Codes of constant Lee or Euclidean weight

Jay A. Wood*
Department of Mathematics
Purdue University Calumet†
Hammond, IN 46323 USA
wood@calumet.purdue.edu
http://www.calumet.purdue.edu/public/math/wood

WCC99, Paris
January 13, 1999

*Supported in part by Purdue University Calumet Scholarly Research Awards.

†A regional campus in the Purdue University system, located in northwest Indiana, about 30 miles (50km) southeast of downtown Chicago.

Thanks to Claude Carlet (Lee weights over $\mathbb{Z}/(2^m)$) and to Thann Ward (use of the extension theorem).

1. An example.

Over $R = \mathbb{Z}/(4)$, consider the generator matrix

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 2 & 2 & 2 & 0 \\ 0 & 1 & 2 & -1 & 1 & 1 & 0 & 2 & 2 \end{pmatrix}.$$

Then G generates a code C which is a free R-module of rank 2. The elements and their Euclidean weights follow.

0	0	0	0	0	0	0	0	0	0
1	1	1	1	0	2	2	2	0	16
2	2	2	2	0	0	0	0	0	16
−1	−1	−1	−1	0	2	2	2	0	16
0	1	2	−1	1	1	0	2	2	16
0	2	0	2	2	2	0	0	0	16
0	−1	2	1	−1	−1	0	2	2	16
1	2	−1	0	1	−1	2	0	2	16
1	−1	1	−1	2	0	2	2	0	16
1	0	−1	2	−1	1	2	0	2	16
2	−1	0	1	1	1	0	2	2	16
2	0	2	0	2	2	0	0	0	16
2	1	0	−1	−1	−1	0	2	2	16
−1	0	1	2	1	−1	2	0	2	16
−1	1	−1	1	2	0	2	2	0	16
−1	2	1	0	−1	1	2	0	2	16

This code has constant Euclidean weight 16.

2. Generalities.

Let $R = \mathbb{Z}/(p^k)$, p prime. *Linear codes* are submodules $C \subset R^n$. As an R-module,

$$C \cong (\mathbb{Z}/(p))^{l_1} \oplus (\mathbb{Z}/(p^2))^{l_2} \oplus \cdots \oplus (\mathbb{Z}/(p^k))^{l_k}.$$

Linear codes $C \subset R^n$ are determined by *coordinate functionals* $\lambda_1, \ldots, \lambda_n \in C^\sharp = \mathrm{Hom}_R(C, R)$.

The group $\mathrm{Aut}(C)$ of *module automorphisms* acts on C and on $C^\sharp$.

Weight function: assign a weight a_r to each $r \in R$; $a_0 = 0$. Then $w(x) = \sum_{i=1}^n a_{x_i} = \sum_{r \in R} a_r c_r(x)$. Here, $c_r(x) = |\{i : x_i = r\}|$, with $x \in R^n$.

Example. Lee weight on $\mathbb{Z}/(4)$: $a_0 = 0$, $a_1 = a_3 = 1$, $a_2 = 2$. Euclidean weight on $\mathbb{Z}/(4)$ has $a_2 = 4$ instead.

Proposition *If C has constant weight, then every element of* $\mathrm{Aut}(C)$ *is a code automorphism (i.e., preserves $w(x)$).*

3. Using the extension theorem.

Let $\mathcal{U}$ be the group of units of R. Define

$$\text{Sym}(w) = \{u \in \mathcal{U} : a_{ur} = a_r, r \in R\}.$$

For Lee or Euclidean weight, $\text{Sym}(w) = \{\pm 1\}$.

Theorem *Under a technical hypothesis on w, every code automorphism is a monomial transformation with units from* $\text{Sym}(w)$.

Theorem *Suppose C is a constant weight code. If λ is a coordinate functional of C, then, modulo* $\text{Sym}(w)$ *scaling, so is every other functional in the* $\text{Aut}(C)$*-orbit of λ. In addition, multiplicities are equal within orbits.*

4. Method of attack.

- Determine Aut(C).
- Determine orbits of Aut(C) on $C^\sharp$.
- Express $w(x)$ in terms of the numbers of orbits appearing.
- Use constant weight condition to find restrictions on the numbers of orbits which can appear.

5. An example.

Suppose $R = \mathbb{Z}/(4)$. Consider Euclidean weight, so that $\mathrm{Sym}(w) = \{\pm 1\}$. Also, suppose that C is a constant weight code and that C is a free module of rank 2.

$$\mathrm{Aut}(C) = GL_2(R) \quad (i.e., \det = \pm 1).$$

Orbits:

$$\left(\begin{array}{cccccc|cccccc} 1 & 1 & 1 & 1 & 0 & 2 & 2 & 0 & -1 & -1 & -1 & -1 \\ 0 & 1 & 2 & -1 & 1 & 1 & -1 & -1 & 1 & 2 & -1 & 0 \end{array}\right)$$

$$\begin{array}{ccc} 2 & 2 & 0 \\ 0 & 2 & 2 \end{array}$$

$$\begin{array}{c} 0 \\ 0 \end{array}$$

Assume no zero functionals, α_0 of the first type (modulo ± 1), α_1 of the second type.

Let x be the first row of the resulting generator matrix. (By symmetry, the same analysis works for the second row.)

$$\begin{aligned} w(x) &= 8\alpha_0 + 8\alpha_1 \\ w(2x) &= 16\alpha_0 \end{aligned}$$

Equality implies that $\alpha_0 = \alpha_1$. Thus any constant Euclidean weight code of rank 2 is a replication of our earlier example (which had $\alpha_0 = \alpha_1 = 1$).

(In the Lee case, $w(x) = 6\alpha_0 + 4\alpha_1$, $w(2x) = 8\alpha_0$, so that $\alpha_0 = 2\alpha_1$.)

6. Other results.

(a) Bonisoli (84): Hamming weight over fields. Use all nonzero linear functionals, modulo scalars

(b) Carlet (98): Lee weight over $\mathbb{Z}/(2^k)$. Use *all* the nonzero functionals.

(c) Euclidean weight over $\mathbb{Z}/(2^k)$, C free of rank l. There are k nonzero orbit types on $C^\sharp$; let $\alpha_0, \alpha_1, \ldots, \alpha_{k-1}$ denote their numbers. Then

$$\begin{aligned}
\alpha_0 &= t \\
\alpha_1 &= \frac{1}{2}(2^{l-1}+2)t \\
\alpha_2 &= \frac{1}{2}(2^{2(l-1)}+2^{l-1}+2)t \\
&\vdots \\
\alpha_{k-2} &= \frac{1}{2}(2^{(k-2)(l-1)}+\cdots+2^{l-1}+2)t \\
\alpha_{k-1} &= \frac{1}{4}(2^{(k-1)(l-1)}+\cdots+2^{l-1}+2)t
\end{aligned}$$

(d) Let $R = \mathbb{Z}/(p^2)$, p odd prime.

Proposition *A code has constant Lee weight if and only if it has constant Euclidean weight.*

Theorem *If* $C \cong (\mathbb{Z}/(p))^{l_1} \oplus (\mathbb{Z}/(p^2))^{l_2}$ *has constant weight, then* $l_2 = 0$ *or* $l_1 + l_2 \leq 2$.

The proofs all follow the same method of attack. The details are more complicated.