Relative One-Weight Codes

Jay A. Wood

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

AMS meeting, Lincoln, Nebraska
October 14, 2011

Acknowledgments

- This work was inspired by the paper "Notes on the Value Function," by Zihui Liu and Wende Chen, Des. Codes Cryptogr. **54** (2010), 11–19.
- Also: "Further results on support weights of certain subcodes," by Zihui Liu, Wende Chen, Zhimin Sun, and Xiangyong Zeng, Des. Codes Cryptogr. **61** (2011), 119–129.

Definitions

- A linear code is a *one-weight code* if all its nonzero codewords have the same weight.
- A linear code C is a *relative one-weight code* with respect to a subcode C_1 if all elements of C that are not in C_1 have the same weight.
- A linear code is a *two-weight code* if the weight of every nonzero codeword is one of two values.

Example

- Let $R = \mathbb{F}_2$, with $\dim C = 4$ and $\dim C_1 = 2$.
- Generator matrix for C below, with C_1 spanned by the last two rows. Blocks are repeated with multiplicities m_i.

m_1			m_2				m_3				m_4			
1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
0	0	0	0	0	0	0	1	1	1	1	1	1	1	1

Example, continued

m_1			m_2				m_3				m_4			
1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
0	0	0	0	0	0	0	1	1	1	1	1	1	1	1

- The three nonzero elements of C_1 have Hamming weights $4(m_2 + m_4)$, $4(m_3 + m_4)$, and $4(m_2 + m_3)$.
- The elements of C that are not in C_1 all have Hamming weight $2(m_1 + m_2 + m_3 + m_4)$.

Linear Codes via Functionals (a)

- Follow Assmus-Mattson (1963). Let R be a finite ring with 1 and M a finite left R-module.
- Given functionals $\lambda_1, \ldots, \lambda_n \in M^\sharp := \mathrm{Hom}_R(M, R)$, the image of $M \longrightarrow R^n$, $x \mapsto (\lambda_1(x), \ldots, \lambda_n(x))$, is a linear code in R^n.
- If one fixes a set of generators $x_1, \ldots, x_k$ for M, then the matrix with (i, j)-entry $\lambda_j(x_i)$ is a generator matrix for this linear code.
- Up to permutation equivalence, all that matters is the number of times a functional $\lambda \in M^\sharp$ appears in the list $\lambda_1, \ldots, \lambda_n$: call it the *multiplicity* $\eta(\lambda)$.

Linear Codes via Functionals (b)

- Conversely, a multiplicity function $\eta : M^\sharp \longrightarrow \mathbb{N}$ determines a linear code, up to permutation equivalence.
- For a weight w on R, the weight of a codeword is

$$w(x) = \sum_{\lambda \in M^\sharp} w(\lambda(x))\,\eta(\lambda), \quad x \in M.$$

- For an alphabet A, a finite left R-module, use $\mathrm{Hom}_R(M, A)$ instead.
- One can also consider monomial equivalence, but not today.

Homogeneous Weights

- Draw on work of Constantinescu, Greferath, Heise, Honold, Nechaev, Schmidt, ...
- Every finite ring R admits a weight w such that
  - $w(ur) = w(r)$, $r \in R$, u unit of R; and
  - there is a constant γ such that $\sum_{r \in aR} w(r) = \gamma |aR|$, for every nonzero $a \in R$.
- If R is Frobenius, then $\sum_{r \in I} w(s + r) = \gamma |I|$ for every $s \in R$ and nonzero right ideal $I \subset R$.
- Example. $R = \mathbb{Z}/p^k\mathbb{Z}$. $w(0) = 0$, $w(up^{k-1}) = p$ (u unit), $w(r) = p - 1$ (rest). Then $\gamma = p - 1$.

Key Lemma

- For $E \subset M^\sharp$, $\mathrm{ann}(E) = \{x \in M : \lambda(x) = 0, \lambda \in E\}$.

Lemma

Let R be a finite Frobenius ring with homogeneous weight w. For any nonzero right submodule $E \subset M^\sharp$, $\lambda_0 \in M^\sharp$, and $x \in M$,

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

Proof

- Image of $E \longrightarrow R$, $\nu \mapsto \nu(x)$, is a right ideal of R.
- Image of $\lambda_0 + E \longrightarrow R$, $\lambda \mapsto \lambda(x)$ is a coset of this ideal.
- Apply the homogeneous property and a homomorphism argument.

Main Theorem

For left submodule $N \subset M$, $N^\circ := \{\lambda \in M^\sharp : \lambda(N) = 0\}$ is a right submodule of $M^\sharp$.

Theorem

Let R be a finite Frobenius ring with homogeneous weight w, and let $N \subset M$ be left R-modules. Assume a multiplicity function $\eta : M^\sharp \longrightarrow \mathbb{N}$ is constant on each coset of $N^\circ \subset M^\sharp$. Then the linear code defined by η is a relative one-weight code with respect to N. (That is, $w(x)$ is constant for $x \in M \setminus N$.)

Proof

- Calculate $w(x) = \sum_{\lambda \in M^\sharp} w(\lambda(x))\,\eta(\lambda)$, $x \in M$.
- Break into sums over cosets $\lambda_0 + N^\circ$ and apply Lemma with $E = N^\circ$.
- Note that $\operatorname{ann}(N^\circ) = N$. (Uses R quasi-Frobenius.)

Liu-Chen Motivation

- Linear codes $C_1 \subset C \subset \mathbb{F}_q^n$.
- Consider generalized Hamming weight $w_r(D)$ of linear codes $D \subset C$, with $\dim D = r$ and $D \cap C_1 = 0$.
- If $w_r(D)$ is constant for all such D, then C is a relative one-weight code with respect to C_1.
- When an additional condition is satisfied, C is a two-weight code, with the weights supported on C_1 and its complement.

Certain Two-Weight Codes

- Similar techniques allow one to construct two-weight codes on M with the weight supported on N and its complement. Liu, Chen, Sun, and Zeng have done this over $\mathbb{F}_q$.

Theorem

Let R be a finite Frobenius ring with homogeneous weight w, and let $N \subset M$ be left R-modules. Assume a multiplicity function $\eta : M^\sharp \to \mathbb{N}$ takes one value on N° and a different value on the complement of N°. Then the linear code defined by η is a two-weight code supported on N and its complement.

More Detailed Statement

- More precisely, if

$$\eta(\lambda) = \begin{cases} a+b, & \lambda \in N^{\circ}, \lambda \neq 0, \\ a, & \lambda \notin N^{\circ}, \end{cases}$$

then

$$w(x) = \begin{cases} a\gamma|M^{\sharp}|, & x \in N, x \neq 0, \\ a\gamma|M^{\sharp}| + b\gamma|N^{\circ}|, & x \notin N. \end{cases}$$