Equivalence of codes: general weights

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 will discuss the extension problem for a general weight function over a finite Frobenius ring.
- An intermediate result is the extension theorem for symmetrized weight compositions.
- While there are results for Frobenius principal ideal rings, the general case is still open.

Set up

- Let R be a finite Frobenius ring with 1, equipped with a weight w.
- Let G_l and G_r be the left and right symmetry groups of w. Both groups are subgroups of $\mathcal{U}(R)$.
- We will consider left R-linear codes $C \subset R^n$.

Counting

- For a vector $x = (x_1, x_2, \ldots, x_n) \in R^n$ and an element $r \in R$, define

$$c_r(x) := |\{i : x_i = r\}|.$$

- $c_r(x)$ counts the number of entries of x that equal r.
- $\sum_{r \in R} c_r(x) = n$ and $\sum_{r \neq 0} c_r(x) = \mathrm{wt}(x)$, the Hamming weight of x.

Symmetrized weight compositions

- The group G_r acts on R on the right. Write $r_1 \sim r_2$ if there exists $u \in G_r$ with $r_2 = r_1 u$.
- For $x \in R^n$ and $r \in R$, define the *symmetrized weight composition* by

$$\mathrm{swc}_r(x) = \sum_{s \sim r} c_s(x).$$

- $swc_r(x)$ counts the number of entries of x that are in the same G_r-orbit as r.

Example: $\mathbb{Z}/4\mathbb{Z}$ with Lee weight

- Let $R = \mathbb{Z}/4\mathbb{Z}$ with the Lee weight: $w(0) = 0$, $w(1) = w(-1) = 1$, $w(2) = 2$. ($3 = -1$, of course.)
- $G_l = G_r = \{\pm 1\}$.
- $\mathrm{swc}_1(x)$ counts the number of ± 1s in x.

G_r-monomial transformations preserve swc

- Suppose T is a G_r-monomial transformation.
- For every $x \in R^n$ and $r \in R$, $\mathrm{swc}_r(xT) = \mathrm{swc}_r(x)$.
- If $C_1, C_2 \subset R^n$ are R-linear codes with $C_1 T = C_2$, then $T : C_1 \longrightarrow C_2$ is an R-linear isomorphism that preserves swc.
- Converse?

Extension theorem for swc

Theorem

Let R be a finite Frobenius ring. Suppose $C_1, C_2 \subset R^n$ are R-linear codes. If $f : C_1 \longrightarrow C_2$ is an R-linear isomorphism that preserves swc *(i.e.,* $\mathrm{swc}_r(xf) = \mathrm{swc}_r(x)$*, for all $x \in C_1$ and $r \in R$), then f extends to a G_r-monomial transformation.*

- This result dates to 1997, using linear independence of averaged characters. Aleams Barra has an improved proof, 2012 dissertation.

Extension problem for weight w

- Suppose R is a finite Frobenius ring with weight w and symmetry groups G_l, G_r. Suppose $C_1, C_2 \subset R^n$ are R-linear codes. If $f : C_1 \longrightarrow C_2$ is an R-linear isomorphism that preserves w (i.e., $w(xf) = w(x)$, for all $x \in C_1$), does f extend to a G_r-monomial transformation?
- It is important that the units lie in G_r, because a general monomial transformation may not preserve w on all of R^n.

Expressing $w(x)$ in terms of swc

- We express $w(x)$ in terms of swc:

$$w(x) = \sum_{r \in R} w(r) c_r(x) = \sum_{[r]} w(r) \operatorname{swc}_r(x),$$

where the last sum is over the G_r-orbits $[r]$.

Use linearity

- Now consider $w(tx)$, $t \in R$:

$$w(tx) = \sum_{[r]} w(tr)\,\mathrm{swc}_r(x).$$

- If $u \in G_l$, then $w(utx) = w(tx)$, so only the left G_l-orbit of t matters.

Coefficient matrix

- Define a matrix W whose rows are indexed by the nonzero left G_l-orbits on R, and whose columns are indexed by the nonzero right G_r-orbits on R. The entry in position $(G_l t, rG_r)$ is $w(tr)$, i.e., w evaluated at the product $tr \in R$.
- This is well-defined, by the definitions of G_l and G_r.

Extension criterion

Theorem

Suppose R is a finite Frobenius ring with weight w and symmetry groups G_l, G_r. Suppose the matrix $W = (w(tr))_{(G_l t, r G_r)}$ has zero right nullspace. Then the extension property is satisfied for w.

- This result dates to 1997.

