Equivalence of codes: necessary conditions

Jay A. Wood

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

Algebra for Secure and Reliable Communications Modeling
Morelia, Michoacán, Mexico
October 13, 2012

Introduction

- In this lecture we show that if the extension property is satisfied for linear codes over a finite ring R with respect to the Hamming weight, then the ring is Frobenius.
- We will follow a strategy due to Dinh and López-Permouth, 2004.
- We will use the re-formulation of the extension property as the injectivity of the weight mapping $W : F(\mathcal{O}^\sharp, \mathbb{N}) \to F(M, \mathbb{C})$:

$$\eta \mapsto (m \mapsto \sum_{[\lambda] \in \mathcal{O}^\sharp} w(m\lambda)\eta([\lambda])).$$

The strategy of Dinh and López-Permouth

- Prove the contrapositive as follows.
  1. If R is not Frobenius, then $\mathrm{Soc}(R)$ contains a matrix module of the form $M_{n\times k}(\mathbb{F}_q)$, with $n < k$.
  2. Use $A = M_{n\times k}(\mathbb{F}_q)$ as alphabet, and show that the extension property fails for this alphabet.
  3. Show that the counterexamples for A are also counterexamples for R.
- Dinh and López-Permouth proved 1 and 3. They proved 2 is certain special cases.

Socle condition

- We saw in an earlier lecture that matrix rings $M_n(\mathbb{F}_q)$ admit a generating character $\rho = \theta_q \circ \mathrm{Tr}$.
- By restriction, any left $M_n(\mathbb{F}_q)$-module of the form $M_{n\times k}(\mathbb{F}_q)$ with $n \geq k$ admits a generating character. Include $M_{n\times k}(\mathbb{F}_q)$ inside $M_n(\mathbb{F}_q)$ as the first k columns, and restrict ρ to $M_{n\times k}(\mathbb{F}_q)$.
- Any ring R having $\mathrm{Soc}(R) \cong \oplus M_{n_i\times k_i}(\mathbb{F}_{q_i})$ with all $n_i \geq k_i$ is Frobenius. Because $\mathrm{Soc}(R)$ admits a generating character θ, θ extends to a generating character on R. Thus R is Frobenius.

The weight mapping again

- The weight mapping is $W : F(\mathcal{O}^\sharp, \mathbb{N}) \to F(M, \mathbb{C})$:

$$\eta \mapsto (m \mapsto \sum_{[\lambda] \in \mathcal{O}^\sharp} w(m\lambda)\eta([\lambda])).$$

- If $u \in G_l$, then $W(\eta)(um) = W(\eta)(m)$, all $m \in M$.
- Thus the image of W lies inside $F(M, \mathbb{C})^{G_l}$, the vector space of G_l-invariant functions on M. This space can be identified with $F(\mathcal{O}, \mathbb{C})$, the functions on the set $\mathcal{O}$ of all the G_l-scale classes of M.

And again

- Suppose w has values in $\mathbb{Q}$, which happens for the Hamming, Lee, Euclidean, homogeneous weights.
- Then $W : F(\mathcal{O}^\sharp, \mathbb{N}) \to F(\mathcal{O}, \mathbb{Q})$.
- By tensoring with $\mathbb{Q}$ (formally allowing η to take rational values), we get a linear transformation of $\mathbb{Q}$-vector spaces:

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

- The $\mathbb{Q}$-version of W is injective iff the $\mathbb{N}$-version is injective. Now we can use linear algebra over $\mathbb{Q}$.

Alphabet $M_{n\times k}(\mathbb{F}_q)$, $n < k$

- Let $R = M_n(\mathbb{F}_q)$ and alphabet $A = M_{n\times k}(\mathbb{F}_q)$, a left R-module. We use the Hamming weight wt on A.
- For the Hamming weight, the symmetry groups are $G_l = \mathcal{U}(R) = GL_n(\mathbb{F}_q)$, the group of invertible matrices of size $n \times n$, and $G_r = \mathrm{Aut}(A) = GL_k(\mathbb{F}_q)$ (under right matrix multiplication).
- We examine the weight mapping $W : F(\mathcal{O}^\sharp, \mathbb{Q}) \to F(\mathcal{O}, \mathbb{Q})$ in detail for a left R-module M.

