Equivalence of codes: sufficient 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 12, 2012

Introduction

- The next three lectures will address the topic of code equivalence.
- If two linear codes are isomorphic via an isomorphism that preserves weight, does the isomorphism extend to a weight-preserving monomial transformation?
- In the first two lectures I will concentrate on linear codes over rings with the Hamming weight.
- More general weights and alphabets are the subject of the final lecture.

Monomial transformations

- Let R be a finite associative ring with 1.
- A *monomial transformation* $T : R^n \longrightarrow R^n$ is a homomorphism of left R-modules of the form

$$(a_1, \ldots, a_n)T = (a_{\sigma(1)}u_1, \ldots, a_{\sigma(n)}u_n),$$

  where the u_i are units in R and σ is a permutation of $\{1, \ldots, n\}$.
- Homomorphisms of left modules are written on the right.

Weights and symmetry groups

- A *weight* on R is a function $w : R \to \mathbb{C}$ with $w(0) = 0$.
- The *left symmetry group* is $G_l := \{u \in \mathcal{U}(R) : w(ua) = w(a), a \in R\}$.
- The *right symmetry group* is $G_r := \{v \in \mathcal{U}(R) : w(av) = w(a), a \in R\}$.
- $\mathcal{U}(R)$ denotes the group of units in R.
- For Hamming weight wt, $G_l = G_r = \mathcal{U}(R)$.

G_r-monomial transformations

- If the units of a monomial transformation T belong to the subgroup G_r, then T is a *G_r-monomial transformation*.
- G_r-monomial transformations preserve weight: $w(aT) = w(a)$, for all $a \in R^n$.
- The G_r-monomial transformations are *isometries* for the weight w. (Alonzo Sepúlveda's talk.)

Equivalence of codes

- Suppose $C_1, C_2 \subset R^n$ are two left R-linear codes, where R has weight w.
- The codes C_1, C_2 are *equivalent* if there exists a G_r-monomial transformation T such that $C_1 T = C_2$.
- If so, the restriction of T to C_1, $T : C_1 \longrightarrow C_2$, is an R-linear isomorphism that preserves the weight w (an *isometry*).

The extension problem

- Suppose $f : C_1 \longrightarrow C_2$ is an R-linear isomorphism that preserves the weight w. Does f extend to a G_r-monomial transformation?
- For $R = \mathbb{F}_q$ and Hamming weight wt, the answer is 'yes': MacWilliams, 1961-1962.
- Also true for Frobenius rings, 1999, by character theoretic methods; Greferath and Schmidt, 2000, by combinatorial methods; Greferath, 2002.

Main Theorem

Theorem

Let R be a finite Frobenius ring equipped with the Hamming weight wt. *Suppose $C_1, C_2 \subset R^n$ are two left R-linear codes. If $f : C_1 \longrightarrow C_2$ is an R-linear isomorphism that preserves* wt, *then f extends to a monomial transformation.*

- For $w =$ wt, $G_r = \mathcal{U}(R)$.

Idea

- Express weight-preservation as an equation of characters. (This idea comes from Ward and was used to prove the extension theorem for finite fields, 1996.)
- Use linear independence of characters and a partial ordering to match up terms and produce the monomial transformation.

Vanishing formula for characters

- If G is a finite abelian group, then

$$\sum_{\pi \in \widehat{G}} \pi(g) = \begin{cases} |G|, & g = 0, \\ 0, & g \neq 0. \end{cases}$$

- For $a = (a_1, a_2, \ldots, a_n) \in R^n$,

$$\mathrm{wt}(a) = n - \frac{1}{|R|} \sum_{i=1}^{n} \sum_{\pi \in \widehat{R}} \pi(a_i).$$

Re-cast the problem

- Re-phrase the hypothesis slightly. Let M be a finite left R-module (the module underlying the linear code C_1).
- Suppose there are two embeddings $g, h : M \hookrightarrow R^n$ such that $\mathrm{wt}(mg) = \mathrm{wt}(mh)$ for all $m \in M$. (View g as the inclusion of $C_1 \subset R^n$, and h as $g \circ f : M \longrightarrow C_2$.)
- Write the components of g, h as $g = (g_1, \ldots, g_n)$, $h = (h_1, \ldots, h_n)$.

