Understanding Linear Codes of Constant Weight Using Virtual Linear Codes

Jay A. Wood
Department of Mathematics and Statistics
Western Michigan University
1903 W. Michigan Ave.
Kalamazoo, MI 49008–5248
jay.wood@wmich.edu
http://unix.cc.wmich.edu/jwood/

October 6, 2000
Allerton Conference

Outline

- $\mathbb{Z}/4\mathbb{Z}$-example
- Terminology and basic questions
- Codes via functionals
- Virtual codes
- Uniqueness
- Existence
- Final example

$\mathbb{Z}/4\mathbb{Z}$-example

$R = \mathbb{Z}/4\mathbb{Z}$ $\quad$ $M \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

Element weights

	0	1	2	3
Hamming	0	1	1	1
Lee	0	1	2	1
Euclidean	0	1	4	1

0	0	0	0	0	0	0
0	**1**	**1**	**2**	**3**	**3**	**2**
0	2	2	0	2	2	0
0	3	3	2	1	1	2
2	**0**	**2**	**2**	**0**	**2**	**0**
2	1	3	0	3	1	2
2	2	0	2	2	0	0
2	3	1	0	1	3	2

Multiplicities

	a	b
Hamming	1	-1
Lee	1	1
Euclidean	1	2

Terminology

$R = \mathbb{Z}/N\mathbb{Z}$

Element weights a_r, $r \in R$

Weight function $w(x) = \sum_{i=1}^{n} a_{x_i}$, $x \in R^n$

A linear code C has *constant weight* L if

$$w(x) = L$$

for all nonzero $x \in C$.

Basic questions

- Which modules underlie constant weight linear codes?
- Uniqueness? (up to replication)
- Existence?

Linear codes via functionals

Module M over $R = \mathbb{Z}/N\mathbb{Z}$

$N = p_1^{\beta_1} p_2^{\beta_2} \cdots p_l^{\beta_l}$

$$M \cong \oplus_{i=1}^{l} \oplus_{j=1}^{\beta_i} \left(\mathbb{Z}/p_i^j\mathbb{Z}\right)^{k_{i,j}} \qquad (k_{i,\beta_i} > 0)$$

$M^\sharp := \mathsf{Hom_R(M, R)}$, linear functionals

Linear code $C = (M, \eta)$, $\eta : M^\sharp \to \mathbb{N}$

$\lambda \in M^\sharp$ corresponds to column of generator matrix

$\eta(\lambda)$ gives its multiplicity

A correspondence

Disclaimer: There are technical definitions of equivalence which I am going to leave out.

Linear codes $C = (M, \eta)$ supported by M correspond to $\eta \in \mathbb{N}[M^\sharp] = \{\eta : M^\sharp \to \mathbb{N}\}$

Bring in a weight function w, with $a_r \in \mathbb{Q}$

$$W : \mathbb{N}[M^\sharp] \to \mathbb{Q}[M] \quad \eta \mapsto w_\eta$$

$$w_\eta(x) = \sum_{\lambda \in M^\sharp} \eta(\lambda) a_{\lambda(x)}$$

Theorem 1 *Up to equivalence, W is injective.*

Virtual codes

Virtual codes are a technical device tailor-made for the constant weight problem. Will there be other uses?

Allow negative, even rational, multiplicities

Virtual linear code $C = (M, \eta)$, $\eta : M^\sharp \to \mathbb{Q}$

$$W : \mathbb{Q}[M^\sharp] \to \mathbb{Q}[M]$$

Theorem 2 *Up to equivalence, W is an isomorphism of $\mathbb{Q}$-vector spaces.*

Uniqueness

$W : \mathbb{Q}[M^\sharp] \to \mathbb{Q}[M]$ is an isomorphism. Constant weight yields a one-dimensional subspace on the right, hence also on the left.

Theorem 3 *For a fixed M, integral virtual constant weight codes are unique up to replication.*

We want integral coefficients: clear denominators, factor out greatest common divisors. All other integral solutions are integral multiples.

Warning: some coefficients may be negative.

A code is *classical* if all coefficients are positive.

Existence

This requires case by case analysis for different weight functions. But, the uniqueness theorem allows us to "guess and check."

