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 11, 2017

7. MacWilliams extension theorem for other weights

- Homogeneous and egalitarian weights
- Symmetrized weight compositions
- General weight: reducing to symmetrized weight compositions
- Weights with maximal symmetry
- Lee and Euclidean weights on $\mathbb{Z}/N\mathbb{Z}$

Notation

- Let R be a finite associative ring with 1.
- Let A be a finite unital left R-module: the **alphabet**.
- Let $w : A \to \mathbb{Q}$ be a **weight**: $w(0) = 0$. Extend to A^n by

$$w(a_1, \ldots, a_n) = \sum_{i=1}^{n} w(a_i).$$

Symmetry groups

- Recall the **symmetry groups** of w:

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

- $\mathcal{U} = \mathcal{U}(R)$ is the group of units of R, and $\mathrm{GL}_R(A)$ is the group of invertible R-linear homomorphisms $A \to A$.
- Recall that I will usually write homomorphisms of left modules on the right side; $f : A \to A$, $(ra)f = r(af)$.

Orbit spaces

- For an information module M, recall the **orbit spaces**:

$$\mathcal{O} = G_{\mathrm{lt}} \backslash M$$

$$\mathcal{O}^\sharp = \mathrm{Hom}_R(M, A) / G_{\mathrm{rt}}$$

W-map

- F denotes "functions"; F_0: those that vanish at 0.
- The W-**map** is

$$W : F_0(\mathcal{O}^\sharp, \mathbb{Q}) \to F_0(\mathcal{O}, \mathbb{Q}).$$

- For $x \in M$,

$$W(\eta)(x) = \sum_{[\lambda] \in \mathcal{O}^\sharp} w(x\lambda)\eta([\lambda]).$$

Using generating character to define a weight

- Suppose the alphabet A admits a generating character ρ: $\mathrm{Soc}(A)$ cyclic.
- Fix a subgroup $U \subseteq \mathrm{GL}_R(A)$.
- Define a weight $w_U : A \to \mathbb{C}$:

$$w_U(a) = 1 - \frac{1}{|U|} \sum_{\phi \in U} \rho(a\phi), \quad a \in A.$$

Properties of w_U

- $w_U(0) = 0$.
- $U \subseteq G_{\mathrm{rt}}(w_U)$.
- Indeed, suppose $\psi \in U$. Then

$$w_U(a\psi) = 1 - \frac{1}{|U|} \sum_{\phi \in U} \rho(a\psi\phi), \quad a \in A.$$

- Re-index the summation with $\phi' = \psi\phi$ to see that $w_U(a\psi) = w_U(a)$ for all $a \in A$.

Egalitarian property

- For any nonzero left R-submodule $B \subseteq A$, and any $a_0 \in A$,
$$\sum_{b \in B} w_U(a_0 + b) = |B|.$$

$$\begin{aligned}\sum_{b \in B} w_U(a_0 + b) &= \sum_{b \in B} \left(1 - \frac{1}{|U|} \sum_{\phi \in U} \rho((a_0 + b)\phi) \right) \\ &= \sum_{b \in B} \left(1 - \frac{1}{|U|} \sum_{\phi \in U} \rho(a_0\phi)\rho(b\phi) \right)\end{aligned}$$

Egalitarian property, continued

$$\begin{aligned}\sum_{b\in B} w_U(a_0+b) &= |B| - \frac{1}{|U|}\sum_{\phi\in U}\left(\rho(a_0\phi)\sum_{b\in B}\rho(b\phi)\right)\\ &= |B|.\end{aligned}$$

- $\sum_{b\in B}\rho(b\phi) = 0$ because $B\phi \not\subseteq \ker\rho$, which in turn follows from ρ being a generating character.
- We say that w_U is **egalitarian** on cosets of B.
- $w_{\mathrm{GL}_R(A)}$ is called **homogeneous**: Constantinescu, Heise, Greferath, Schmidt, Honold, Nechaev.

w_U has EP, with U-monomial tranformations

- Suppose $w_U(x\Lambda) = w_U(xN)$ for all $x \in M$.
- Equation of characters: for all $x \in M$,

$$\sum_{i=1}^{n} \sum_{\phi \in U} \rho(x\lambda_i\phi) = \sum_{j=1}^{n} \sum_{\psi \in U} \rho(x\nu_j\psi).$$

- Use linear independence of characters: for $j = 1$, $\psi = \mathrm{id}_A$, there exist $i = \sigma(1)$ and $\phi_1 \in U$ with $\rho(x\lambda_{\sigma(1)}\phi_1) = \rho(x\nu_1)$ for all $x \in M$.
- ρ generating: $\nu_1 = \lambda_{\sigma(1)}\phi_1$. Inner sums agree, reduce outer sum, and continue by induction.

