Linear codes over finite rings and modules: The MacWilliams extension theorem over Frobenius rings

Jay A. Wood

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

Coding Theory Seminar
Eastern Kentucky University
March 5, 2013 (Emily is 20 (!))

Code equivalence

- When should two linear codes be considered to be equivalent?
- One way: when there exists a monomial transformation taking one code to the other.
- Another way: when there is a weight-preserving isomorphism between them.
- MacWilliams, 1961-62: these notions are the same.
- Every weight-preserving isomorphism between codes can be extended to a monomial transformation.

Definitions

- Let R be a finite ring with 1.
- Let $\mathrm{wt}(x)$ be the *Hamming weight* of $x \in R^n$: $\mathrm{wt}(x) = |\{i : x_i \neq 0\}|$.
- A *linear code* of length n over R is a left R-submodule $C \subset R^n$.
- A homomorphism $f : C_1 \to C_2$ *preserves Hamming weight* if $\mathrm{wt}(f(x)) = \mathrm{wt}(x)$ for all $x \in C_1$.

Monomial transformations

- A *monomial transformation* $T : R^n \to R^n$ has the form

$$T(x_1, \ldots, x_n) = (x_{\sigma(1)}u_1, \ldots, x_{\sigma(n)}u_n),$$

  for some permutation σ of $\{1, \ldots, n\}$ and units (invertible elements) $u_i \in R$.
- Any monomial transformation is a left R-linear homomorphism that preserves Hamming weight.

MacWilliams Extension Theorem (1961/62)

- Assume $C_1, C_2 \subset \mathbb{F}_q^n$ are linear codes.
- If $f : C_1 \longrightarrow C_2$ is a linear isomorphism that preserves Hamming weight, then f extends to a monomial transformation of $\mathbb{F}_q^n$.

Can this be generalized?

- For linear codes defined over a finite ring R, the extension theorem for Hamming weight holds if and only if R is Frobenius.
- Greferath-Schmidt: the extension theorem holds over Frobenius rings for the homogeneous weight.
- Greferath-Nechaev-Wisbauer: the extension theorem holds for module alphabets $A = \widehat{R}$ (for any finite ring R) for the homogeneous weight.
- It is possible to characterize the module alphabets for which the extension theorem holds (for either Hamming or homogeneous weights).

Why Frobenius?

- There are character-theoretic proofs over finite fields that use the crucial property $\widehat{\mathbb{F}_q} \cong \mathbb{F}_q$.
- Frobenius rings satisfy $\widehat{R} \cong R$, and the same proofs will work.
- For weights other than Hamming or homogeneous: that's Wednesday's talk.

MacWilliams Extension Theorem over Finite Frobenius Rings

Theorem (1999)

Let R be a finite Frobenius ring, and suppose $C_1, C_2 \subset R^n$ are left linear codes. If $f : C_1 \rightarrow C_2$ is an R-linear isomorphism that preserves Hamming weight, then f extends to a monomial transformation of R^n.

Character-Theoretic Proof (a)

- The proof follows a proof of Ward and Wood in the finite field case (1996).
- View C_i as the image of $\Lambda_i : M \longrightarrow R^n$, with $\Lambda_i = (\lambda_{i,1}, \ldots, \lambda_{i,n})$ and $\Lambda_2 = f \circ \Lambda_1$.
- Using character sums, express Hamming weight as:

$$\mathrm{wt}(\Lambda_i(x)) = n - \sum_{j=1}^{n} \frac{1}{|R|} \sum_{\pi \in \widehat{R}} \pi(\lambda_{i,j}(x)), x \in M.$$

Character-Theoretic Proof (b)

- Because f preserves Hamming weight, we get

$$\sum_{j=1}^{n} \sum_{\pi \in \widehat{R}} \pi(\lambda_{1,j}(x)) = \sum_{k=1}^{n} \sum_{\psi \in \widehat{R}} \psi(\lambda_{2,k}(x)), x \in M.$$

- In a Frobenius ring, $\widehat{R} \cong R$. There is a character ρ such that every character of R has the form ${}^{a}\rho$, $a \in R$.
- $({}^{a}\rho)(r) := \rho(ra)$, $r \in R$.

