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 13, 2017
9. Using semigroup rings

- Report on joint work with Gnilke, Greferath, Honold, and Zumbrägel
- Semigroup rings
- Modules over semigroup rings
- Connections to EP
- The case of bi-invariant weights over Frobenius bimodules
Semigroups

- Consider a finite \textbf{semigroup}: one associative operation, written as multiplication.
- Main example for us: the multiplicative semigroup of a finite ring $R$ with 1.
- This semigroup has a 1 (a \textbf{monoid}) and a 0.
Semigroup rings

- Analogous to group rings.
- We will use complex coefficients.
- One way: form $\mathbb{C}$-vector space with basis $e_r$, $r \in R$.
- Define multiplication of basis elements to be $e_re_s = e_{rs}$, where $rs$ is the product in $R$.
- Extend linearly.
- Note that $\mathbb{C}e_0$ is a two-sided ideal
Equivalent approach

- Define $\mathcal{R} = \{\alpha : R \to \mathbb{C}\}$ to be the $\mathbb{C}$-vector space of all $\mathbb{C}$-valued functions on $R$; dim $\mathcal{R} = |R|$.

- Product on $\mathcal{R}$ ("multiplicative convolution"): 

$$ (\alpha * \beta)(r) = \sum_{st=r} \alpha(s)\beta(t), \quad r \in R, $$

where the sum is over pairs $s, t$ in $R$ with $st = r$.

- Then $\alpha \leftrightarrow \sum_{r \in R} \alpha(r)e_r$ of other approach.
**$R$-modules induce $\mathcal{R}$-modules**

- Let $A$ be a finite left $R$-module.
- Set $\mathcal{A} = \{w : A \to \mathbb{C}\}$, a $\mathbb{C}$-vector space with $\dim \mathcal{A} = |A|$.
- Then $\mathcal{A}$ is a right $\mathcal{R}$-module via “right correlation”:

\[(w \ast \alpha)(a) = \sum_{r \in R} w(ra)\alpha(r), \quad a \in A.\]

- $w \ast (\alpha \ast \beta) = (w \ast \alpha) \ast \beta$, $w \in \mathcal{A}$, $\alpha, \beta \in \mathcal{R}$.
- Similarly for right $R$-module; get left $\mathcal{R}$-module.
Some splittings

- Set $\mathcal{R}_0 = \{\alpha \in \mathcal{R} : \sum_{r \in \mathcal{R}} \alpha(r) = 0\}$: augmentation ideal.
- $\mathcal{R}_0$ is a two-sided ideal of $\mathcal{R}$; $\mathcal{R} = \mathbb{C}e_0 \oplus \mathcal{R}_0$.
- Set $\mathcal{A}_0 = \{w \in \mathcal{A} : w(0) = 0\}$; $\mathcal{A}_0$ is a right $\mathcal{R}$-submodule, and $\mathcal{A} = \mathbb{C}1 \oplus \mathcal{A}_0$, where $1 \in \mathcal{A}$ is the constant function 1.
Recall the extension property EP

- Recall that a **weight** \( w \) on an alphabet \( A \) is any function \( w : A \rightarrow \mathbb{C} \) with \( w(0) = 0 \); i.e., \( w \in A_0 \).

- Recall that \( A \) has the extension property (EP) with respect to a weight \( w \) if every linear \( w \)-isometry \( f : \mathbb{C} \rightarrow A^n \) extends to a monomial transformation of \( A^n \) that is a \( w \)-isometry.
Isometries

Theorem (Greferath-Honold)

If $f$ is a $w$-isometry, then $f$ is a $(w \otimes \alpha)$-isometry for any $\alpha \in \mathcal{R}$.

$$(w \otimes \alpha)(xf) = \sum_{r \in \mathcal{R}} w(rxf)\alpha(r)$$

$$= \sum_{r \in \mathcal{R}} w(rx)\alpha(r) = (w \otimes \alpha)(x)$$
Connections to EP

Corollary

*If $A$ has EP with respect to $w \ast \alpha$, then $A$ has EP with respect to $w$. *

- If $f$ is a $w$-isometry, then it is a $(w \ast \alpha)$-isometry. By EP for $w \ast \alpha$, $f$ extends to a monomial transformation.

- *Fine print: need to worry about the right symmetry groups being different: $w \ast \alpha$ may have more symmetry than $w$. 