More about posets

- Let S be a finite poset with $\preceq$.
- Define the **Möbius function** $\mu : S \times S \to \mathbb{Z}$ as follows.
- $\mu(s, s) = 1$ for all $s \in S$.
- $\mu(s, t) = 0$ when $s \not\preceq t$.
- Recursive: for $s \prec t$ (i.e., $s \preceq t$ but $s \neq t$),

$$\sum_{x : s \preceq x \preceq t} \mu(s, x) = 0.$$

- Can solve for $\mu(s, t)$ in terms of "lower" $\mu(s, x)$.

Example

- Let $\mathcal{L}(\mathbb{F}_q^n)$ be the poset of linear subspaces of $\mathbb{F}_q^n$ under set inclusion.
- When $V \subseteq W$, let $c = \dim W - \dim V$ be the codimension. Then

$$\mu(V, W) = \begin{cases} 0, & V \not\subseteq W, \\ (-1)^c q^{\binom{c}{2}}, & V \subseteq W. \end{cases}$$

- Verification involves the Cauchy Binomial Theorem.

More about the homogeneous weight

- Greferath, Nechaev, Wisbauer, 2004.
- Let A be a finite left R-module.
- Let $S = \{Ra : a \in A\}$ be the poset of all cyclic left R-submodules of A under set inclusion.
- For $a \in A$, define

$$w(a) = 1 - \frac{\mu(0, Ra)}{|\mathcal{U}(R)a|}.$$

Properties of homogeneous weight

- If $Ra = Rb$ (iff $\mathcal{U}a = \mathcal{U}b$), then $w(a) = w(b)$.
- w is egalitarian on nonzero cyclic left submodules B:

$$\sum_{b \in B} w(b) = |B|.$$

- w is egalitarian on all nonzero left submodules if and only if $\mathrm{Soc}(A)$ is cyclic.

Relation to orbit sums

- Suppose $\mathrm{Soc}(A)$ is cyclic, so that A admits a generating character ρ.
- Summing the generating character over the $\mathcal{U}$-orbit of $a \in A$ yields $\mu(0, Ra)$:

$$\sum_{x \in \mathcal{U}a} \rho(x) = \mu(0, Ra).$$

Corollary (Honold)

$$w(a) = 1 - \frac{1}{|\mathcal{U}a|} \sum_{x \in \mathcal{U}a} \rho(x).$$

Proof

- Set $f(a) = \sum_{x \in \mathcal{U}a} \rho(x)$.
- Note that $f(0) = 1$.
- For $a \neq 0$, the left submodule Ra is the disjoint union of the left $\mathcal{U}$-orbits inside Ra:

$$\sum_{x \in Ra} \rho(x) = \sum_{\mathcal{U}b \subseteq Ra} \sum_{x \in \mathcal{U}b} \rho(x) = \sum_{Rb \subseteq Ra} f(b).$$

- But $\sum_{x \in Ra} \rho(x) = 0$, because ρ is a generating character and $Ra \neq 0$.
- Thus $f(a)$ satisfies the properties defining $\mu(0, Ra)$.

Symmetrized weight composition

- This time, no weight. Just ring R, alphabet A, and a subgroup $G \subseteq \mathrm{GL}_R(A)$.
- Define an equivalence relation from the right action of G on A: for $a, b \in A$, $a \sim b$ if $b = a\phi$ for some $\phi \in G$. Denote equivalence class of a by $[a]$.
- For $a \in A$ and $x = (x_1, \ldots, x_n) \in A^n$, define the **symmetrized weight composition** (swc) by

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

- Example: $R = A = \mathbb{Z}/4\mathbb{Z}$, $G = \{\pm 1\}$.

swc has EP with G-monomial transformations

- Assume A has generating character ρ (cyclic socle).
- Suppose $C_1, C_2 \subseteq A^n$ are two left R-linear codes.
- Suppose $f : C_1 \to C_2$ is a linear isomorphism of R-modules that preserves swc:

$$\mathrm{swc}_{[a]}(xf) = \mathrm{swc}_{[a]}(x), \quad a \in A, x \in C_1.$$

- Then f extends to a G-monomial transformation.

Proof (a)

- Result dates from 1997, but we will use the local-global idea of Barra, Gluesing-Luerssen (2014). This is joint work with N. El Garem and N. Megahed (2015).
- As before, view preservation of swc in terms of $\Lambda, N : M \to A^n$:

$$\mathrm{swc}_{[a]}(x\Lambda) = \mathrm{swc}_{[a]}(xN), \quad a \in A, x \in M.$$

- Local: for each $x \in M$, there exist a permutation σ_x and elements $\phi_{1,x}, \ldots, \phi_{n,x} \in G$ with $x\nu_i = x\lambda_{\sigma_x(i)}\phi_{i,x}$.

