Codes of constant Lee or Euclidean weight

Jay A. Wood
Department of Mathematics, Computer Science & Statistics
Purdue University Calumet
Hammond, Indiana 46323–2094 USA
wood@calumet.purdue.edu
http://www.calumet.purdue.edu/public/math/wood

Abstract. Carlet [**2**] has determined the linear codes over $\mathbb{Z}/(4)$ of constant Lee weight. This extended abstract describes a different approach to this problem, along the lines of [**4**], which has the potential to apply to a wide class of examples. In particular, we show that linear codes of constant Lee or Euclidean weight seldom exist over $\mathbb{Z}/(p^2)$ when p is an odd prime.

Over finite fields, any linear code with constant Hamming weight is a replication of simplex (i.e., dual Hamming) codes. There are several proofs of this result, including [**1**], [**3**], and [**4**]. Recently, Carlet [**2**] has proved a similar result for linear codes of constant Lee weight over $\mathbb{Z}/(4)$, indeed, over any $\mathbb{Z}/(2^m)$.

In this extended abstract we generalize the approach of [**4**]. While more complicated than Carlet's proof, our approach has the potential to apply to a wide class of weight functions over any finite commutative chain ring.

For the purposes of this extended abstract, we will discuss codes over rings of the form $\mathbb{Z}/(p^2)$, p prime. In the case of $\mathbb{Z}/(4)$, we recover Carlet's result as Theorem 6. For p odd, we show in Theorem 11 that very few constant weight codes exist.

1991 *Mathematics Subject Classification.* Primary 94B05.

Key words and phrases. Constant weight codes, Lee weight, Euclidean weight, extension theorem.

Partially supported by Purdue University Calumet Scholarly Research Awards.

1. Linear codes as modules

Throughout this extended abstract, the ground ring will be $R = \mathbb{Z}/(p^2)$, p prime. It will be convenient to view $\mathbb{Z}/(p^2)$ as the set

$$\mathbb{Z}/(p^2) = \{t \in \mathbb{Z} : -p^2/2 < t \leq p^2/2\}. \tag{1}$$

Only for $p^2 = 4$ is equality possible in $t \leq p^2/2$. A *linear code* C of length n is a submodule of R^n.

The *Lee weight* $w(x)$ of any element $x = (x_1, \ldots, x_n) \in R^n$ is defined to be

$$w(x) = \sum_{i=1}^{n} a_{x_i}, \tag{2}$$

where $a_t = |t|$, with $t \in R$, as in (1). Similarly, the *Euclidean weight* uses $a_t = |t|^2$. We will denote both types of weight by $w(x)$; the context will make clear which is being discussed.

We wish to determine the linear codes of *constant weight*, i.e., codes for which there exists $L > 0$ with $w(x) = L$ for all nonzero $x \in C$. As above, $w(x)$ refers to a fixed choice of either Lee or Euclidean weight.

Observe that reduction mod p makes $\mathbb{Z}/(p)$ a module over $R = \mathbb{Z}/(p^2)$.

PROPOSITION 1. *Any linear code C is isomorphic, as an R-module, to a direct sum*

$$C \cong (\mathbb{Z}/(p))^{l_1} \oplus \left(\mathbb{Z}/(p^2)\right)^{l_2}. \tag{3}$$

A *linear automorphism* of C is any R-homomorphism $f : C \to C$ which is invertible. Note that this definition does not involve the weight function w, so that f need not be a code automorphism. However, if C has constant weight, then any linear automorphism f is a code automorphism. Denote the group of all linear automorphisms of C by $\mathrm{Aut}(C)$.

THEOREM 2. *For C as in* (3), $\mathrm{Aut}(C)$ *consists of all equivalence classes of matrices over R of the form*

$$A = \begin{pmatrix} M & N \\ pP & Q \end{pmatrix},$$

where M and Q are invertible. Two such matrices A, A' are equivalent if $M \equiv M' \bmod p$ and $N \equiv N' \bmod p$.

