The Structure of Linear Codes of Constant Weight

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

WCC2001, Paris
January 9, 2001

Two years ago, at WCC1999, I gave a talk entitled *Codes of constant Lee or Euclidean weight* in which I presented some preliminary results about linear codes of constant Lee or Euclidean weight over $\mathbb{Z}/2^{\beta}\mathbb{Z}$ or $\mathbb{Z}/p^2\mathbb{Z}$. At the end of that talk I expressed the hope of returning in two years time with a more complete set of results. That is the subject of today's talk.

Outline:

- Preliminaries
- Setting up the problem: virtual codes
- Uniqueness theorem
- Existence: case by case

Preliminaries

Ground ring is $R = \mathbb{Z}/N\mathbb{Z}$.

Linear code $C = (M, \eta)$, where M is a finitely generated R-module, and

$$\eta : M^\sharp := \mathsf{Hom}_R(M, R) \to \mathbb{N}$$

is a *multiplicity function*.

Think of columns of a generator matrix.

Non-degenerate: $\eta(0) = 0$.

Weights

A *weight function* w on R assigns weights a_r to $r \in R$; $a_0 = 0$. We assume $a_r \in \mathbb{Q}$.

For a code $C = (M, \eta)$, $x \in M$ has *weight*

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

A linear code has *constant weight* $L > 0$ if $w_\eta(x) = L$ for all nonzero $x \in M$.

There are appropriate notions of equivalence of codes, but I will suppress them in the talk. Refer to the printed version for details.

Fix an R-module M.

$$\eta \in \mathbb{N}[M^\sharp] \mapsto w_\eta \in \mathbb{Q}[M].$$

Passing to appropriate equivalence classes:

$$\eta_S \in \mathbb{N}[\mathcal{O}^\sharp] \mapsto w_{\eta_S} \in \mathbb{Q}[\mathcal{O}].$$

We assume that this map is injective
(the MacWilliams Equivalence Theorem).

Known: Hamming weight, all N; Lee or Euclidean weight, $N \leq 256$, $N = 2^\beta$, $N = 3^\beta$.

Virtual linear codes

A *virtual linear code* $C = (M, \eta)$, where now

$$\eta : M^\sharp \to \mathbb{Q}.$$

Classical codes: where η takes values in $\mathbb{N}$.

Theorem *The mapping*

$$\eta_S \in \mathbb{Q}[\mathcal{O}^\sharp] \mapsto w_{\eta_S} \in \mathbb{Q}[\mathcal{O}]$$

is an isomorphism of vector spaces.

Uniqueness Theorem

$$\eta_S \in \mathbb{Q}[\mathcal{O}^\sharp] \mapsto w_{\eta_S} \in \mathbb{Q}[\mathcal{O}]$$

A code having constant weight means that w_{η_S} lies in a 1-dimensional subspace of $\mathbb{Q}[\mathcal{O}]$. Thus, virtual linear codes of constant weight form a 1-dimensional subspace of $\mathbb{Q}[\mathcal{O}^\sharp]$.

By clearing denominators and factoring out greatest common divisors, we obtain a minimal integral virtual code of constant weight.

All other integral examples are replications of the minimal example.

Caution: η_S may assume both positive and negative values.

Existence

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

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

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

Hamming case

Theorem *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 *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 *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 *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 *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 $k_{i,j}$, and $\nu(\lambda)$ measures the 2-divisibility of λ.

Corollary *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

Comments on linear two-weight codes

Suppose the nonzero elements $x \in M$ have one of two weights, a or b. In

$$\eta_S \in \mathbb{Q}[\mathcal{O}^\sharp] \mapsto w_{\eta_S} \in \mathbb{Q}[\mathcal{O}],$$

the difficulty lies in determining which orbits in M have weight a, say. This leads directly to the "projective sets" of Calderbank and Kantor.