Case of bi-invariant weights over Frobenius bimodules

- For the rest of today, let $A$ be a Frobenius bimodule over $R$. I.e., $A$ is a bimodule over $R$ with $A \cong \hat{R}$ as left and as right $R$-modules. Ex.: bimodule $A = \hat{R}$.
- $A$ admits a left generating character $\chi$, and $\chi$ is also a right generating character.
- $\alpha \in \mathcal{R}$, $w \in A$ are **bi-invariant** if $\alpha(urv) = \alpha(r)$, $w(uav) = w(a)$ for all $r \in R$, $a \in A$, and units $u, v \in \mathcal{U}$. 
Conditions on \( w \)

- Consider the poset \( \{ aR : a \in A \} \) of all cyclic right \( R \)-submodules of \( A \), under set inclusion.
- Möbius function \( \mu(0,aR) \).
- Suppose \( w \in A_0 \) satisfies

\[
\sum_{aR \subseteq B} w(a)\mu(0,aR) \neq 0, \tag{1}
\]

for all nonzero right \( R \)-submodules \( B \subseteq A \).
Main results

**Theorem**
Suppose $A$ is a Frobenius bimodule over $R$, and suppose $w$ is a bi-invariant weight in $A_0$ satisfying (1), then $A$ has EP with respect to $w$.

**Corollary**
If $R$ is a finite Frobenius ring and $w$ is a bi-invariant weight on $R$ satisfying (1), then $R$ has EP with respect to $w$. 
Fourier transform

- The generating character $\chi$ of $A$ is an element of $A$.
- The map $\mathcal{R} \rightarrow A$, $\alpha \mapsto \chi \ast \alpha$, is a Fourier transform:

  \[(\chi \ast \alpha)(a) = \sum_{r \in R} \chi(ra)\alpha(r).\]

- Invert: $\chi \ast \tilde{w} = w$, where

  \[\tilde{w}(r) = \frac{1}{|A|} \sum_{a \in A} w(a)\chi(-ra).\]
Homogeneous weight

- Recall that the homogeneous weight $w_{\text{Hom}}$ has EP on any Frobenius bimodule.
- Both symmetry groups of $w_{\text{Hom}}$ are maximal: all of $U$.
- Recall that

$$w_{\text{Hom}}(a) = 1 - \frac{1}{|U|} \sum_{u \in U} \chi(ua), \quad a \in A.$$
Inverting $w_{\text{Hom}}$

- Define $\varepsilon \in \mathcal{R}$:

$$
\varepsilon(r) = \begin{cases} 
-\frac{1}{|U|}, & r \in U, \\
1, & r = 0, \\
0, & \text{otherwise}.
\end{cases}
$$

- Then $\chi \ast \varepsilon = w_{\text{Hom}}$:

$$(\chi \ast \varepsilon)(a) = \sum_{r \in \mathcal{R}} \chi(ra)\varepsilon(r) = w_{\text{Hom}}(a).$$
Outline of argument

- Suppose we can find $\gamma \in \mathcal{R}$ such that $\tilde{w} \ast \gamma = \varepsilon$.
- Then $w \ast \gamma = w_{\text{Hom}}$:
  
  $$w \ast \gamma = (\chi \ast \tilde{w}) \ast \gamma = \chi \ast (\tilde{w} \ast \gamma) = \chi \ast \varepsilon = w_{\text{Hom}}.$$  
- Apply earlier result, as $w_{\text{Hom}}$ has EP.
- Condition (1) will allow us to solve $\tilde{w} \ast \gamma = \varepsilon$ for $\gamma$.  

Condition (1)

**Theorem**

*Condition (1) is equivalent to*

\[ \sum_{b \in B} w(b) \chi(b) \neq 0, \quad (2) \]

*for all nonzero right R-submodules \( B \subseteq A \).*
Proof

- Break up into sum over right $\mathcal{U}$-orbits.
- Using results from lecture 7:

\[
\sum_{b \in B} w(b)\chi(b) = \sum_{a\mathcal{U} \subseteq B} \sum_{b \in a\mathcal{U}} w(b)\chi(b) = \sum_{aR \subseteq B} w(a)\mu(0, aR).
\]
Solving $\tilde{w} \ast \gamma = \varepsilon$

- We want to solve $\tilde{w} \ast \gamma = \varepsilon$ for $\gamma$.
- Note that $\tilde{w}$ and $\varepsilon$ are bi-invariant and in $R_0$.
- We want $\gamma$ to be bi-invariant and in $R_0$, too.
- The equation, for any $r \in R$, is
  \[ \sum_{st=r} \tilde{w}(s)\gamma(t) = \varepsilon(r). \]
- Solve recursively, starting with $r \in U$. 
When $r \in \mathcal{U}$

- If $r \in \mathcal{U}$, then $st = r$ implies $s, t \in \mathcal{U}$.
- Using bi-invariance of $\tilde{w}$ and $\gamma$, equation becomes

$$-rac{1}{|\mathcal{U}|} = \sum_{t \in \mathcal{U}} \tilde{w}(rt^{-1})\gamma(t) = |\mathcal{U}|\tilde{w}(1)\gamma(1).$$

- $\tilde{w}(1) \neq 0$ is the case $B = A$ of (2).
- So $\gamma(u) = -1/(|\mathcal{U}|^2\tilde{w}(1))$ for $u \in \mathcal{U}$. 