Analysis of W mapping: $\mathcal{O}$

- Any left R-module has the form $M = M_{n \times t}(\mathbb{F}_q)$.
- $\mathcal{O}$ is the set of $G_l = GL_n(\mathbb{F}_q)$ scale classes of M.
- Classes in $\mathcal{O}$ are represented by row-reduced echelon matrices of size $n \times t$.

Analysis of W mapping: $\mathcal{O}^\sharp$

- $\mathrm{Hom}_R(M, A) = M_{t\times k}(\mathbb{F}_q)$ (under right matrix multiplication).
- $\mathcal{O}^\sharp$ is the set of (right) $G_r = GL_k(\mathbb{F}_q)$ scale classes of $\mathrm{Hom}_R(M, A)$.
- Classes in $\mathcal{O}^\sharp$ are represented by column-reduced echelon matrices of size $t \times k$.

Analysis of W mapping: dimensions

- For any finite set S, $\dim_{\mathbb{Q}} F(S, \mathbb{Q}) = |S|$.
- Then $\dim_{\mathbb{Q}} F(\mathcal{O}^\sharp, \mathbb{Q}) = |\mathcal{O}^\sharp|$, which equals the number of column-reduced echelon matrices of size $t \times k$.
- Similarly, $\dim_{\mathbb{Q}} F(\mathcal{O}, \mathbb{Q}) = |\mathcal{O}|$, which equals the number of row-reduced echelon matrices of size $n \times t$.
- Because $n < k$ (by hypothesis), $|\mathcal{O}^\sharp| > |\mathcal{O}|$.
- Thus, $\dim_{\mathbb{Q}} F(\mathcal{O}^\sharp, \mathbb{Q}) > \dim_{\mathbb{Q}} F(\mathcal{O}, \mathbb{Q})$, and W cannot be injective.

Form of counterexample

- Suppose $R = M_n(\mathbb{F}_q)$ and $A = M_{n\times(n+1)}(\mathbb{F}_q)$.
- Choose $M = A$. Then $\mathrm{Hom}_R(M, A) = M_{n+1}(\mathbb{F}_q)$.
- Define $\eta_+ : \mathcal{O}^\sharp \to \mathbb{N}$ by: any column-reduced echelon matrix of size $(n+1)\times(n+1)$ of EVEN rank r is assigned multiplicity $q^{\binom{r}{2}}$.
- Define $\eta_- : \mathcal{O}^\sharp \to \mathbb{N}$ by: any column-reduced echelon matrix of size $(n+1)\times(n+1)$ of ODD rank r is assigned multiplicity $q^{\binom{r}{2}}$.
- The codes determined by $\eta_\pm$ are not equivalent (η_+ has a zero position corresponding to the zero matrix), but they have the same image under W.

Step three

- R non-Frobenius with $R/J \cong \oplus M_{n_i}(\mathbb{F}_{q_i})$.
- By step 1, there exists an index i so that $M_{n_i \times k_i}(\mathbb{F}_{q_i}) \subset \mathrm{Soc}(R)$, with $n_i < k_i$.
- Apply Step 2, with $M_{n_i}(\mathbb{F}_{q_i})$ and $M_{n_i \times k_i}(\mathbb{F}_{q_i})$.
- The counterexamples from Step 2 are $M_{n_i}(\mathbb{F}_{q_i})$-linear codes inside $M_{n_i \times k_i}(\mathbb{F}_{q_i})^N \subset \mathrm{Soc}(R)^N \subset R^N$. They are considered R-linear codes via $R \to R/J \to M_{n_i}(\mathbb{F}_{q_i})$.
- The zero position in η_+ shows that the codes from $\eta_\pm$ are not equivalent over the original ring R.

