- For each $\tau \in \mathrm{Stab}(\sigma)\backslash \mathrm{GL}_R(A)/G_{\mathrm{rt}}$, set

$$\beta(\tau) = |\{i : \lambda_i \in \sigma\tau G_{\mathrm{rt}}\}| - |\{j : \nu_j \in \sigma\tau G_{\mathrm{rt}}\}|.$$

- At π^u, $u \in \mathrm{Stab}(\pi)\backslash\mathcal{U}/G_{\mathrm{lt}}$, Fourier transform equation becomes

$$\sum_{\tau} \beta(\tau)(\mathcal{F}_{\mathrm{im}\,\sigma\tau} w)(\pi^u) = 0.$$

- View as matrix equation with rows given by τ and columns given by u.

Bringing in condition (1)

- Condition (1) had $Q^B_{\phi,u} = \sum_{b\in B} w(b\phi)\chi(ub)$.
- Recall: $(\mathcal{F}_{\operatorname{im}\sigma\tau} w)(\pi^u) = \sum_{x\in M/\ker\sigma} w(x\sigma\tau)\pi^u(x)$.
- Use $(\widehat{M} : \ker\sigma) \cong (M/\ker\sigma)\widehat{\ } \cong (\operatorname{im}\sigma)\widehat{\ }$:
  $\pi \in (\widehat{M} : \ker\sigma) \leftrightarrow \rho \in (\operatorname{im}\sigma)\widehat{\ }$, with $\pi(x) = \rho(x\sigma)$ or $\rho(b) = \pi(x_b)$ where $x_b\sigma = b$.
- Then $(\mathcal{F}_{\operatorname{im}\sigma\tau} w)(\pi^u) = \sum_{b\in\operatorname{im}\sigma} w(b\tau)\rho(ub)$.
- This is condition (1) for $B = \operatorname{im}\sigma$.
- Generating character χ for $\widehat{A}$ restricts to a generator for any $\widehat{B}$.

Applying condition (1)

- By condition (1), we have $\beta(\tau) = 0$ for all τ. I.e., $|\{i : \lambda_i \in \sigma\tau G_{\mathrm{rt}}\}| = |\{j : \nu_j \in \sigma\tau G_{\mathrm{rt}}\}|$, any τ.
- Choose a matching: for any of these j, there is an $i = P(j)$ and $\phi_j \in G_{\mathrm{rt}}$ such that $\nu_j = \lambda_{P(j)}\phi_j$.
- Then $w(x\nu_j) = w(x\lambda_{P(j)}\phi_j) = w(x\lambda_{P(j)})$, $x \in M$.
- Subtract these terms from the isometry condtion, and proceed recursively.
- From remaining $\mathrm{im}\,\hat{\lambda}_i$, $\mathrm{im}\,\hat{\nu}_j$, choose one that is maximal, etc. Repeat.

Dyshko's result on Lee weight

- Consider $R = \mathbb{Z}/N\mathbb{Z}$ with the Lee weight.
- By some clever estimates, Dyshko shows that (a permutation of) the matrix Q^B is diagonally dominant, hence invertible.
- Uses fact that for $ab = c$, $\mathbb{Z}/a\mathbb{Z} \hookrightarrow \mathbb{Z}/c\mathbb{Z}$, $x \mapsto bx$, the restriction of the Lee weight of $\mathbb{Z}/c\mathbb{Z}$ to $b(\mathbb{Z}/a\mathbb{Z})$ is b times the Lee weight of $\mathbb{Z}/a\mathbb{Z}$.
- I won't go into the details.

Thank you

- Thank you for your kind attention during this series of lectures.
- Thanks again to the organizers for all their work and their hospitality.