Using semi-group rings
Recursive step

- Suppose $\gamma$ has been defined to be bi-invariant and to satisfy $\tilde{w} \ast \gamma = \varepsilon$ for some values of $r \in R$.
- Let $r \in R$ be any element, neither zero nor a unit, such that $Rr$ is maximal among principal left ideals of $R$ where $\gamma$ is not defined on $\mathcal{U}r$.
- Consider $(\tilde{w} \ast \gamma)(r) = \varepsilon(r) = 0$. 
Recursive step, part 2

- If $st = r$, then $Rr \subseteq Rt$.
- If $Rr \subsetneq Rt$, then maximality of $Rr$ implies that $\gamma(t)$ is already defined.
- Then $(\tilde{w} \ast \gamma)(r) = 0$ becomes

$$0 = \sum_{st = r \atop Rr \subsetneq Rt} \tilde{w}(s)\gamma(t) + \sum_{st = r \atop Rr = Rt} \tilde{w}(s)\gamma(t).$$
Recursive step, part 3

- Focus on sum with $Rr = Rt$.
- Then $Ur = Ut$, so $t = ur$ for some $u \in U$.
- Thus $r = st = sur$, so that $(su - 1)r = 0$.
- Let $\text{ann}_{lt}(r) = \{q \in R : qr = 0\}$, a left ideal of $R$.
- Then $su - 1 \in \text{ann}_{lt}(r)$.
- Every factorization $st = r$ with $Rr = Rt$ has the form $s = (q + 1)u^{-1}$, $t = ur$, with $u \in U$ and $q \in \text{ann}_{lt}(r)$. 
Using bi-invariance, the sum with $Rr = Rt$ becomes

$$
\sum_{s \cdot t = r, \quad Rr = Rt} \tilde{w}(s) \gamma(t) = \sum_{q \in \text{ann}_{\text{lt}}(r)} \tilde{w}((q + 1)u^{-1})\gamma(ur)
$$

$$
= |U| \gamma(r) \sum_{q \in \text{ann}_{\text{lt}}(r)} \tilde{w}(q + 1)
$$
But $\sum_{q \in \text{ann}_{lt}(r)} \tilde{w}(q + 1)$ simplifies:

$$|A| \sum_{q \in \text{ann}_{lt}(r)} \tilde{w}(q + 1) = \sum_{q \in \text{ann}_{lt}(r)} \sum_{a \in A} w(a) \chi(-(1 + q)a)$$

$$= \sum_{a \in A} w(a) \chi(a) \sum_{q \in \text{ann}_{lt}(r)} \chi(qa).$$

What about $\sum_{q \in \text{ann}_{lt}(r)} \chi(qa)$?
Recursive step, part 6

- \( \sum_{q \in \text{ann}_{lt}(r)} \chi(qa) \) is a sum over the left submodule \( \text{ann}_{lt}(r)a \subseteq A \).

- Since \( \chi \) is a generating character, this sum vanishes unless \( \text{ann}_{lt}(r)a = 0 \). In that case, the sum equals \( |\text{ann}_{lt}(r)| \).

- Set \( B_r = \{ a \in A : \text{ann}_{lt}(r)a = 0 \} \), a right submodule of \( A \). Then

\[
\sum_{q \in \text{ann}_{lt}(r)} \chi(qa) = \begin{cases} 
|\text{ann}_{lt}(r)|, & a \in B_r, \\
0, & a \notin B_r.
\end{cases}
\]
Recursive step, part 7

- Going back to $\sum_{q \in \text{ann}_{lt}(r)} \tilde{w}(q + 1)$, we have

$$|A| \sum_{q \in \text{ann}_{lt}(r)} \tilde{w}(q + 1) = |\text{ann}_{lt}(r)| \sum_{a \in B_r} w(a) \chi(a).$$

- This is nonzero: the $B = B_r$ case of (2). Thus,

$$\gamma(r) = - \left( \sum_{st = r \in Rr \subseteq Rt} \tilde{w}(s) \gamma(t) \right) / \left( |U| \sum_{q \in \text{ann}_{lt}(r)} \tilde{w}(1 + q) \right).$$
Recursive step, part 8

- Check that $\gamma$ is still bi-invariant.
- Continue recursively. Eventually get to case $r = 0$.
- Coefficient of $\gamma(0)$ term vanishes, so we are free to define $\gamma(0)$ so that $\gamma \in R_0$.
- I’ll spare you those details.