Why do $\eta_\pm$ give the same weights?

- One can calculate that $W(\eta_+) = W(\eta_-)$.
- This is a long, detailed argument involving the Cauchy binomial theorem.
- Equivalently, the argument involves properties of the Möbius function of the poset of all linear subspaces in $\mathbb{F}_q^k$.
- The multiplicities involved in $\eta_\pm$ are values of the Möbius function.

Example (a)

- $R = \mathbb{F}_q$, $M = A = M_{1\times 2}(\mathbb{F}_q) = \mathbb{F}_q^2$.
- DANGER: the Hamming weight on A means that $\mathrm{wt}(ab) = 1$ unless $ab = 00$ ($ab \in \mathbb{F}_q^2$).
- $\mathrm{Hom}_R(M, A) = M_2(\mathbb{F}_q)$, so look at 2×2 column-reduced echelon matrices.
- For η_+: zero matrix with multiplicity 1; the identity matrix with multiplicity q.
- For η_-: the following, each with multiplicity 1:

$$\begin{pmatrix} 1 & 0 \\ c & 0 \end{pmatrix} (c \in \mathbb{F}_q), \quad \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

Example (b)

- For any $ab \in M = \mathbb{F}_q^2$, form an element in A^{q+1} by multiplying ab times the matrices above. Because $G_l = \mathbb{F}_q^\times$, it suffices to compute elements of M of the form $1b$ or 01. (b varies over $\mathbb{F}_q$.)

code	input	output
η_+	$1b$	$00, 1b, 1b, \ldots, 1b$
η_-	$1b$	$\ldots, (1+bc)0, \ldots, b0$
η_+	01	$00, 01, 01, \ldots, 01$
η_-	01	$\ldots, c0, \ldots, 10$

Example (c)

- For nonzero inputs, check that wt(output) $= q$ for both $\eta_\pm$.
- Also verify that η_+ has a zero position (the first), but η_- does not. In fact, for the $q+1$ different inputs shown, the zero positions in η_-(input) occur in every possible position. ($c = 0$ comes first.)

input	zero position in η_- output
10	$q+1$
$1b\,(b \neq 0)$	$c = -b^{-1}$
01	1

Benson's example from lecture 3

- Let R be a ring consisting of all matrices over $\mathbb{F}_2$ of the following form:

$$\begin{pmatrix} a_1 & 0 & a_2 & 0 & 0 & 0 \\ 0 & a_1 & 0 & a_2 & a_3 & 0 \\ a_4 & 0 & a_5 & 0 & 0 & 0 \\ 0 & a_4 & 0 & a_5 & a_6 & 0 \\ 0 & 0 & 0 & 0 & a_9 & 0 \\ a_7 & 0 & a_8 & 0 & 0 & a_9 \end{pmatrix}.$$

- This R is QF but not Frobenius.

Benson's example: not Frobenius

- Setting all entries equal to zero except a_7 and a_8 yields an $\mathbb{F}_2^2 = M_{1\times 2}(\mathbb{F}_2) \subset \mathrm{Soc}(R)$:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ a_7 & 0 & a_8 & 0 & 0 & 0 \end{pmatrix}.$$

Other alphabets

- Assume alphabet A, a left R-module, with Hamming weight.
- Just as for rings, if $\mathrm{Soc}(A) \cong \oplus M_{n_i \times k_i}(\mathbb{F}_{q_i})$ with all $n_i \geq k_i$, then $\mathrm{Soc}(A)$, and hence A, admits a left generating character. This defines an embedding of A into $\widehat{R}$.
- Thus if A does not embed into $\widehat{R}$, it has an $M_{n_i \times k_i}(\mathbb{F}_{q_i})$, $n_i < k_i$, inside $\mathrm{Soc}(A)$.
- The same argument proves the existence of counterexamples over the alphabet A.
- The extension theorem holds for A iff A is pseudo-injective and A embeds in $\widehat{R}$.