Proof (a)

- Suppose $f : C_1 \longrightarrow C_2$ preserves w. Then $w(xf) - w(x) = 0$ for all $x \in C_1$.
- As $tx \in C_1$, we also have $w(txf) - w(tx) = 0$, for all $t \in R$, $x \in C_1$.
- By $w(tx) = \sum_{[r]} w(tr)\,\mathrm{swc}_r(x)$, we have, for all $t \in R$, $x \in C_1$:

$$0 = w(txf) - w(tx) = \sum_{[r]} w(tr)(\mathrm{swc}_r(xf) - \mathrm{swc}_r(x)).$$

Proof (b)

- This says that $\mathrm{swc}_r(xf) - \mathrm{swc}_r(x)$, regarded as a vector indexed by $[r]$, is in the right null space of the matrix W.
- By hypothesis on W, we have $\mathrm{swc}_r(xf) - \mathrm{swc}_r(x) = 0$ for all $r \in R$, $x \in C_1$.
- That is, f preserves swc.
- By earlier theorem, f extends to a G_r-monomial transformation.

A few general results

- When R is commutative, the matrix W is square. One can then use $\det(W) \neq 0$ to show that the extension property holds for w.
- Extension property holds for Lee weight on $\mathbb{Z}/n\mathbb{Z}$ for all $n \leq 256$ (2001), and for all primes up to the 2012th prime (Barra, 2012). Also, for all n of the form 2^k, 3^k; and primes p of the form $p = 2q + 1$ with q prime (2001), and primes $p = 4q + 1$ with q prime (Barra, 2012).
- For Euclidean weight on $\mathbb{Z}/n\mathbb{Z}$: true for $n \leq 256$, for all n of the form 3^k, and primes p of the form $p = 2q + 1$ with q prime.
- True for homogeneous weight on finite chain rings.

Can we say anything more specific?

- Is it possible to write down conditions on w in a more tractable form?
- Yes, in some circumstances.
- First, some small examples.

Example: $\mathbb{Z}/6\mathbb{Z}$

- Suppose $R = \mathbb{Z}/6\mathbb{Z}$, and suppose w is a weight with maximal symmetry $G = \mathcal{U}(\mathbb{Z}/6\mathbb{Z}) = \{\pm 1\}$.
- Index rows/columns by $1, 2, 3$, and write w_i for $w(i)$:

$$W = \begin{pmatrix} w_1 & w_2 & w_3 \\ w_2 & w_2 & 0 \\ w_3 & 0 & w_3 \end{pmatrix}.$$

- $\det(W) = w_2 w_3 (w_1 - w_2 - w_3)$.
- Compare codes generated by 10 and by 23, $n = 2$.

Example: $\mathbb{Z}/12\mathbb{Z}$

- Suppose $R = \mathbb{Z}/12\mathbb{Z}$, and suppose w is a weight with maximal symmetry $G = \mathcal{U}(\mathbb{Z}/12\mathbb{Z}) = \{1, 5, 7, 11\}$.
- Index rows/columns by $1, 2, 3, 4, 6$, and write w_i for $w(i)$.
- A MAPLE computation gives $\det(W) = w_4 w_6^2 (w_2 - w_4 - w_6)^2$.

Chain rings

- Let R be a chain ring. Suppose the unique maximal ideal is $\mathfrak{m} = (\gamma)$, and that γ has nilpotency t.
- Let w be a weight with maximal symmetry, i.e., $G_l = G_r = \mathcal{U}(R)$.
- Every element $a \in R$ can be written as $a = u\gamma^i$, where i is uniquely determined. Then $w(a) = w(\gamma^i)$.
- The only distinct nonzero values of the weight w are $w_i := w(\gamma^i)$, $i = 0, \ldots, t-1$.
- The matrix W has an anti-triangular form, and $\det(W) = \pm w_{t-1}^t$.

Weights with maximal symmetry

- Suppose R is a finite Frobenius ring with weight w.
- Assume maximal symmetry: $G_l = G_r = \mathcal{U}(R)$.
- Then the right G_r-orbits on R are in one-to-one correspondence with the principal right ideals. (This follows from work of Bass and was used in the partial order in lecture 6.)
- The set P_r of principal right ideals of R is a poset under set inclusion.
- Let μ_r be the Möbius function of P_r.

Conjecture

- In the maximal symmetry situation, the conjecture is that

$$\det(W) = \prod_{0 \neq aR \in P_r} \sum_{0 \neq bR \subset \mathrm{Soc}(aR)} w(b)\mu_r(0, bR).$$

Known cases

- Matrix rings $M_n(\mathbb{F}_q)$, circa 2004:

$$\det(W) = C \prod_{s=1}^{n} \left(\sum_{i=1}^{s} (-1)^i q^{\binom{s}{i}} \begin{bmatrix} s \\ i \end{bmatrix}_q w_i \right)^{\begin{bmatrix} n \\ s \end{bmatrix}_q}.$$

- $\mathbb{Z}/n\mathbb{Z}$, Greferath and Honold, 2006.
- Products of chain rings, Greferath, Mc Fadden, and Zumbrägel, 2012.
- Principal ideal rings, Greferath, Honold, Mc Fadden, Wood, Zumbrägel, in preparation.

Thanks

- I want to thank CIMPA, the sponsors, the organizers, and local committee members, especially our local host Mustapha Lahyane, for their kind hospitality.
- I also thank all the particpants in the research school for their interest and enthusiasm.
- And a special thanks to Brenda de la Rosa Navarro for all she has done to make the school a success.
- ¡Muchas gracias!