Linear Codes over $\mathbb{Z}/(2^k)$ of Constant Euclidean Weight

Jay A. Wood
Department of Mathematics, Computer Science & Statistics
Purdue University Calumet
Hammond, Indiana 46323–2094
wood@calumet.purdue.edu

Over finite fields, any linear code with constant Hamming weight is a replication of simplex (i.e., dual Hamming) codes [**1**]. Recently, Carlet [**2**] proved a similar result for linear codes of constant Lee weight over $\mathbb{Z}/(2^k)$. In this short paper we prove the existence of linear codes of constant Euclidean weight over $\mathbb{Z}/(2^k)$.

Throughout this paper, the ground ring will be $R = \mathbb{Z}/(2^k)$. A *linear code* of length n is a submodule of R^n, and it will be viewed as an underlying finite R-module M equipped with a linear embedding $\lambda : M \to R^n$ given by n *coordinate functionals* $\lambda_1, \ldots, \lambda_n \in M^\sharp := \mathrm{Hom}_R(M, R)$. Taking representatives satisfying $-2^{k-1} < t \leq 2^{k-1}$, the *Euclidean weight* of $t \in R$ is $w(t) = t^2 \in \mathbb{Z}$. The Euclidean weight of $x \in M$ is $w(x) = \sum w(\lambda_i(x)) \in \mathbb{Z}$. A linear code has *constant Euclidean weight* $L > 0$ if $w(x) = L$ for all nonzero $x \in M$.

Any finite R-module M determines nonnegative integers $l_1, l_2, \ldots, l_k$ so that

$$M \cong \bigoplus_{i=1}^{k} \left(\mathbb{Z}/(2^i)\right)^{l_i}, \tag{1}$$

as R-modules. Set $e_0 = 1$ and $e_i = l_1 + 2l_2 + \cdots + (i-1)l_{i-1} + i(l_i + \cdots + l_k) - i$, for $1 \leq i \leq k$. The R-module $M^\sharp$ admits a filtration (its upper Loewy chain)

$$M^\sharp \supset 2M^\sharp \supset 4M^\sharp \supset \cdots \supset 2^{k-1}M^\sharp \supset 2^k M^\sharp = 0. \tag{2}$$

For $\lambda \in M^\sharp$, let $\nu(\lambda)$ be the largest exponent such that $\lambda \in 2^{\nu(\lambda)}M^\sharp$.

THEOREM. *Let M be any module over $R = \mathbb{Z}/(2^k)$ of the form (1), with $l_k \geq 1$. As coordinate functionals, use every nonzero linear functional $\lambda \in M^\sharp$, with multiplicity*

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

Then this linear code has cardinality, length, and constant Euclidean weight given by

$$|M| = 2^{l_1 + 2l_2 + \cdots + kl_k},\ n = \frac{|M|}{2^{k-1}}\left(3 \cdot 2^{k-1} - 1\right) - m_{k-1},\ \text{and } L = 2^{2k-2}|M|.$$

PROOF. First note that since we assume $l_k \geq 1$, 2^k divides $|M|$, and n is an integer.

Partially supported by Purdue University Calumet Scholarly Research Awards.

$$w(x) = \sum_{\lambda \in M^\sharp} m_{\nu(\lambda)} w(\lambda(x)) = \sum_{j=0}^{k-1} 2^{e_j} \sum_{\lambda \in 2^j M^\sharp} w(\lambda(x)). \tag{3}$$

Now consider the linear functional $\check{x} : 2^j M^\sharp \to R$, $\lambda \mapsto \lambda(x)$. Suppose x has order 2^i. If $i \le j$, the functional $\check{x}$ is zero. When $i > j$, the image $\mathrm{im}(\check{x}) = \check{x}(2^j M^\sharp) = (2^{k-i+j})$, with $|\mathrm{im}(\check{x})| = 2^{i-j}$. In the latter case, every $r \in \mathrm{im}(\check{x})$ is hit equally often by $\check{x}$, namely

$$|\ker(\check{x})| = \frac{|2^j M^\sharp|}{|\mathrm{im}(\check{x})|} = 2^{l_{j+1}+2l_{j+2}+\cdots+(k-j)l_k - i + j}$$

times. It is straight forward to show that, for Euclidean weight,

$$3 \sum_{r \in (2^\mu)} w(r) = 2^{k+\mu-1} \left(2^{2k-2\mu-1} + 1\right). \tag{4}$$

Remembering that x has order 2^i and using $\mu = k - i + j$ in (4), we conclude that

$$3 \sum_{\lambda \in 2^j M^\sharp} w(\lambda(x)) = \begin{cases} 0, & i \le j, \\ 2^{l_{j+1}+2l_{j+2}+\cdots+(k-j)l_k} \left(1 + 2^{-2i+2j+1}\right) 2^{2k-2}, & i > j. \end{cases}$$

This last expression allows us to rewrite (3) as

$$3w(x) = \sum_{j=0}^{i-1} 2^{e_j + l_{j+1}+2l_{j+2}+\cdots+(k-j)l_k} \left(1 + 2^{-2i+2j+1}\right) 2^{2k-2}. \tag{5}$$

Observe that the complicated exponent in (5) simplifies to

$$e_j + l_{j+1} + 2l_{j+2} + \cdots + (k-j)l_k = \begin{cases} 1 + \sum_{q=1}^{k} q l_q, & j = 0, \\ -j + \sum_{q=1}^{k} q l_q, & j > 0. \end{cases}$$

Since $\log_2 |M| = \sum_{q=1}^{k} q l_q$, (5) simplifies to

$$3w(x) = 2|M| \left(1 + 2^{-2i+1}\right) 2^{2k-2} + \sum_{j=1}^{i-1} |M|\, 2^{-j} \left(1 + 2^{-2i+2j+1}\right) 2^{2k-2}.$$

By summing the geometric series and simplifying, we obtain the constant weight

$$w(x) = 2^{2k-2}|M|.$$

The remaining claims of the theorem can be verified easily. □

REMARK. It can also be proved that the above is essentially the only way to obtain linear codes of constant Euclidean weight over $\mathbb{Z}/(2^k)$. Up to code equivalence (permutations and sign changes of the λ_i) and padding with zeros, every linear code on M of constant Euclidean weight is a replication of the one in the Theorem. (If the multiplicities m_i are not relatively prime, first scale them by their GCD. This gives a "minimal model.") This result will appear in subsequent work of the author.

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.

URL: `http://www.calumet.purdue.edu/public/math/wood/`