Linear Codes from the Axiomatic Viewpoint

Jay A. Wood

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

Noncommutative rings and their applications, IV
University of Artois, Lens
June 10, 2015

6. One-weight and relative one-weight codes

- Definitions
- Using EP: uniqueness theorem
- Guess and check
- Homogeneous weight
- Key lemma: sum over submodules of $\mathrm{Hom}_R(M, A)$
- Converse: only way to get relative one-weight codes
- Concatenate to get certain two-weight codes
- Examples

Setting for this lecture

- Finite ring R, alphabet $A = \widehat{R}$, weight w on A, information module M.
- When R is Frobenius, $A = R$.
- W-map: $W : F_0(\mathcal{O}^\sharp, \mathbb{Q}) \to F_0(\mathcal{O}, \mathbb{Q})$.
- EP holds for w if and only if W is injective.

Definitions

- An R-linear code $C \subseteq \widehat{R}^n$ is a **one-weight code** if there exists a constant w_0 such that $w(c) = w_0$ for all nonzero $c \in C$.
- Fix an R-linear code $C \subseteq \widehat{R}^n$ and a linear subcode C_1. (Liu-Chen) C is a **relative one-weight code** with respect to C_1 if there exists a constant w_0 such that $w(c) = w_0$ for all $c \in C$ with $c \notin C_1$.

Using multiplicity functions

- Suppose EP holds for weight w on $A = \widehat{R}$.
- Examples: an egalitarian weight or the Hamming weight.
- Any R-linear code C over A is modeled by $\Lambda : M \to A^n$, with multiplicity function η.
- C is a one-weight code if and only if $W(\eta) \in F_0(\mathcal{O}, \mathbb{Q})$ is a constant function.

Using EP: uniqueness theorem

- The constant functions form a one-dimensional subspace S of $F_0(\mathcal{O}, \mathbb{Q})$.
- If EP holds for w, $W : F_0(\mathcal{O}^\sharp, \mathbb{Q}) \to F_0(\mathcal{O}, \mathbb{Q})$ is injective. Then $W^{-1}(S)$ has dimension 0 or 1.
- For a fixed M: if one-weight codes exist at all, they are unique up to **replication** (concatenation, repeating columns).
- Weiss, Bonisoli: binary one-weight codes are replications of simplex codes.

Guess and check

- Fix M. If one can **guess** a formula for η and **check** that all weights agree, then every one-weight code modeled on M must be a multiple of η.
- Caveat! A priori, η could have rational values. Clear denominators to get integer values.
- If all the $\pm$-signs are the same, then $\pm\eta$ solves the problem.
- However, if the signs are mixed (some positive, some negative), this proves that one-weight codes modeled on M do not exist.

Example

- Let $R = A = \mathbb{Z}/9\mathbb{Z}$ with Hamming weight, $M = R^2$.
- Generator matrix: columns with multiplicities above.

$$
\begin{array}{|cccccccccccc|cccc|}
3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & -2 & -2 & -2 & -2 \\
\hline
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 3 & 3 & 0 & 3 & 3 & 3 \\
1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 1 & 2 & 3 & 0 & 3 & 6
\end{array}
$$

- All nonzero codewords have Hamming weight 27.
- "Classical" linear one-weight code for $M = R^2$ does not exist.

Egalitarian weight

- Recall that an egalitarian weight w has the property that there exists a constant γ such that
$$\sum_{b \in B} w(a_0 + b) = \gamma |B|,$$
for any nonzero submodule B of $A = \widehat{R}$ and $a_0 \in A$.
- For any M, set $\eta(\lambda) = 1$ for all nonzero $\lambda \in \mathrm{Hom}_R(M, A)$. (Use every column-type once.)
- Then η defines a one-weight code with weight $\gamma |\mathrm{Hom}_R(M, A)|$.

Proof

- Take any nonzero $x \in M$. Define
$$\check{x} : \mathrm{Hom}_R(M, A) \to A, \quad \lambda \mapsto x\lambda.$$
$\check{x}$ is a homomorphism of right R-modules.
- Image $\mathrm{im}\,\check{x}$ is a nonzero submodule of A.

$$\begin{aligned} W(\eta)(x) &= \sum_{\lambda} w(x\lambda) = |\ker \check{x}| \sum_{b \in \mathrm{im}\,\check{x}} w(b) \\ &= \gamma |\mathrm{im}\,\check{x}||\ker \check{x}| = \gamma |\mathrm{Hom}_R(M, A)| \end{aligned}$$

Key lemma: sum over cosets in $\mathrm{Hom}_R(M, A)$

- Generalize this idea: let $E \subseteq \mathrm{Hom}_R(M, A)$ be a right R-submodule.
- Define $E^\circ = \{x \in M : x\lambda = 0, \lambda \in E\}$, left submodule of M.
- Let λ_0 be any element of $\mathrm{Hom}_R(M, A)$. Then

$$\sum_{\lambda \in \lambda_0 + E} w(x\lambda) = \begin{cases} w(x\lambda_0)|E|, & x \in E^\circ, \\ \gamma|E|, & x \notin E^\circ. \end{cases}$$

Producing relative one-weight codes

- Set $E = M_1^\circ = \{\lambda \in \mathrm{Hom}_R(M, A) : M_1\lambda = 0\}$, for submodule $M_1 \subset M$. Then $E^\circ = M_1$.

Theorem

Suppose η is constant along the cosets of E in $\mathrm{Hom}_R(M, A)$. Then η defines a relative one-weight code relative to M_1.

- Apply key lemma on each coset. $W(\eta)(x)$ does not depend on x provided $x \notin M_1$.
- Converse is true, but harder.

Concatenate to get certain two-weight codes

- Addition of multiplicity functions corresponds to concatenation of generator matrices. Weights of codewords add.
- Key lemma with $\lambda_0 = 0$:

$$\sum_{\lambda \in E} w(x\lambda) = \begin{cases} 0, & x \in E^\circ, \\ \gamma |E|, & x \notin E^\circ. \end{cases}$$

- Put these together for different choices of E.

Example (a)

- Let $M_1 \subset M$. Set $E_1 = M_1^\circ$.
- Define $\eta_1(\lambda) = s_1$ for $\lambda \in E_1$ and 0 elsewhere. Define $\eta_2(\lambda) = s_2$ for all $\lambda \in \mathrm{Hom}_R(M, A)$.
- For $\eta = \eta_1 + \eta_2$ and $x \neq 0$:

$$W(\eta)(x) = \begin{cases} s_2\gamma|\mathrm{Hom}_R(M, A)|, & x \in M_1, \\ s_1\gamma|E| + s_2\gamma|\mathrm{Hom}_R(M, A)|, & x \notin M_1. \end{cases}$$

Example (b)

- More specifically, let $R = A = \mathbb{F}_q$, $M = \mathbb{F}_q^m$, $M_1 = \{(*, 0, \ldots, 0)\} \cong \mathbb{F}_q$.
- Then $|\mathrm{Hom}_R(M, A)| = q^m$ and $|E| = q^{m-1}$.
- Set $s_2 = 1$, $s_1 = -1$, $\gamma = (q-1)/q$ (Hamming). Then, $n = (q-1)q^{m-1}$ and, for $x \neq 0$:

$$W(\eta)(x) = \begin{cases} (q-1)q^{m-1}, & x \in M_1, \\ (q-1)^2 q^{m-2}, & x \notin M_1. \end{cases}$$

- A $(q-1)$-fold replicate of a generalized Reed-Muller code $GRM(m-1, 1, q)$.