Linear codes over finite rings and modules: The MacWilliams extension theorem for general weights

Jay A. Wood

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

Coding Theory Seminar
Eastern Kentucky University
March 6, 2013

Today's topics

- More information about finite Frobenius rings.
- Characterizing Frobenius rings via $R \cong \widehat{R}$.
- Extension theorem for general weight functions.

Finite Frobenius Rings

- Finite ring R with 1.
- The (Jacobson) *radical* $\mathrm{Rad}(R)$ of R is the intersection of all the maximal left ideals of R; $\mathrm{Rad}(R)$ is a two-sided ideal of R.
- The (left/right) *socle* $\mathrm{Soc}(R)$ of R is the ideal of R generated by all the simple left/right ideals of R.
- R is *Frobenius* if $R/\mathrm{Rad}(R) \cong \mathrm{Soc}(R)$ as one-sided modules (both left and right).

$\mathbb{Z}/m\mathbb{Z}$

- Let $R = \mathbb{Z}/m\mathbb{Z}$, where m has prime factorization $m = p_1^{k_1} p_2^{k_2} \cdots p_l^{k_l}$.
- Chinese remainder theorem:

$$\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \mathbb{Z}/p_2^{k_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_l^{k_l}\mathbb{Z}.$$

- $J = (p_1 p_2 \cdots p_l)$ and $R/J \cong \mathbb{Z}/(p_1 p_2 \cdots p_l)\mathbb{Z} \cong \mathbb{Z}/p_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_l\mathbb{Z}$.
- $\mathrm{Soc}(R) = (p_1^{k_1-1} \cdots p_l^{k_l-1}) \cong \mathbb{Z}/p_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_l\mathbb{Z}$.

$M_m(\mathbb{F}_q)$

- Let $R = M_m(\mathbb{F}_q)$ be the ring of $m \times m$ matrices over $\mathbb{F}_q$.
- R has no nontrivial two-sided ideals, so $J = 0$.
- $\mathbb{F}_q^m$ is a simple module, and $R = \mathrm{Soc}(R) \cong m\mathbb{F}_q^m$.

Klemm's example

- Let $R = \mathbb{F}_2[X, Y]/(X^2, XY, Y^2)$. R is a 3-dimensional algebra over $\mathbb{F}_2$, with vector space basis $1, X, Y$.
- $J = (X, Y)$, with $R/J \cong \mathbb{F}_2$. R is a local ring.
- $\mathrm{Soc}(R) = J \cong 2\mathbb{F}_2$.

Two Useful Theorems About Finite Frobenius Rings

- (Honold, 2001) $R/\operatorname{Rad}(R) \cong \operatorname{Soc}({}_R R)$ as left modules iff $R/\operatorname{Rad}(R) \cong \operatorname{Soc}(R_R)$ as right modules.
- R is Frobenius iff $R \cong \widehat{R}$ as left modules iff $R \cong \widehat{R}$ as right modules (Hirano, 1997; indep. 1999).
- Corollary: R is Frobenius iff there exists a character χ of R such that $\ker \chi$ contains no nonzero left (right) ideal of R. This χ is a *generating character*.

Characters on a Finite Ring

- Let R be a finite ring, with 1.
- A *character* of R is a homomorphism $\pi : (R, +) \to (\mathbb{C}^\times, \cdot)$.
- The set $\widehat{R}$ of all characters of R is an (R, R)-bimodule with scalar multiplications

$$({}^r\pi)(x) = \pi(xr),$$
$$(\pi^r)(x) = \pi(rx),$$

for $\pi \in \widehat{R}$, $r, x \in R$.

Generating Characters

- For any character $\pi \in \widehat{R}$, there are two homomorphisms $R \longrightarrow \widehat{R}$:

$$r \longmapsto {}^{r}\pi,$$
$$r \longmapsto \pi^{r}.$$

  The first is left linear; the second is right linear.
- A character π is a *left (right) generating character* if the first (second) map is surjective.

Equivalent Conditions

- Remember $|\widehat{R}| = |R|$.
- A map $R \longrightarrow \widehat{R}$ is surjective iff it is injective iff it is bijective.
- The first map $r \longmapsto {}^{r}\pi$ is injective iff $\ker \pi$ contains no nonzero left ideal of R.
- The second map $r \longmapsto \pi^{r}$ is injective iff $\ker \pi$ contains no nonzero right ideal of R.