2. Orbit structures

The linear automorphism group $\mathrm{Aut}(C)$ acts on C and on $C^\sharp = \mathrm{Hom}_R(C, R)$, the linear dual of C. Our main interest is the action on $C^\sharp$. However, $C^\sharp \cong C$, so we will work directly with the action on C.

In the next theorem, we will denote elements of C as pairs $x = (x_{(1)}, x_{(2)})$, where $x_{(i)} \in \mathbb{Z}/(p^i)^{l_i}$, as in (3). An asterisk $*$ means the entry can assume any value; $p*$ means that every component of the entry is a multiple of p; u means that *at least one* component of the entry is a unit. We write e for the tuple $e = (1, 0, \ldots, 0)$.

Theorem 3. *The orbits of* $\mathrm{Aut}(C)$ *on* C *are as in Table 1.*

Orbit	Representative	Size
$(*, u)$	$(0, e)$	$p^{l_1+l_2}(p^{l_2} - 1)$
$(u, p*)$	$(e, 0)$	$(p^{l_1} - 1)p^{l_2}$
$(0, pu)$	$(0, pe)$	$p^{l_2} - 1$
$(0, 0)$	$(0, 0)$	1

Table 1. Orbits of $\mathrm{Aut}(C)$ on C.

3. Constant weight codes

A linear code $C \subset R^n$ can be viewed as an abstract R-module as in (3), equipped with an embedding in R^n. The embedding is given by n *coordinate functionals* $\lambda_1, \ldots, \lambda_n \in C^\sharp$. If C has a generator matrix G, then the columns of G are the values of the λ_i evaluated on a set of generators for C.

The main restriction on constant weight codes is that entire orbits of linear functionals must occur as coordinate functionals of C.

Theorem 4. *Let $C \subset R^n$ be a linear code of constant weight, either Lee or Euclidean weight. If $\lambda \in C^\sharp$ occurs as a coordinate functional of C, then (up to $\pm$ signs) every other linear functional μ in the* $\mathrm{Aut}(C)$*-orbit of λ also occurs as a coordinate functional of C.*

Proof. Given μ in the orbit of λ, there exists some $f \in \mathrm{Aut}(C)$ carrying λ to μ. On the other hand, f preserves weight (i.e., $w(f(x)) = w(x)$, for all $x \in C$), since C has constant weight. By the extension theorem [**5**], [**6**], f extends to a signed permutation automorphism of R^n. Thus $\pm\mu$ is another coordinate functional of C. □

A similar argument shows that $\pm\lambda$ and $\pm\mu$ occur with the same multiplicity.

REMARK 5. We caution the reader that Theorem 4 is a theorem only to the extent that the extension theorem holds for Lee or Euclidean weight. The extension theorem is *not* known for the general case of $R = \mathbb{Z}/(p^k)$. It holds for various small values of p^k where the conditions of [**5**] and [**6**] can be verified by hand.

4. Classification of constant weight codes: $p = 2$

A linear code of length n can always be viewed as a code of length $n+1$ by adding a zero entry, i.e., by enlarging the set of coordinate functionals $\lambda_1, \ldots, \lambda_n$ to include $\lambda_{n+1} = 0$. We call a linear code *nondegenerate* if it has no zero coordinate functionals.

THEOREM 6 (Carlet [**2**]). *Let C be a nondegenerate linear code of constant Lee weight over $R = \mathbb{Z}/(4)$. Then C is equivalent to the replication of a code D whose coordinate functionals consist of all the nonzero linear functionals on D.*

The linear codes C and D are isomorphic as R-modules, each of cardinality $2^{l_1} 4^{l_2} = 2^{l_1+2l_2}$. The code D has length $|D| - 1 = 2^{l_1+2l_2} - 1$, while the code C has length $r(2^{l_1+2l_2} - 1)$, for some positive integer r. Every nonzero element of D has Lee weight $L = |D| = 2^{l_1+2l_2}$, while every nonzero element of C has Lee weight rL.

