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 7, 2018

6. MacWilliams extension theorem

- Extension property (EP)
- EP for Hamming weight over Frobenius bimodules via linear independence of characters
- EP for Hamming weight over Frobenius rings
- Generalization for module alphabets

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

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

Convention

- I will usually write homomorphisms of left modules on the right side: inputs on the left.
- A homomorphism $f : A \to A$ satisfies

$$(a_1 + a_2)f = a_1 f + a_2 f,$$
$$(ra)f = r(af),$$

for $r \in R$ and $a, a_1, a_2 \in A$.

Symmetry groups

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

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

- $\mathcal{U}(R)$ is the group of units of R, and $\mathrm{GL}_R(A)$ is the group of invertible R-linear homomorphisms $A \to A$.

Monomial transformations

- For a subgroup $G \subseteq \mathrm{GL}_R(A)$, a G-**monomial transformation** of A^n is an invertible R-linear homomorphism $T : A^n \to A^n$ of the form

$$(a_1, a_2, \ldots, a_n)T = (a_{\sigma(1)}\phi_1, a_{\sigma(2)}\phi_2, \ldots, a_{\sigma(n)}\phi_n),$$

  for $(a_1, a_2, \ldots, a_n) \in A^n$.
- Here, σ is a permutation of $\{1, 2, \ldots, n\}$ and $\phi_i \in G$ for $i = 1, 2, \ldots, n$.

Isometries

- Let $C_1, C_2 \subseteq A^n$ be two linear codes. An R-linear isomorphism $f : C_1 \to C_2$ is a linear **isometry** with respect to w if $w(xf) = w(x)$ for all $x \in C_1$.
- Every G_{rt}-monomial transformation is an isometry from A^n to itself.

Extension property (EP)

- Given ring R, alphabet A, and weight w on A.
- The alphabet A has the **extension property** (EP) with respect to w if the following holds: For any left linear codes $C_1, C_2 \subseteq A^n$, if $f : C_1 \to C_2$ is a linear isometry, then f extends to a G_{rt}-monomial transformation $A^n \to A^n$.
- That is, there exists a G_{rt}-monomial transformation $T : A^n \to A^n$ such that $xT = xf$ for all $x \in C_1$.

Slightly different point of view

- Linear codes are often presented by generator matrices. A generator matrix serves as a linear encoder from an information space to a message space.
- If $f : C_1 \to C_2$ is a linear isometry, then C_1 and C_2 are isomorphic as R-modules. Let M be a left R-module isomorphic to C_1 and C_2. Call M the **information module**.
- Then C_1 and C_2 are the images of R-linear homomorphisms $\Lambda : M \to A^n$ and $N : M \to A^n$, respectively. We have $N = \Lambda f$: inputs on left!

Coordinate functionals

- C_1 was given by $\Lambda : M \to A^n$. Write the individual components as $\Lambda = (\lambda_1, \ldots, \lambda_n)$, with $\lambda_i \in \mathrm{Hom}_R(M, A)$. Call the λ_i **coordinate functionals**.
- Similarly, $N = (\nu_1, \ldots, \nu_n)$, $\nu_i \in \mathrm{Hom}_R(M, A)$.
- The isometry f extends to a G_{rt}-monomial transformation if there exists a permutation σ and $\phi_i \in G_{\mathrm{rt}}$ such that $\nu_i = \lambda_{\sigma(i)}\phi_i$ for all $i = 1, \ldots, n$.

Case of $\widehat{R}$

- Our first result will show that, for any finite ring R, $A = \widehat{R}$ has EP with respect to the Hamming weight.
- It follows that $A = R$ itself has EP with respect to the Hamming weight when R is Frobenius.
- The Frobenius ring case came first (1999).
- The more general $A = \widehat{R}$ case is due to Greferath, Nechaev, and Wisbauer (2004).

Techniques

- For any alphabet A, the summation formulas for characters imply that the Hamming weight wt satisfies

$$\mathrm{wt}(a) = 1 - \frac{1}{|A|} \sum_{\pi \in \widehat{A}} \pi(a), \quad a \in A.$$

- Characters (in multiplicative form) are linearly independent functions on A over $\mathbb{C}$ (Lecture 9).
- Recursive argument using maximal elements in a finite poset.