Recall $R = \mathbb{Z}/N\mathbb{Z}$, $N = p_1^{\beta_1} p_2^{\beta_2} \cdots p_l^{\beta_l}$

$$M \cong \oplus_{i=1}^{l} \oplus_{j=1}^{\beta_i} \left(\mathbb{Z}/p_i^j\mathbb{Z}\right)^{k_{i,j}} \qquad (k_{i,\beta_i} > 0)$$

Hamming case

Theorem 4 *Set* $K_i := \sum_{j=1}^{\beta_i} k_{i,j}$. *For every nonzero* $\lambda \in M^\sharp$, *assign the multiplicity*

$$\eta(\lambda) = \prod_{\substack{i: \\ \lambda \in p_i M^\sharp}} \left(1 - p_i^{K_i - 1}\right).$$

The resulting virtual linear code has constant Hamming weight

$$L = |M| \prod_{i=1}^{l} (1 - 1/p_i).$$

Corollary 5 *An* R*-module* M *underlies a classical linear code of constant Hamming weight only in the following circumstances:*

- $N = p$, *a prime, in which case* $\eta(\lambda) = 1$ *for all nonzero* $\lambda \in M^\sharp$, *(Bonisoli), or*

- M *is free of rank* 1.

Lee Case

Theorem 6 *For nonzero $\lambda \in M^\sharp$, set*

$$\eta(\lambda) = \prod_{\substack{p_i \text{ odd:} \\ \lambda \in p_i M^\sharp}} \left(1 - p_i^{K_i - 2}\right).$$

This yields constant Lee weight

$$L = (N/4)\,|M| \prod_{i:\, p_i \text{ odd}} (1 - 1/p_i^2).$$

Corollary 7 *An R-module M underlies a classical linear code of constant Lee weight only in the following circumstances:*

- *$N = p$, a prime, M arbitrary, in which case $\eta(\lambda) = 1$ for all nonzero $\lambda \in M^\sharp$.*

- *$N = 2^{\beta_0}$, M arbitrary, $\eta(\lambda) = 1$: Carlet.*

- *N arbitrary, but M restricted by $K_i \leq 2$, for all i with p_i odd.*

Euclidean case

Theorem 8 *Virtual linear codes of constant Euclidean weight L have multiplicities as follows.*

- *N odd: (same as Lee case)*

$$\eta(\lambda) = \prod_{\substack{p_i \text{ odd:} \\ \lambda \in p_i M^\sharp}} \left(1 - p_i^{K_i - 2}\right).$$

$$L = (N^2/12)\,|M| \prod_{i:\, p_i \text{ odd}} (1 - 1/p_i^2).$$

- $N = 2^{\beta_0}$*:*

$$\eta(\lambda) = \sum_{i=0}^{\nu(\lambda)} 2^{e_i}.$$

$$L = 2^{2\beta_0 - 2}\,|M| = (N^2/4)\,|M|\,.$$

- *N even, but not a 2-power:*

$$\eta(\lambda) = \left(\sum_{i=0}^{\nu(\lambda)} 2^{e_i'}\right) \prod_{\substack{p_i \text{ odd:} \\ \lambda \in p_i M^\sharp}} \left(1 - p_i^{K_i - 2}\right).$$

$$L = (N^2/4)\,|M| \prod_{i:\, p_i \text{ odd}} (1 - 1/p_i^2).$$

The e_i, e_i' depend on the $k_{0,j}$, and $\nu(\lambda)$ measures the 2-divisibility of λ.

Corollary 9 *Over $R = \mathbb{Z}/N\mathbb{Z}$, an R-module M underlies a classical linear code of constant Euclidean weight only in the following circumstances:*

- *$N = p$, a prime, M arbitrary, in which case $\eta(\lambda) = 1$ for all nonzero $\lambda \in M^\sharp$.*

- *$N = 2^{\beta_0}$, M arbitrary.*

- *N arbitrary, but M restricted by $K_i \leq 2$, for all i with p_i odd.*

$\mathbb{Z}/6\mathbb{Z}$ example

$M \cong \mathbb{Z}/6\mathbb{Z} \oplus (\mathbb{Z}/3\mathbb{Z})^2 \cong \mathbb{Z}/2\mathbb{Z} \oplus (\mathbb{Z}/3\mathbb{Z})^3$

Columns look like transpose of $(*, 2*, 2*)$.

Multiplicities of nonzero functionals:

Type	Form	#	H	L	E
$3M^\sharp$	$(3, 0, 0)$	1	-8	-2	-2
$2M^\sharp$	$(2*, 2*, 2*)$	26	0	1	2
Rest	(odd,$2*, 2*$)	26	1	1	1
Weight			18	72	216