Character-Theoretic Proof (c)

- Re-write weight-preservation equation as

$$\sum_{j=1}^{n}\sum_{a\in R}({}^{a}\rho)(\lambda_{1,j}(x)) = \sum_{k=1}^{n}\sum_{b\in R}({}^{b}\rho)(\lambda_{2,k}(x)), x \in M.$$

- Or as

$$\sum_{j=1}^{n}\sum_{a\in R}\rho(\lambda_{1,j}(x)a) = \sum_{k=1}^{n}\sum_{b\in R}\rho(\lambda_{2,k}(x)b), x \in M.$$

Character-Theoretic Proof (d)

- The last equation is an equation of characters on M.
- Characters are linearly independent, so one can match up terms (carefully).
- A technical argument involving a preordering given by divisibility in R shows how to match up terms with units as multipliers.
- This produces a permutation σ and units u_i in R such that $\lambda_{2,k} = \lambda_{1,\sigma(k)} u_k$, as desired.

Module alphabets

- Essentially the same proof works for the alphabet $A = \widehat{R}$.
- Use ρ equal to evaluation at $1 \in R$.
- Can then use the $A = \widehat{R}$ result to prove the extension theorem for any alphabet A such that A is a (pseudo-injective) left R-module with $A \subset \widehat{R}$.

Converse?

- Suppose R is a finite ring for which the extension theorem holds.
- Must R be Frobenius? Yes!
- We will ultimately follow a strategy of Dinh and López-Permouth.
- First we will generalize an approach due to MacWilliams, Bogart, Goldberg, and Gordon in order to re-formulate the extension problem.
- Will use R-linear codes over an alphabet A.

Monomial Transformations

- R finite ring, A finite left R-module.
- Recall, a *linear code* over A is a left R-submodule $C \subset A^n$.
- A *monomial transformation* $T : A^n \to A^n$ has the form

$$T(x_1, \ldots, x_n) = (x_{\sigma(1)}\phi_1, \ldots, x_{\sigma(n)}\phi_n),$$

for $(x_1, \ldots, x_n) \in A^n$, where σ is a permutation of $\{1, \ldots, n\}$ and $\phi_1, \ldots, \phi_n \in \mathrm{Aut}(A)$.

Re-Formulation of Extension Problem (a)

- Approach inspired by Assmus and Mattson, 1963.
- View a left R-linear code $C \subset A^n$ as the image of an R-linear homomorphism $\Lambda : M \to A^n$, where $\Lambda = (\lambda_1, \ldots, \lambda_n)$ and $\lambda_i : M \to A$ are R-linear.
- Up to monomial equivalence, what matters is the number of λ_i's in a given scale class (under right action by automorphisms of A).
- The group $\mathrm{Aut}(A)$ of R-automorphisms of A acts on the right on the group $\mathrm{Hom}_R(M, A)$ of R-linear homomorphisms from M to A.

Re-Formulation of Extension Problem (b)

- Let $\mathcal{O}^\sharp$ be the set of nonzero orbits of the action of $\mathrm{Aut}(A)$ on $\mathrm{Hom}_R(M, A)$.
- Let $\eta : \mathcal{O}^\sharp \to \mathbb{N}$ be the *multiplicity function* that counts how many of the λ_i belong to each scale class.
- Functions equivalent to η have appeared elsewhere under various names (value function, multiset, etc.).

Re-Formulation of Extension Problem (c)

- Summary, so far: the monomial equivalence class of $\Lambda : M \longrightarrow A^n$ is encoded by its multiplicity function $\eta : \mathcal{O}^\sharp \to \mathbb{N}$.

Re-Formulation of Extension Problem (d)

- Now, turn to Hamming weights.
- Note that the Hamming weight depends only on the left scale class of $x \in M$ via units of R:

$$\mathrm{wt}(\Lambda(ux)) = \mathrm{wt}(u\Lambda(x)) = \mathrm{wt}(\Lambda(x)), x \in M, u \in \mathcal{U}.$$

- Let $\mathcal{O}$ be the set of nonzero orbits of the left action of the group of units $\mathcal{U}$ on M.

Re-Formulation of Extension Problem (e)

- The Hamming weight $\mathrm{wt}(\Lambda(x))$ depends only on the scale classes of the λ_i ($\phi_i \in \mathrm{Aut}(A)$):

$$\mathrm{wt}(\Lambda(x)) = \sum_{i=1}^{n} \mathrm{wt}(\lambda_i(x)) = \sum_{i=1}^{n} \mathrm{wt}(\lambda_i(x)\phi_i).$$

- The Hamming weight does not depend on the order of the λ_i.