Weight preservation condition

- Weight-preservation means $\mathrm{wt}(mg) = \mathrm{wt}(mh)$, for all $m \in M$.
- By vanishing formula, for all $m \in M$,

$$n - \frac{1}{|R|} \sum_{i=1}^{n} \sum_{\pi \in \widehat{R}} \pi(mg_i) = n - \frac{1}{|R|} \sum_{i=1}^{n} \sum_{\pi \in \widehat{R}} \pi(mh_i).$$

- Simplifying, and changing summation variables, for all $m \in M$,

$$\sum_{i=1}^{n} \sum_{\pi \in \widehat{R}} \pi(mg_i) = \sum_{j=1}^{n} \sum_{\pi \in \widehat{R}} \pi(mh_j).$$

Using Frobenius hypothesis

- Because R is Frobenius, there exists a (left) generating character ρ on R. Every character $\pi \in \widehat{R}$ is of the form $r\rho$ for $r \in R$.
- Remember that $(r\rho)(a) = \rho(ar)$, for $a, r \in R$.
- Weight-preservation becomes, for all $m \in M$,

$$\sum_{i=1}^{n} \sum_{r \in R} \rho(mg_i r) = \sum_{j=1}^{n} \sum_{s \in R} \rho(mh_j s).$$

- This is an equation of characters on the module M.

Using linear independence—trial run

- The weight-preservation condition, again, is, for all $m \in M$,

$$\sum_{i=1}^{n} \sum_{r \in R} \rho(mg_i r) = \sum_{j=1}^{n} \sum_{s \in R} \rho(mh_j s).$$

- This is an equation of characters (with all coefficients equal to $1 \in \mathbb{C}$).
- By linear independence of characters, the terms on the left must match the terms on the right.
- But how to get units?

A partial ordering

- Let $M^\sharp := \mathrm{Hom}_R(M, R)$ be the collection of all left R-homomorphisms from M to R.
- $M^\sharp$ is itself a right R-module under $m(gr) = (rm)g$.
- Let P be the set of principal right R-submodules of $M^\sharp$, $gR \subset M^\sharp$, partially ordered by inclusion.
- Fact: it follows from work of Bass that $gR = hR$ iff there exists a unit $u \in \mathcal{U}(R)$ such that $h = gu$.
- In their work, Greferath-Schmidt use a similar poset construction directly on R.

Using linear independence

- The weight-preservation condition, again, is, for all $m \in M$,

$$\sum_{i=1}^{n} \sum_{r \in R} \rho(mg_i r) = \sum_{j=1}^{n} \sum_{s \in R} \rho(mh_j s).$$

- This is an equation of characters (with all coefficients equal to $1 \in \mathbb{C}$).
- By linear independence of characters, the terms on the left must match the terms on the right.

Matching

- From the finite list of principal submodules $g_1R, g_2R, \ldots, g_nR, h_1R, \ldots, h_nR$, choose one that is maximal in the partial ordering. (Say, h_1R.)
- Consider the term on the right with $j = 1$ and $s = 1_R$. By linear independence, there exists i_0 and $r \in R$ on the left so that $\rho(mg_{i_0}r) = \rho(mh_1)$ for all $m \in M$.
- This says that $M(h_1 - g_{i_0}r) \subset \ker \rho$ is a left R-submodule of $\ker \rho$.

Frobenius condition, again

- But ρ is a left generating character on R, so $M(h_1 - g_{i_0} r) = 0$; that is, $h_1 = g_{i_0} r$.
- Thus, $h_1 R \subset g_{i_0} R$.
- But $h_1 R$ was chosen to be maximal. Thus $h_1 R = g_{i_0} R$.
- By Bass, there exists a unit $u_1 \in \mathcal{U}(R)$ such that $h_1 = g_{i_0} u_1$.
- Begin to define a permutation σ of $\{1, \ldots, n\}$ with $\sigma(1) = i_0$.

Inner sums

- In the weight-preservation condition

$$\sum_{i=1}^{n} \sum_{r \in R} \rho(m g_i r) = \sum_{j=1}^{n} \sum_{s \in R} \rho(m h_j s),$$

  we now examine the "inner sums" for h_1 and $g_{\sigma(1)}$.
- Because $h_1 = g_{\sigma(1)} u_1$, $h_1 s = g_{\sigma(1)} u_1 s$.
- As s varies over all of R, so does $u_1 s$.
- Thus $\sum_{s \in R} \rho(m h_1 s) = \sum_{r \in R} \rho(m g_{\sigma(1)} r)$, for all $m \in M$.