Symmetry groups for the Hamming weight

- Consider the Hamming weight wt on $A = \widehat{R}$, which is an (R, R)-bimodule.
- Both symmetry groups G_{lt} and G_{rt} equal $\mathcal{U}(R)$.

Posets

- Given a set S, a (non-strict) **partial order** $\preceq$ on S is reflexive, antisymmetric, and transitive. The pair $(S, \preceq)$ is a **partially ordered set** or **poset**.
- Example. Let X be a nonempty set. Then $S = \mathcal{P}(X)$, the set of all subsets of X, is a poset under set inclusion, i.e., $U \preceq V$ when $U \subseteq V$.

Poset of cyclic submodules

- Example. Let B be a finite right R-module. Then $S = \{bR : b \in B\}$ is the poset of all cyclic right R-submodules of B under set inclusion.
- Fact: For finite rings R, $b_1R = b_2R$ if and only if $b_1 = b_2u$, where $u \in \mathcal{U}(R)$.
- This fact uses of work of Bass on rings of stable range one.

Proof of EP for $A = \widehat{R}$ (i)

- Same set up as before: ring R, alphabet $A = \widehat{R}$, with Hamming weight.
- $C_1, C_2 \subseteq \widehat{R}^n$, with $f : C_1 \to C_2$ linear isometry.
- C_1 is image of $\Lambda : M \to \widehat{R}^n$; C_2 is image of $N : M \to \widehat{R}^n$. $N = \Lambda f$.
- Isometry: $\mathrm{wt}(x\Lambda) = \mathrm{wt}(xN)$, for all $x \in M$.

Proof (ii)

- Remember, $A = \widehat{R}$.
- A has a left generating character: $\rho : A \to \mathbb{C}$, $\rho(\pi) = \pi(1)$ for $\pi \in \widehat{R}$. (Evaluate at $1 \in R$.)
- Every character of A (element of $\widehat{A}$) has the form ${}^r\rho$ for some unique $r \in R$.
- Recall: $({}^r\rho)(a) = \rho(ar)$.

Proof (iii)

- Hamming weight as character sum:

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

- That is,

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

- This is an equation of characters on M.

Proof (iv)

- Let $B = \mathrm{Hom}_R(M, A)$, a right R-module. Poset $S = \{\lambda R : \lambda \in \mathrm{Hom}_R(M, A)\}$ under $\subseteq$.
- Among the $\lambda_i R, \nu_j R$, choose one that is maximal for $\subseteq$. Say, $\nu_1 R$.
- Let $j = 1$ and $s = 1$ on the right side of the character equation:

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

Proof (v)

- Let $j = 1$ and $s = 1$ on the right side of the character equation:

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

- By linear independence of characters, there exists i_1 and $r \in R$ so that $\rho(x\lambda_{i_1} r) = \rho(x\nu_1)$ for all $x \in M$.
- Thus $\rho(x(\nu_1 - \lambda_{i_1} r)) = 1$ for all $x \in M$.
- That is, $M(\nu_1 - \lambda_{i_1} r) \subseteq \ker \rho$.

Proof (vi)

- We had $M(\nu_1 - \lambda_{i_1} r) \subseteq \ker \rho$.
- $M(\nu_1 - \lambda_{i_1} r)$ is a left R-module.
- Because ρ a generating character, $\nu_1 = \lambda_{i_1} r$.
- Thus, $\nu_1 \in \lambda_{i_1} R$ and $\nu_1 R \subseteq \lambda_{i_1} R$.
- By maximality of $\nu_1 R$, $\nu_1 R = \lambda_{i_1} R$.
- Thus, $\nu_1 = \lambda_{i_1} u_1$, for some $u_1 \in \mathcal{U}(R)$.

Proof (vii)

- Recall,

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

- Then inner sums agree:
  $\sum_{r\in R}\rho(x\lambda_{i_1}r)=\sum_{s\in R}\rho(x\nu_1 s)$, $x\in M$.
- Set $\sigma(1)=i_1$. Subtract inner sums to reduce the size of the outer sums by 1. Proceed by induction.