Let us clarify some terminology. In the context of Lee or Euclidean weight, two linear codes of length n over R are *equivalent* if one can be obtained from the other by a signed permutation automorphism of R^n. This means the two codes have the same collections of coordinate functionals, up to ± signs. An r-fold *replication* of a code D of length n is a new code of length rn having the same coordinate functionals as D, but with each having multiplicity r.

PROOF. By Theorem 4, entire orbits of linear functionals (up to ± signs) must occur in the collection of coordinate functionals of C. Because C is nondegenerate, no zero functionals occur.

Referring to Table 1, let α, β, γ denote the number of times the orbits $(*, u)$, $(u, 2*)$, $(0, 2u)$, modulo ± signs (relevant for $(*, u)$ only), occur in the coordinate functionals of C.

For any $x \in R^n$, let $s_1(x) = |\{i : x_i = \pm 1\}|$ and $s_2(x) = |\{i : x_i = 2\}|$. Then $w(x) = s_1(x) + 2s_2(x)$. Note that $w(2x) = 2s_1(x)$.

Over $R = \mathbb{Z}/(4)$, any nonzero element of C has order 2 or 4. Suppose $x \in C$ has order 4. A consequence of constant Lee weight is that $w(x) = w(2x)$. It then follows that $s_1(x) = 2s_2(x)$. If y has order 2, then $s_1(y) = 0$, so that $w(y) = 2s_2(y)$. Because $2y = 0$, there is no additional restriction on $w(y)$.

Let $x = (0, e)$ and $y = (e, 0)$; x has order 4, while y has order 2. A detailed examination of the orbits in Table 1 reveals that

$$\begin{aligned} s_1(x) &= 2^{l_1+2l_2-2}\alpha, \\ s_2(x) &= 2^{l_1+l_2-2}(2^{l_2-1}-1)\alpha + (2^{l_1}-1)2^{l_2-1}\beta + 2^{l_2-1}\gamma, \\ s_2(y) &= 2^{l_1+l_2-2}(2^{l_2}-1)\alpha + 2^{l_1+l_2-1}\beta. \end{aligned}$$

From the constant weight conditions $w(x) = w(2x) = w(y)$, it follows that $s_1(x) = 2s_2(x) = s_2(y)$. We then conclude that $\beta = \gamma$ and $\alpha = 2\beta = 2\gamma$. Thus C is a β-fold replication of D. (Note that the orbit $(*, u)$ is effectively cut in half by the ± sign restriction. Having $\alpha = 2\beta$ restores the orbit to full size.) □

Example 7. For $l_1 = l_2 = 1$, the smallest example occurs when $\alpha = 2$, $\beta = \gamma = 1$. A generating matrix has the form

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

The code has cardinality 8, length 7, and constant Lee weight 8.

Turn now to Euclidean weight, so that the weight function w has $a_2 = 4$, as in (2). An argument similar to that in the proof of Theorem 6 shows that $\alpha = 2\beta$ and $\gamma = (2^{l_1+l_2-2}+1)\beta$. This proves the next theorem.

Theorem 8. *For a fixed isomorphism type* (3)*, there exists a linear code D of constant Euclidean weight having minimal length. The code D is unique up to equivalence. The cardinality of D is $|D| = 2^{l_1}4^{l_2} = 2^{l_1+2l_2}$, and its length is $2^{l_1+2l_2} - 1 + 2^{l_1+l_2-2}(2^{l_2}-1)$. Every nonzero element of D has Euclidean weight $L = 2|D| = 2^{l_1+2l_2+1}$.*

Any nondegenerate linear code C of constant Euclidean weight and having isomorphism type (3) *is equivalent to an r-fold replication of D.*

Example 9. If $l_1 = l_2 = 1$, then $\alpha = \gamma = 2\beta$. The smallest example has $\beta = 1$, $\alpha = \gamma = 2$. A generating matrix has the form

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

The code has cardinality 8, length 8, and constant Euclidean weight 16.