Re-Formulation of Extension Problem (f)

- Let $F(\mathcal{O}^\sharp, \mathbb{N})$ denote the set of all functions from $\mathcal{O}^\sharp$ to $\mathbb{N}$. Similarly for $F(\mathcal{O}, \mathbb{N})$.
- The Hamming weight gives a well-defined map $W : F(\mathcal{O}^\sharp, \mathbb{N}) \to F(\mathcal{O}, \mathbb{N})$:

$$W(\eta)(x) = \sum_{\lambda \in \mathcal{O}^\sharp} \eta(\lambda)\, \mathrm{wt}(\lambda(x)).$$

- Summary: the Extension Theorem holds iff the map W is injective for every finite module M.

Re-Formulation of Extension Problem (g)

- By formally allowing rational coefficients (tensoring with $\mathbb{Q}$), we get

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

- W is a linear transformation of $\mathbb{Q}$-vector spaces.
- The Extension Theorem holds iff the map W is injective for every finite module M.

Example: Linear One-Weight Codes

- A linear code $C \subset A^n$ is a *one-weight code* if every nonzero element $x \in C$ has the same weight.
- Theorem. If one-weight codes exist at all, they are unique up to replication.
- Proof: The constant functions form a one-dimensional subspace of $F(\mathcal{O}, \mathbb{Q})$. Pull back under W.
- Example: Over $\mathbb{F}_q$, use every scale class of columns exactly once (simplex code).

A Counter-Example to Extension (a)

- For R-linear codes defined over a module A, the extension theorem might not hold.
- Let $R = M_m(\mathbb{F}_q)$, the ring of $m \times m$ matrices over $\mathbb{F}_q$. The group of units is $\mathcal{U} = GL(m, \mathbb{F}_q)$.
- Let $A = M_{m,k}(\mathbb{F}_q)$, the space of all $m \times k$ matrices. A is a left R-module. $\mathrm{Aut}(A) = GL(k, \mathbb{F}_q)$.
- Assume $m < k$.

A Counter-Example to Extension (b)

- A general left R-module has the form $M = M_{m,j}(\mathbb{F}_q)$. Then $Hom_R(M, A) = M_{j,k}(\mathbb{F}_q)$ (via right matrix multiplication).
- Left action of $\mathcal{U} = GL(m, \mathbb{F}_q)$ on $M = M_{m,j}(\mathbb{F}_q)$: orbits $\mathcal{O}$ consist of row reduced echelon matrices of size $m \times j$.
- Right action of $\mathrm{Aut}(A) = GL(k, \mathbb{F}_q)$ on $Hom_R(M, A) = M_{j,k}(\mathbb{F}_q)$: orbits $\mathcal{O}^\sharp$ consist of column reduced echelon matrices of size $j \times k$.

A Counter-Example to Extension (c)

- In $W : F(\mathcal{O}^\sharp, \mathbb{Q}) \to F(\mathcal{O}, \mathbb{Q})$, the dimensions over $\mathbb{Q}$ of the domain and range equal the number of elements in $\mathcal{O}^\sharp$ and $\mathcal{O}$, respectively.
- $\dim_{\mathbb{Q}} F(\mathcal{O}^\sharp, \mathbb{Q})$ equals the number of column reduced echelon matrices of size $j \times k$.
- $\dim_{\mathbb{Q}} F(\mathcal{O}, \mathbb{Q})$ equals the number of row reduced echelon matrices of size $m \times j$.
- Since $k > m$, $\dim_{\mathbb{Q}} F(\mathcal{O}^\sharp, \mathbb{Q}) > \dim_{\mathbb{Q}} F(\mathcal{O}, \mathbb{Q})$, and W is not injective.

Form of Counter-Examples (a)

- Let $M = A = M_{m,k}(\mathbb{F}_q)$. We will define two homomorphisms $\Lambda_\pm : M \to A^n$, where $n = \prod_{i=1}^{k-1}(1 + q^i)$.
- Start by defining two vectors $v_\pm \subset M_k(\mathbb{F}_q)^n$.
- Vector v_+ consists of all $k \times k$ column reduced echelon matrices of even rank, appearing with multiplicity $q^{\binom{r}{2}}$, where r is the (even) rank.
- Vector v_- does the same, but with odd rank.