Slightly more general result

- The exact same proof applies to a **Frobenius bimodule**, a bimodule A over R such that A is isomorphic to $\widehat{R}$ as left R-modules and as right R-modules (but not necessarily isomorphic as bimodules).

Generalize to module alphabets

- For ring R, alphabet A, and Hamming weight wt, EP holds if A: (1) is pseudo-injective and (2) has a cyclic socle (embeds into $\widehat{R}$).
- **Pseudo-injective** means injective with respect to submodules. That is, if B is a submodule of A and $h : B \to A$ is any injective module homomorphism, then h extends to injective $\tilde{h} : A \to A$.

EP for linear codes of length 1

- Dinh, López-Permouth: EP for linear codes over A of length 1 is equivalent to A being pseudo-injective.
- A linear code of length 1 is a submodule C of A.
- Any injection $C \hookrightarrow A$ preserves Hamming weight.
- EP reduces to the algebraic question of whether an injection of a submodule always extends to all of A: pseudo-injectivity.

EP for Hamming weight over module alphabets

Theorem

Suppose a left R-module A is pseudo-injective and has a cyclic socle. Then A has EP with respect to the Hamming weight.

- Because $\mathrm{Soc}(A)$ is cyclic, A embeds into $\widehat{R}$.

Proof (i)

- Suppose $C_1, C_2 \subset A^n$ are R-linear codes with isomorphism $f : C_1 \to C_2$ that preserves the Hamming weight on A^n.
- Via $A \hookrightarrow \widehat{R}$, view $C_1, C_2 \subseteq \widehat{R}^n$.
- The Hamming weight of $x \in A^n \subseteq \widehat{R}^n$ is the same, whether x is considered as an element of A^n or as an element of $\widehat{R}^n$.
- So, $C_1, C_2 \subseteq \widehat{R}^n$, with $f : C_1 \to C_2$ preserving the Hamming weight from $\widehat{R}^n$.

Proof (ii)

- $\widehat{R}$ has EP with respect to Hamming weight.
- So $f : C_1 \to C_2$ extends to a monomial transformation F of $\widehat{R}^n$.
- Write $(x_1, \ldots, x_n)F = (x_{\sigma(1)}u_1, \ldots, x_{\sigma(n)}u_n)$, for $(x_1, \ldots, x_n) \in \widehat{R}^n$, where σ is a permutation of $\{1, 2, \ldots, n\}$ and $u_i \in \mathcal{U}(R) = \mathrm{Aut}({}_R\widehat{R})$.
- Does u_i map A back to A? No way to tell.
- Write $F = PD$, where P is the permutation part and D is the diagonal part.

Proof (iii)

- Set $C_3 = C_1 P \subseteq A^n \subseteq \widehat{R}^n$.
- Then D maps $C_3 \to C_2$ and preserves Hamming weight.
- Look at individual components of D.
- For $i = 1, \ldots, n$, project C_3, C_2 to the ith entry, $C_3^{(i)}, C_2^{(i)} \subseteq A \subseteq \widehat{R}$.
- Define $D^{(i)}$ by $xD^{(i)} = xu_i$, $x \in \widehat{R}$. Then $D^{(i)}$ maps $C_3^{(i)} \to C_2^{(i)}$ and preserves the Hamming weight.

Proof (iv)

- Recall, $C_3^{(i)}, C_2^{(i)} \subseteq A$ and $D^{(i)}$ maps $C_3^{(i)} \to C_2^{(i)}$ injectively. In particular, $D^{(i)} : C_3^{(i)} \hookrightarrow A$.
- Because A is pseudo-injective, $D^{(i)}$ extends to an automorphism $\tau_i \in \mathrm{Aut}({}_R A)$.
- Then F', defined by $(x_1, \ldots, x_n)F' = (x_{\sigma(1)}\tau_1, \ldots, x_{\sigma(n)}\tau_n)$, is a monomial transformation of A^n extending f.

What is coming next?

- Converses!
- If a ring alphabet R has EP with respect to the Hamming weight, then R is Frobenius.
- If a module alphabet A has EP with respect to the Hamming weight, then A is pseudo-injective and has a cyclic socle.