5. Classification of constant weight codes: p odd

When the prime p is odd, there are several surprises. One technical difference from the case of $p = 2$ is that $x = -x$ implies $x = 0$ when p

is odd. In contrast, $x = -x$ implies $x = 0$ or 2 in $\mathbb{Z}/(4)$. This affects the counting of orbits modulo ± signs.

Throughout this section $R = \mathbb{Z}/(p^2)$ with p an odd prime.

PROPOSITION 10. *A linear code has constant Lee weight over R if and only if it has constant Euclidean weight. The ratio of the weights is $p^2/3$.*

THEOREM 11. *Suppose C is a nondegenerate linear code over R of constant Lee or Euclidean weight. Then the isomorphism type* (3) *of C satisfies $l_2 = 0$ or $l_1 + l_2 \leq 2$.*

The code C is equivalent to an r-fold replication of a constant weight code D whose properties are listed in Table 2. The codes C and D are isomorphic as R-modules and of the same cardinality $|C| = |D| = p^{l_1+2l_2}$. The length and constant Lee weight of C are r times those of D.

When $l_2 = 0$, the coordinate functionals of D consist of all the nonzero linear functionals on D, modulo ± signs.

l_1	l_2	$\lvert D\rvert$	Length	Weight L
l_1	0	p^{l_1}	$(p^{l_1}-1)/2$	$p^{l_1}(p^2-1)/8$
0	1	p^2	$(p^3-2p+1)/2$	$p^3(p^2-1)/8$
1	1	p^3	$p(p^2-1)/2$	$p^3(p^2-1)/8$
0	2	p^4	$p^2(p^2-1)/2$	$p^4(p^2-1)/8$

TABLE 2. Properties of constant weight code D.

PROOF. We keep the notation from the proof of Theorem 6. If $l_2 = 0$, only orbit $(u, p*)$ can occur. Then $\alpha = \gamma = 0$, and β is arbitrary. When $l_2 > 0$, the constant weight condition implies that

$$\begin{aligned} ps_p(x) &= (p-1)s_1(x), \\ ps_1(x) &= s_p(y). \end{aligned}$$

The second condition occurs only when $l_1 > 0$.

In terms of orbit contributions (± signs are now relevant for all three types of orbits), we see that

$$\begin{aligned} s_1(x) &= p^{l_1+2l_2-2}\alpha, \\ s_p(x) &= (p^{l_1+2l_2-2} - p^{l_1+l_2-1})\alpha + (p^{l_1+l_2-1} - p^{l_2-1})\beta + p^{l_2-1}\gamma, \\ s_p(y) &= (p^{l_1+2l_2-1} - p^{l_1+l_2-1})\alpha + p^{l_1+l_2-1}\beta. \end{aligned}$$

From the condition $ps_1(x) = s_p(y)$ it follows that $\alpha = \beta$. From $ps_p(x) = (p-1)s_1(x)$ we obtain

$$(p^{l_1+l_2-2} - 1)\alpha + \gamma = 0.$$

Since $\alpha, \gamma \geq 0$, there are only zero solutions once $l_1 + l_2 > 2$.

The reader may verify the other claims and cases. □

Example 12. Let $l_1 = 2$, $l_2 = 0$. Then $\alpha = \gamma = 0$, with β arbitrary. The shortest example has $\beta = 1$. Over $R = \mathbb{Z}/(9)$, a generating matrix has the form

$$G = \begin{pmatrix} 3 & 3 & 3 & 0 \\ 0 & 3 & -3 & 3 \end{pmatrix}.$$

The code has cardinality 9, length 4, constant Lee weight 9, and constant Euclidean weight 27.

Over $R = \mathbb{Z}/(25)$, a generating matrix has the form

$$G = \begin{pmatrix} 5 & 5 & 5 & 5 & 5 & 10 & 10 & 10 & 10 & 10 & 0 & 0 \\ 0 & 5 & 10 & -10 & -5 & 0 & 5 & 10 & -10 & -5 & 5 & 10 \end{pmatrix}.$$

The code has cardinality 25, length 12, constant Lee weight 75, and constant Euclidean weight 625.