Form of Counter-Examples (b)

- Define $\Lambda_{\pm} : M \longrightarrow A^n$ by $\Lambda_{\pm}(X) = Xv_{\pm}$ (matrix multiplication), for $X \in M$.
- A somewhat involved calculation shows that $\mathrm{wt}(\Lambda_{+}(X)) = \mathrm{wt}(\Lambda_{-}(X))$ for all $X \in M$.
- There cannot be a monomial transformation between them because $\Lambda_{+}(X)$ always has a fixed zero entry (coming from the zero matrix, which has even rank). But $\Lambda_{-}(X)$ never has a consistent zero entry.

Explicit Counter-Examples (a)

- $R = M_1(\mathbb{F}_q) = \mathbb{F}_q$, $A = M_{1,2}(\mathbb{F}_q)$. Remember that Hamming weight depends on elements being nonzero in A (nonzero as a pair).
- For $q = 2$, $n = 3$:

$$\begin{array}{cc} C_+ & C_- \\ (00, 00, 00) & (00, 00, 00) \\ (00, 10, 10) & (10, 10, 00) \\ (00, 01, 01) & (00, 10, 10) \\ (00, 11, 11) & (10, 00, 10) \end{array}$$

Explicit Counter-Examples (b)

- For $q = 3$, $n = 4$:

C_+	C_-
$(00, 00, 00, 00)$	$(00, 00, 00, 00)$
$(00, 01, 01, 01)$	$(00, 10, 20, 10)$
$(00, 02, 02, 02)$	$(00, 20, 10, 20)$
$(00, 10, 10, 10)$	$(10, 10, 10, 00)$
$(00, 11, 11, 11)$	$(10, 20, 00, 10)$
$(00, 12, 12, 12)$	$(10, 00, 20, 20)$
$(00, 20, 20, 20)$	$(20, 20, 20, 00)$
$(00, 21, 21, 21)$	$(20, 00, 10, 10)$
$(00, 22, 22, 22)$	$(20, 10, 00, 20)$

Characterizing Finite Frobenius Rings

- Theorem (2008). Suppose R is a finite ring, and set $A = R$. If the extension theorem holds for linear codes over R, then R is a Frobenius ring.
- Dinh and López-Permouth (2004–2005) proved some special cases and developed a strategy to prove the general result.

The Strategy of Dinh and López-Permouth

- Every non-Frobenius ring has a copy of some $M_{m,k}(\mathbb{F}_q) \subset \mathrm{Soc}(R)$, with $m < k$.
- The extension theorem fails for $M_{m,k}(\mathbb{F}_q) \subset \mathrm{Soc}(R)$, with $m < k$ (as a module over $M_m(\mathbb{F}_q)$).
- View the $M_{m,k}(\mathbb{F}_q)$ counter-examples as modules (and hence counter-examples) over R itself.

Structure of a Finite Ring

- Let R be a finite ring with 1.
- $R/\operatorname{Rad}(R)$ is a sum of simple rings, which must be matrix rings over finite fields:

$$R/\operatorname{Rad}(R) \cong \bigoplus M_{m_i}(\mathbb{F}_{q_i}).$$

- $\operatorname{Soc}({}_R R)$ is a left module over $R/\operatorname{Rad}(R)$, so

$$\operatorname{Soc}({}_R R) \cong \bigoplus M_{m_i,k_i}(\mathbb{F}_{q_i}).$$

Frobenius Rings

- Remember that a finite ring is Frobenius if $R/\operatorname{Rad}(R)$ is isomorphic to $\operatorname{Soc}(R)$ as one-sided modules (so $k_i = m_i$).
- In a non-Frobenius ring, there exist $k_i \neq m_i$, with some larger and some smaller.
- These provide the counter-examples to the extension theorem.

Additional Comments (a)

- One can characterize the alphabets A for which the extension theorem for Hamming weight holds: $A \subset \widehat{R}$ plus one more condition (pseudo-injective).
- In particular, $A = \widehat{R}$ always satisfies the extension theorem (for any finite ring R, Frobenius or not). This is a theorem of Greferath, Nechaev, Wisbauer (2004) that extends the original Frobenius result.

Additional Comments (b)

- Some results are known for other weight functions, especially the homogenous weight (again, by Greferath, Nechaev, Wisbauer).
- But, there is much that is not known about other weight functions. For example, it is not known if the extension theorem is always true for the Lee weight over $R = \mathbb{Z}/n\mathbb{Z}$ for all n. (More tomorrow.)
- Are there other uses of $W : F(\mathcal{O}^\sharp, \mathbb{Q}) \to F(\mathcal{O}, \mathbb{Q})$?