Proof (b)

- Local to global: apply $\phi \in G$ and ρ, then sum over ϕ and i. For every $x \in M$:

$$\sum_{i=1}^{n} \sum_{\phi \in G} \rho(x\nu_i\phi) = \sum_{i=1}^{n} \sum_{\phi \in G} \rho(x\lambda_{\sigma_x(i)}\phi_{i,x}\phi).$$

- Dependence on x disappears! For all $x \in M$:

$$\sum_{i=1}^{n} \sum_{\phi \in G} \rho(x\nu_i\phi) = \sum_{i=1}^{n} \sum_{\phi \in G} \rho(x\lambda_i\phi).$$

- Proceed as before to get G-monomial transformation.

General weight: reducing to swc

- Now include a weight w. Suppose alphabet A has cyclic socle. Form swc using $G = G_{\mathrm{rt}}(w)$.
- For any $b = (b_1, \ldots, b_n) \in A^n$,

$$w(b) = \sum_{i=i}^{n} w(b_i) = \sum_{[a] \in A/G_{\mathrm{rt}}} w(a)\, \mathrm{swc}_{[a]}(b).$$

- For a scalar multiple $rb \in A^n$, $r \in R$:

$$w(rb) = \sum_{[a] \in A/G_{\mathrm{rt}}} w(ra)\, \mathrm{swc}_{[a]}(b).$$

- $w(rb)$ depends only on class $[r] \in G_{\mathrm{lt}} \backslash R$.

Sufficient condition for EP for w

- Form matrix $\mathcal{A}$ with rows indexed by nonzero $[r] \in G_{\mathrm{lt}} \backslash R$ and columns indexed by nonzero $[a] \in A / G_{\mathrm{rt}}$:
$$\mathcal{A}_{[r],[a]} = w(ra).$$

Theorem (1999)

If matrix $\mathcal{A}$ has a trivial right nullspace, then alphabet A has EP for w.

- When $A = R$ is commutative, $\mathcal{A}$ is square. Condition is $\det \mathcal{A} \neq 0$.

Proof (a)

- Suppose $f : C_1 \to C_2$ is an isomorphism of R-modules and that f is a linear isometry with respect to w. Codes are given by $\Lambda : M \to A^n$ and $N : M \to A^n$, as usual.
- Isometry: $w(x\Lambda) = w(xN)$, for all $x \in M$.
- For every $x \in M$, $r \in R$:

$$\begin{aligned} 0 &= w(rx\Lambda) - w(rxN) \\ &= \sum_{[a] \in A/G_{\mathrm{rt}}} w(ra) \left\{ \mathrm{swc}_{[a]}(x\Lambda) - \mathrm{swc}_{[a]}(xN) \right\} \end{aligned}$$

Proof (b)

- The condition on matrix $\mathcal{A}$ implies $\mathrm{swc}_{[a]}(x\Lambda) = \mathrm{swc}_{[a]}(xN)$ for every $a \in A$ and $x \in M$.
- This means that $f : C_1 \to C_2$ preserves swc.
- Apply EP for swc to conclude that f extends to a G_{rt}-monomial transformation.

Cases of maximal symmetry

- Progress on finding more explicit conditions over ring alphabets ($A = R$) when the weight w has maximal symmetry: $G_{\mathrm{lt}} = G_{\mathrm{rt}} = \mathcal{U}(R)$.
- When R is a product of chain rings: Greferath, Mc Fadden, Zumbrägel, 2013.
- When R is a principal ideal ring: Greferath, Honold, Mc Fadden, Wood, Zumbrägel, 2014. Here $\det \mathcal{A}$ is factored into terms $\sum_{0<dR\leq aR} w(d)\mu(0, dR)$, for $a \in R$, where μ is the Möbius function for the poset of principal right ideals of R.
- Maximal symmetry case for $A = \widehat{R}$ in lecture 9.

Examples over $\mathbb{Z}/N\mathbb{Z}$

- In addition to the Hamming weight, there are three additional weights that are easy to define on $\mathbb{Z}/NZ$.
- Lee weight: viewing $\mathbb{Z}/NZ = \{0, 1, \ldots, N-1\}$, Lee weight is $w_L(a) = \min\{a, N-a\}$.
- Euclidean weight: $w_E(a) = w_L(a)^2$.
- Complex Euclidean weight: $|\exp(2\pi ia/N) - 1|^2 = 2 - 2\cos(2\pi a/N)$ (square of complex length).

Facts about EP over $\mathbb{Z}/N\mathbb{Z}$

- Only the complex Euclidean weight is easy: it is the egalitarian weight using $U = \{\pm 1\}$.
- EP for Lee weight and Euclidean weight has been numerically verified ($\mathcal{A}$ invertible) for $N \leq 2048$.
- EP for Lee weight and Euclidean weight holds for $N = p^k$, p prime. Work of Barra, Dyshko, Langevin, Wood.
- EP for Lee weight holds for any N: Dyshko. Dyshko's approach will be discussed in Lecture 10.