Example 13. Let $l_1 = 0$, $l_2 = 1$. Then $\beta = 0$ and $(p-1)\alpha = p\gamma$. The shortest example has $\alpha = p$, $\gamma = p - 1$. Over $R = \mathbb{Z}/(9)$, a generating matrix has the form

$$G = \begin{pmatrix} 1 & 2 & 4 & 1 & 2 & 4 & 1 & 2 & 4 & 3 & 3 \end{pmatrix}.$$

The code has cardinality 9, length 11, constant Lee weight 27, and constant Euclidean weight 81.

Over $R = \mathbb{Z}/(25)$, a generating matrix G has one row, consisting of 5 copies of

$$1 \quad 2 \quad 3 \quad 4 \quad 6 \quad 7 \quad 8 \quad 9 \quad 11 \quad 12$$

concatenated with 4 copies of

$$5 \quad 10.$$

The code has cardinality 25, length 58, constant Lee weight 375, and constant Euclidean weight 3125.

Example 14. Let $l_1 = 1$, $l_2 = 1$. Then $\gamma = 0$ and $\alpha = \beta$. The shortest example has $\alpha = \beta = 1$. Over $R = \mathbb{Z}/(9)$, a generating matrix has the form

$$G = \begin{pmatrix} 0 & 3 & -3 & 0 & 3 & -3 & 0 & 3 & -3 & 3 & 3 & 3 \\ 1 & 1 & 1 & 2 & 2 & 2 & 4 & 4 & 4 & 0 & 3 & -3 \end{pmatrix}.$$

The code has cardinality 27, length 12, constant Lee weight 27, and constant Euclidean weight 81.

EXAMPLE 15. Let $l_1 = 0$, $l_2 = 2$. Then $\beta = \gamma = 0$, with α arbitrary. The shortest example has $\alpha = 1$. Over $R = \mathbb{Z}/(9)$, a generating matrix has the form

$$G = \begin{pmatrix} 1 & 2 & 4 & 0 & 0 & 0 & 3 & 3 & 3 & -3 & -3 & -3 \\ * & * & * & 1 & 2 & 4 & 1 & 2 & 4 & 1 & 2 & 4 \end{pmatrix},$$

where $*$ indicates 9 entries, running over the elements of $\mathbb{Z}/(9)$. The code has cardinality 81, length 36, constant Lee weight 81, and constant Euclidean weight 243.

6. Possible generalizations

The major ideas in this extended abstract generalize to any finite commutative chain ring (i.e., local, with principal ideals). However, there are serious technical and notational difficulties to be overcome in order to understand the orbit structure of $\mathrm{Aut}(C)$ on C and to manipulate the equations arising from the constant weight condition.

ACKNOWLEDGMENTS. I thank the referee and C. Carlet for their advice on revising this extended abstract.

References

[1] A. Bonisoli, *Every equidistant linear code is a sequence of dual Hamming codes*, Ars Combin. **18** (1984), 181–186.

[2] C. Carlet, *One-weight $\mathbb{Z}_4$-linear codes*, preprint, 1998.

[3] H. N. Ward, *A bound for divisible codes*, IEEE Trans. Inform. Theory **38** (1992), 191–194.

[4] H. N. Ward and J. A. Wood, *Characters and the equivalence of codes*, J. Combin. Theory, series A **73** (1996), 348–352.

[5] J. A. Wood, *Weight functions and the extension theorem for linear codes over finite rings*, Finite Fields: Theory, Applications and Algorithms (R. C. Mullin and G. L. Mullen, eds.), Contemp. Math., vol. 225, Amer. Math. Soc., Providence, 1999, pp. 231–243.

[6] ______, *Factoring the semigroup determinant of a finite commutative chain ring*, Lecture Notes in Comput. Sci., Springer-Verlag, (to appear).