

Two Fundamental Theorems of MacWilliams: The MacWilliams Extension Theorem over Finite Rings

Jay A. Wood

Department of Mathematics
Western Michigan University
<http://homepages.wmich.edu/~jwood/>

Huazhong Normal University, Wuhan, Hubei
July 2, 2011

The MacWilliams Extension Theorem

- ▶ Suppose $C_1, C_2 \subset \mathbb{F}_q^n$ are two linear codes. If $f : C_1 \rightarrow C_2$ is a linear isomorphism that preserves Hamming weight, then f extends to a monomial transformation of \mathbb{F}_q^n .
- ▶ Generalize to finite Frobenius rings (1999).
- ▶ Conversely, if the extension property holds over a finite ring R , then R is Frobenius (2008).

Linear Codes via Functionals

- ▶ Let R be a finite ring.
- ▶ View a linear code $C \subset R^n$ as the image of an R -linear homomorphism $\lambda : M \rightarrow R^n$, where M is a left R -module and $\lambda = (\lambda_1, \dots, \lambda_n)$, with $\lambda_j : M \rightarrow R$ being linear functionals.

Extension Theorem over a Frobenius Ring

- ▶ Let R be a finite Frobenius ring. Suppose $C_1, C_2 \subset R^n$ are two 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 .
- ▶ Over R , monomial transformations have the form

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

$(x_1, \dots, x_n) \in R^n$, for some permutation σ of $\{1, \dots, n\}$ and units (invertible elements) $u_i \in R$.

Character-Theoretic Proof (a)

- ▶ View C_i as the image of $\lambda_i : M \rightarrow R^n$, with $\lambda_i = (\lambda_{i,1}, \dots, \lambda_{i,n})$ and $\lambda_2 = f \circ \lambda_1$.
- ▶ Using character sums, express Hamming weight as:

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

Character-Theoretic Proof (b)

- ▶ Because f preserves Hamming weight, we get

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

- ▶ In a Frobenius ring, there is a generating character χ . Every character of R has the form $a\chi$, $a \in R$.
- ▶ $(a\chi)(r) := \chi(ra)$, $r \in R$.

Character-Theoretic Proof (c)

- ▶ Re-write weight-preservation equation as

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

- ▶ Or as

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

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 partial ordering 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.

Re-Write the Extension Problem

- ▶ The character-theoretic proof given above generalized the Ward-Wood proof over finite fields.
- ▶ Now we will generalize the MacWilliams, Bogart, et al. approach in order to re-formulate the extension problem.
- ▶ Will use R -linear codes over an alphabet A .

Re-Formulation of Extension Problem (a)

- ▶ View a left R -linear code $C \subset A^n$ as the image of an R -linear homomorphism $\lambda : M \rightarrow A^n$, where $\lambda = (\lambda_1, \dots, \lambda_n)$ and $\lambda_i : M \rightarrow A$ 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 $\text{Aut}(A)$ of R -automorphisms of A acts on the right on the group $\text{Hom}_R(M, A)$ of R -linear homomorphisms from M to A .

Re-Formulation of Extension Problem (b)

- ▶ Let \mathcal{O}^\sharp be the set of orbits of the action of $\text{Aut}(A)$ on $\text{Hom}_R(M, A)$.
- ▶ Let $\eta : \mathcal{O}^\sharp \rightarrow \mathbb{N}$ 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 $\lambda : M \rightarrow A^n$ is encoded by its multiplicity function $\eta : \mathcal{O}^\# \rightarrow \mathbb{N}$.

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 :

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

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

Re-Formulation of Extension Problem (e)

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

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

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

Re-Formulation of Extension Problem (f)

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

$$W(\eta)(x) = \sum_{\lambda \in \mathcal{O}^\#} \eta(\lambda) \text{wt}(\lambda(x)).$$

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

Re-Formulation of Extension Problem (g)

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

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

- ▶ W is a linear transformation of \mathbb{Q} -vector spaces.
- ▶ The Extension Theorem holds iff the map W is injective for every 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.
- ▶ Example: Over \mathbb{F}_q , use every scale class of columns exactly once (simplex code).
- ▶ Proof: One-weight codes form a one-dimensional subspace of $F(\mathcal{O}, \mathbb{Q})$. Pull back under W .

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. $\text{Aut}(A) = GL(k, \mathbb{F}_q)$.
- ▶ 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 $\text{Hom}_R(M, A) = M_{j,k}(\mathbb{F}_q)$ (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 $\text{Aut}(A) = GL(k, \mathbb{F}_q)$ on $\text{Hom}_R(M, A) = M_{j,k}(\mathbb{F}_q)$: orbits $\mathcal{O}^\#$ consist of column reduced echelon matrices of size $j \times k$.

A Counter-Example to Extension (c)

- ▶ In $W : F(\mathcal{O}^\sharp, \mathbb{Q}) \rightarrow F(\mathcal{O}, \mathbb{Q})$, 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 $\lambda_{\pm} : M \rightarrow A^n$, 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 $\lambda_{\pm} : M \rightarrow A^n$ by $\lambda_{\pm}(X) = Xv_{\pm}$ (matrix multiplication), for $X \in M$.
- ▶ A somewhat involved calculation shows that $\text{wt}(\lambda_+(X)) = \text{wt}(\lambda_-(X))$ 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 $q = 2$, $n = 3$:

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)

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 $M_{m,k}(\mathbb{F}_q) \subset \text{Soc}(R)$, with $m < k$.
- ▶ The extension theorem fails for $M_{m,k}(\mathbb{F}_q) \subset \text{Soc}(R)$, 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.
- ▶ $R/\text{Rad}(R)$ is a sum of simple rings, which must be matrix rings over finite fields:

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

- ▶ $\text{Soc}(R)$ is a module over $R/\text{Rad}(R)$, so

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

Frobenius Rings

- ▶ Remember that a finite ring is Frobenius if $R/\text{Rad}(R)$ is isomorphic to $\text{Soc}(R)$ 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 alphabets A for which the extension theorem holds: $A \subset \widehat{R}$ plus one more condition.
- ▶ 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 .
- ▶ Are there other uses of $W : F(\mathcal{O}^\#, \mathbb{Q}) \rightarrow F(\mathcal{O}, \mathbb{Q})$?

References

- ▶ These slides and other papers are available on the web: <http://homepages.wmich.edu/~jwood>
- ▶ Many references in the paper “Foundations of Linear Codes ... ”

Thank You

- ▶ I thank again my host Professor Hongwei Liu.
- ▶ I thank you, the audience members, for your kind attention.
- ▶ Have a good summer break!