Induction step

- Subtract $\sum_{s\in R}\rho(mh_1s)=\sum_{r\in R}\rho(mg_{\sigma(1)}r)$ from both sides of

$$\sum_{i=1}^{n}\sum_{r\in R}\rho(mg_ir)=\sum_{j=1}^{n}\sum_{s\in R}\rho(mh_js).$$

- This reduces the size of the "outer sums" (in i and j) by one.
- Do the same process repeatedly.
- This inductively builds a permutation σ of $\{1,2,\ldots,n\}$ and produces units $u_i\in\mathcal{U}(R)$ such that $h_i=g_{\sigma(i)}u_i$, as desired.

Other alphabets

- Greferath, Nechaev, Wisbauer, 2004, proved the extension theorem for homogeneous and Hamming weights with $A = \widehat{R}$ for ANY finite ring R (Frobenius or not).
- The Frobenius ring case is then a special case.
- Most general, 2008: any ring R, alphabet A with Hamming weight, provided A is pseudo-injective and embeds into $\widehat{R}$ (A admits a left generating character).

Converses?

- If a ring R or an R-module alphabet A satisfy the extension property for Hamming weight, what can we say about R or A?
- In the ring case, R must be Frobenius (2008). (Next lecture.)
- In the module case, A must be pseudo-injective and embed in $\widehat{R}$ (2008).

Other weights?

- For weights other than the Hamming weight and the homogeneous weight, much less is known.
- This topic is the subject of the final lecture.

Parametrized codes

- Setting: ring R, left R-module alphabet A.
- A left R-linear *parametrized code* over A is pair (M, Λ), where M is a finite left R-module, and $\Lambda : M \longrightarrow A^n$ is a homomorphism of left R-modules.
- Λ is given by an n-tuple $(\lambda_1, \lambda_2, \ldots, \lambda_n)$ of homomorphisms $\lambda_i : M \longrightarrow A$. (Evaluation codes.)
- Suppose A has weight w and symmetry groups $G_l \subset \mathcal{U}(R)$ and $G_r \subset \mathrm{Aut}(A)$.

Equivalence of parametrized codes

- Two parametrized codes over the same module M, $(M, \Lambda), (M, \Gamma)$, are *equivalent* if there is a G_r-monomial transformation T on A^n such that $\Gamma = \Lambda \circ T$.
- Then $w(m\Gamma) = w(m\Lambda T) = w(m\Lambda)$ for all $m \in M$.
- Up to equivalence, what matters is the number of coordinate functionals (the λ_i) that belong to each G_r-scale class in $\mathrm{Hom}_R(M, A)$.

Multiplicity functions

- Given a finite left R-module M, let $\mathcal{O}^\sharp$ be the set of G_r-scale classes in $\mathrm{Hom}_R(M, A)$.
- Up to equivalence, a parametrized code on M is completely determined by a *multiplicity function* $\eta : \mathcal{O}^\sharp \to \mathbb{N}$, i.e., an element $\eta \in F(\mathcal{O}^\sharp, \mathbb{N})$.

Weight mapping

- Define an additive mapping $W : F(\mathcal{O}^\sharp, \mathbb{N}) \to F(M, \mathbb{C})$ by

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

- $[\lambda]$ denotes the G_r-scale class of $\lambda \in \mathrm{Hom}_R(M, A)$.
- This calculates the weight $w(m\Lambda)$ for every $m \in M$, where Λ is determined by the multiplicity function η.
- This mapping is well-defined and additive. (Addition in $F(\mathcal{O}^\sharp, \mathbb{N})$ corresponds to concatenation of generator matrices.)

Extension problem re-cast

- The extension problem for the weight w over the alphabet A is satisfied iff the mapping W is injective for every module M.
- I.e., if two parametrized codes based on M yield the same weights (weight preservation), then the codes are equivalent (differ by a G_r-monomial transformation).
- This formulation will be used in the next lecture on necessary conditions.