Left-Right Symmetry

- A character χ is left generating iff it is right generating.
- Suppose χ is right generating and that $Rx \subset \ker \chi$.
- $\chi(rx) = 1$ for all $r \in R$; $\chi^r(x) = 1$ for all $r \in R$.
- Thus x is annihilated by every character of R, implying $x = 0$.

Generating Characters and Frobenius Rings

- Theorem. R is Frobenius iff R admits a generating character.
- All isomorphisms below are as one-sided modules.
- Fact: $(R/\operatorname{Rad}(R))\widehat{\ } \cong \operatorname{Soc}(\widehat{R})$.
- Matrix fact: $(R/\operatorname{Rad}(R))\widehat{\ } \cong R/\operatorname{Rad}(R)$.
- If $R \cong \widehat{R}$ (existence of generating character), then $R/\operatorname{Rad}(R) \cong \operatorname{Soc}(R)$, and R is Frobenius.

Producing a Generating Character

- The converse remains: if R is Frobenius, how to produce a generating character?
- Start with $\mathrm{Soc}(R) \cong R/\mathrm{Rad}(R)$, which is a sum of square matrix modules.
- Suppose θ is a character of $\mathrm{Soc}(R)$ such that $\ker\theta$ contains no nonzero left submodule of $\mathrm{Soc}(R)$.
- Take any extension of θ to a character χ of R.
- Theorem: χ is a generating character of R.

Some Details

- Why does an extension exist?
- $0 \to \mathrm{Soc}(R) \to R \to R/\mathrm{Soc}(R) \to 0$ induces $0 \to (R/\mathrm{Soc}(R))\widehat{\ } \to \widehat{R} \to (\mathrm{Soc}(R))\widehat{\ } \to 0$.
- Suppose I is a left ideal with $I \subset \ker \chi$. Then $\mathrm{Soc}(I) \subset \mathrm{Soc}(R) \cap \ker \chi = \ker \theta$, because $\chi = \theta$ on $\mathrm{Soc}(R)$.
- By hypothesis on θ, $\mathrm{Soc}(I) = 0$. Thus $I = 0$.

Characters on Matrix Modules

- Let $R = M_m(\mathbb{F}_q)$ and $M = M_{m\times k}(\mathbb{F}_q)$; $q = p^e$.
- Theorem. M admits a character θ such that $\ker\theta$ contains no nonzero left R-submodule iff $m \geq k$.
- R itself has generating character: $\chi(P) = \exp(2\pi i \operatorname{Tr}_{q,p}(\operatorname{Tr} P)/p)$, where Tr is the matrix trace and $\operatorname{Tr}_{q,p} : \mathbb{F}_q \longrightarrow \mathbb{F}_p$ is the field trace, $\operatorname{Tr}_{q,p}(x) = x + x^p + x^{p^2} + \cdots + x^{p^{e-1}}$ for $x \in \mathbb{F}_q$.
- For $m \geq k$, embed M into R and restrict χ to M.
- Failure when $m < k$ is an exercise in linear algebra.

Final Argument

- If R is Frobenius, then $\mathrm{Soc}(R) \cong R/\mathrm{Rad}(R)$ is a sum of square matrix modules.
- Each of these matrix modules admits a character with no nonzero left submodules in its kernel.
- The product of these characters is a character of $\mathrm{Soc}(R)$ with no nonzero submodules in its kernel.
- Extend this character (in any way) to a character of R, and the extension is a generating character of R

Examples

- Finite fields $\mathbb{F}_q$: $\chi(x) = \exp(2\pi i \operatorname{Tr}_{q,p}(x)/p)$.
- $\mathbb{Z}/n\mathbb{Z}$: $\chi(x) = \exp(2\pi i x/n)$.
- Galois rings (Galois extensions of $\mathbb{Z}/p^m\mathbb{Z}$). $\operatorname{Soc}(R) \cong \mathbb{F}_{p^m}$; use χ for $\mathbb{F}_{p^m}$ and extend.
- Finite chain rings (all ideals form a chain). Extend from $\operatorname{Soc}(R) \cong \mathbb{F}_q$.
- Products of Frobenius rings. Use product of the generating characters.
- Matrix rings over a Frobenius ring: $M_n(R)$. $\chi = \chi_R \circ \operatorname{Tr}$.
- Finite group rings over a Frobenius ring: $R[G]$. $\chi(\sum a_g g) = \chi_R(a_e)$, e is identity element.

The setting for the extension theorem

- Let R be a finite, associative ring with 1.
- We allow R to be noncommutative.
- The group of units of R is denoted $\mathcal{U}$.
- A left *linear code* over R of length n is a left R-submodule $C \subset R^n$.
- One can consider module alphabets, too, but not today.

Weights

- A *weight* on R is a function $w : R \to \mathbb{C}$ with $w(0) = 0$.
- The *Hamming weight* has $\mathrm{wt}(a) = 1$ for all $a \neq 0$.
- The Lee and Euclidean weights on $\mathbb{Z}/N\mathbb{Z}$: $w_L(r) = |r|$, $w_E(r) = |r|^2$, for $-N/2 < r \leq N/2$.
- Homogeneous weight on any finite ring.
- For $a \in R^n$, define $w(a) = \sum w(a_i)$.

Symmetry groups

- Suppose R has weight w.
- The *left symmetry group* is $G_l := \{v \in \mathcal{U} : w(vr) = w(r), r \in R\}$.
- The *right symmetry group* is $G_r := \{u \in \mathcal{U} : w(ru) = w(r), r \in R\}$.

Monomial transformations (a)

- A *monomial transformation* is a homomorphism $T : R^n \longrightarrow R^n$ of left R-modules of the form

$$T(a_1, \ldots, a_n) = (a_{\sigma(1)}u_1, \ldots, a_{\sigma(n)}u_n),$$

where $u_i \in \mathcal{U}$ and σ is a permutation of $\{1, \ldots, n\}$.

Monomial transformations (b)

- A G_r-*monomial transformation* is one where each $u_i \in G_r$.
- Every G_r-monomial transformation preserves w: $w(T(a)) = w(a)$ for $a \in R^n$.

The Extension Problem

- Suppose $C_1, C_2 \subset R^n$ are two left R-linear codes.
- If $T(C_1) = C_2$, then $T : C_1 \longrightarrow C_2$ is a w-preserving isomorphism between the codes.
- Is the converse true? If $f : C_1 \longrightarrow C_2$ is a w-preserving isomorphism, does f extend to a G_r-monomial transformation?
- True for Hamming weight over finite fields (MacWilliams) and over finite Frobenius rings. Same for homogeneous weight (Greferath-Schmidt).
- What about other weights?

Split the problem in two

- Given a weight w on R, the weight determines the right symmetry group G_r.
- The group G_r determines a partition of R.
- The partition determines a *symmetrized weight composition* swc of a vector in R^n: counting the number of entries that belong to the various partition components.
- Prove an extension theorem for swc.
- Determine conditions on w so that preserving w implies preserving swc.

Partition and swc

- Given G_r, for $r, s \in R$, define $r \sim s$ if there exists $u \in G_r$ with $r = su$. This is an equivalence relation (coming from a group action).
- Denote the equivalence class of $r \in R$ by $[r]$. This defines a partition of R.
- For $a \in R^n$ and $r \in R$, define $\mathrm{swc}_{[r]}(a) := |\{i : a_i \in [r]\}|$.
- A G_r-monomial transformation preserves swc: i.e., $\mathrm{swc}_{[r]}(T(a)) = \mathrm{swc}_{[r]}(a)$, for all $a \in C_1$ and all $[r]$.

Extension theorem for swc

Theorem (1997)

Suppose R is a finite Frobenius ring. Suppose $f : C_1 \longrightarrow C_2$ is an isomorphism between linear codes in R^n that preserves swc. *Then f extends to a G_r-monomial transformation of R^n.*

- This is the only result I know that controls the units: they belong to G_r.

Proof (a)

- As in yesterday's talk, suppose the codes are images of $\Lambda_i : M \longrightarrow R^n$, with $\Lambda_i = (\lambda_{i,1}, \ldots, \lambda_{i,n})$ and $\Lambda_2 = f \circ \Lambda_1$.
- Preserving swc means that $\mathrm{swc}_{[r]}(\Lambda_1(x)) = \mathrm{swc}_{[r]}(\Lambda_2(x))$ for all $x \in M$ and $[r]$.
- Improvement by Barra, 2012: for every x, there is a permutation σ_x, depending on x, such that $\lambda_{1,i}(x) \sim \lambda_{2,\sigma_x(i)}(x)$. Say, $\lambda_{1,i}(x) = \lambda_{2,\sigma_x(i)}(x)u_{i,x}$.

Proof (b)

- Then, for a generating character ρ of R,

$$\sum_{i=1}^{n}\sum_{u\in G_r}\rho(\lambda_{1,i}(x)u) = \sum_{i=1}^{n}\sum_{u\in G_r}\rho(\lambda_{2,\sigma_x(i)}(x)u_{i,x}u)$$
$$= \sum_{i=1}^{n}\sum_{u\in G_r}\rho(\lambda_{2,i}(x)u).$$

- Now use the same linear independence argument to match up terms: the units necessarily are in G_r.

Reducing w to swc (a)

- Remember that $w(ru) = w(r)$ when $u \in G_r$, thus

$$w(a) = \sum_{i=1}^{n} w(a_i) = \sum_{[r]} w(r)\,\mathrm{swc}_{[r]}(a),\ a \in R^n.$$

- Scalar multiply on the left by $t \in R$:

$$w(ta) = \sum_{i=1}^{n} w(ta_i) = \sum_{[r]} w(tr)\,\mathrm{swc}_{[r]}(a).$$

- Only the left G_l-orbit of $t \in R$ matters.

Reducing w to swc (b)

- Look at differences of $w(\Lambda_1(tx)) - w(\Lambda_2(tx))$:

$$\begin{aligned} w(\Lambda_1(tx)) - w(\Lambda_2(tx)) &= w(t\Lambda_1(x)) - w(t\Lambda_2(x)) \\ &= \sum_{[r]} w(tr) \left(\mathrm{swc}_{[r]}(\Lambda_1(x)) - \mathrm{swc}_{[r]}(\Lambda_2(x)) \right) . \end{aligned}$$

- Thus, if f preserves w (left side $= 0$), then f preserves swc, provided the matrix

$$\mathcal{A} = \left(w(tr) \right)_{G_l t, r G_r}$$

has zero right null space. (Use only nonzero orbits.)

Summary

Theorem (1999)

Suppose R is a finite Frobenius ring with weight w. Then the extension theorem holds with respect to w if and only if the matrix

$$\mathcal{A} = (w(tr))_{G_l t, rG_r},$$

whose rows and columns are parametrized by the nonzero left G_l- and right G_r-orbits, has zero right null space.

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

- Let $R = \mathbb{Z}/N\mathbb{Z}$.
- Every congruence class mod N has a unique representative r in the range $-N/2 < r \leq N/2$.
- Define the *Lee weight* $w_L(r) := |r|$ and the *Euclidean weight* $w_E(r) := |r|^2$.
- Both these weights have $G_l = G_r = \{\pm 1\}$.

Results for Lee weight

- Can verify by computer that $\mathcal{A}$ is invertible for $N \leq 1024$ (at least).
- One can prove the extension theorem for Lee weight on $\mathbb{Z}/N\mathbb{Z}$ when: $N = 2^k$, $N = 3^k$, $N = p = 2q + 1$ (with p, q both prime), or (Barra, 2012) $N = p = 4q + 1$ (p, q both prime).
- For Euclidean weight when $N = 2^k$ or $N = p = 2q + 1$ (with p, q both prime).

Chain rings

- Suppose R is a finite chain ring, i.e., all its ideals are two-sided and they form a chain.
- Suppose a weight w on R has maximal symmetry, i.e., $G_l = G_r = \mathcal{U}$.
- One shows that the (square) matrix $\mathcal{A}$ has a triangular form and is invertible if and only if $w \neq 0$ on $\mathrm{Soc}(R)$.

Matrix rings (a)

- Suppose R is the matrix ring $M_m(\mathbb{F}_q)$ of all $m \times m$ matrices over $\mathbb{F}_q$.
- Assume again that w has maximal symmetry. Then the value of w depends only on the rank of the matrix in R. Let w_i be the weight of a rank i matrix.
- One can multiply $\mathcal{A}$ by a matrix Q determined by the poset of left ideals of R.
- By its construction, $\det Q = 1$.

Matrix rings (b)

- One proves that $Q\mathcal{A}$ has a block triangular form.
- $\det \mathcal{A}$ factors into expressions of the form

$$\sum_{i=1}^{s} (-1)^i q^{\binom{i}{2}} \begin{bmatrix} s \\ i \end{bmatrix}_q w_i.$$

- Extension theorem holds iff all these factors are nonzero.

Principal ideal rings

- Greferath and Honold have developed a technique essentially dual to the $\mathcal{A}$ matrix approach (2006).
- They and Mc Fadden and Zumbrägel have applied this approach to settle the case of products of chain rings with w having maximal symmetry (2013).
- All of us are now collaborating on the case where R is a principal ideal ring with w having maximal symmetry. The idea is to show that $Q\mathcal{A}$ is triangular, as in the matrix case.

Thank you

- Thank you for your kind attention, questions, and comments.
- Thanks again to Edgar and Steve for their hospitality.