ON THE EXTENDED LEE WEIGHTS MODULO 2^e OF LINEAR CODES OVER $\mathbb{Z}_{2^s}$

BAHATTİN YILDIZ AND ZEYNEP ÖDEMİŞ ÖZGER

ABSTRACT. In this work, linear codes over $\mathbb{Z}_{2^s}$ are considered together with the extended Lee weight that is defined as

$$w_L(x) = \begin{cases} x & \text{if } x \leq 2^{s-1}, \\ 2^s - x & \text{if } x > 2^{s-1}. \end{cases}$$

The ideas used by Wilson and Yıldız are employed to obtain divisibility properties for sums involving binomial coefficients and the extended Lee weight. These results are then used to find bounds on the power of 2 that divides the number of codewords whose Lee weights fall in the same congruence class modulo 2^e. Comparisons are made with the results for the trivial code and the results for the homogeneous weight.

1. INTRODUCTION

There has been a burst of activity on linear codes over rings in recent years. Starting from the ring $\mathbb{Z}_4$ with [1], the research in this area has been generalized to $\mathbb{Z}_{2^k}$, $\mathbb{Z}_{p^k}$, Galois rings and finite chain rings in general. The weight function used in codes over $\mathbb{Z}_4$ is the so called Lee weight that has values $w_L(0) = 0, w_L(1) = w_L(3) = 1$ and $w_L(2) = 2$. When generalizing to Galois rings and finite chain rings in general a new weight called the homogeneous weight was introduced as an extension of the Lee weight on $\mathbb{Z}_4$. We refer the reader to [2] for more details.

The homogeneous weight uses the algebraic structure of the rings and has few non-zero weights. It also has connections with exponential sums and thus, results from number theory can be used to obtain bounds for this weight([3], [4]). Recently, in [5], when constructing the Gray map for the homogeneous weight over Galois rings, it was discovered that the homogenous weight also has connections with hyperplanes in combinatorial

---

Date: November 07, 2012.

2000 *Mathematics Subject Classification*. Primary 94B05; Secondary 94B65.

Key words and phrases. Linear codes, enumerators, Gray map, codes over rings.

This paper is in final form and no version of it will be submitted for publication elsewhere.

geometries. The algebraic constructions for the Gray map of homogeneous weight are given in [2] and [6].

However there is a more natural generalization of the Lee weight from $\mathbb{Z}_4$ to $\mathbb{Z}_{2^k}$. This was given first in [7] by Carlet, however he chose the homogeneous weight instead of this weight to work with. Recently, Dougherty and Fernández-Córdoba have studied linear codes over $\mathbb{Z}_{2^k}$ with respect to this extended Lee weight in [8].

The constraints on the weight enumerators of codes have been of interest in coding theory. Pless looked at the Hamming weight enumerators of binary codes in [9]. Wilson used polynomial ideas to obtain such constraints for general weight functions on codes in a more general context in [10]. Yıldız used ideas from [10] to obtain the best possible results for the Lee weights of linear codes over $\mathbb{Z}_4$ in [6]. In [11] a coset decomposition idea was used to obtain the tightest bounds for the homogeneous weight enumerators of linear codes over Galois rings.

In this work we study linear codes over $\mathbb{Z}_{2^s}$ with the extended Lee weight to prove divisibility results for the weight enumerators using ideas from [10]. Our aim is to combine tools from [10] and [6] to find the power of 2 that divides the coefficients of the extended Lee weight enumerators of linear codes over $\mathbb{Z}_{2^s}$.

The rest of the paper is organized as follows.

In section 2, we give the necessary definitions for codes over $\mathbb{Z}_{2^s}$ and the extended Lee weight. In section 3, we state and prove the main lemmas to be used in obtaining the main results. Section 4 includes the main results for free $\mathbb{Z}_{2^s}$-codes. In section 5 we find the results for the trivial code for comparison. Section 6 concludes the paper with remarks and possible research directions.

2. Linear codes over $\mathbb{Z}_{2^s}$

Definition 1. *A linear code over a ring R of length n is an R-submodule of R^n; more specifically a linear code over $\mathbb{Z}_{2^s}$ of length j is a submodule of $\mathbb{Z}_{2^s}^j$.*

It can be shown, because of the ideal structure of $\mathbb{Z}_{2^s}$, that a linear code over $\mathbb{Z}_{2^s}$ of length j is permutationally equivalent to a code that has a generating matrix of the following form:

$$\begin{bmatrix} I_{k_1} & A_1 & \cdot & \cdot & \cdot & A_{s-1} & A_s \\ 0 & 2I_{k_2} & 2B_1 & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 2^2 I_{k_3} & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 2^{s-2} I_{k_{s-1}} & 2^{s-2} D & 2^{s-2} E \\ 0 & 0 & \cdot & 0 & 0 & 2^{s-1} I_{k_s} & 2^{s-2} F \end{bmatrix}$$

where $A_1, \cdots, A_s, B_1, \cdots, D, E, F$ are matrices over $\mathbb{Z}_{2^s}$ (see [14]). As seen from the generating matrix, a dimension can not be defined for such codes. Instead of dimension, a code over $\mathbb{Z}_{2^s}$ has a type. A code that has the above matrix as a generating matrix is said to be of type $(2^s)^{k_1}(2^{s-1})^{k_2}\cdots(2)^{k_s}$, and it has size

$$|C| = 2^{sk_1+(s-1)k_2+\cdots+k_s}.$$

For the rest of this work we will let the extended Lee weight on $\mathbb{Z}_{2^s}$ be defined as follows:

$$w_L(x) := \begin{cases} x & \text{if } x \leq 2^{s-1}, \\ 2^s - x & \text{if } x > 2^{s-1}, \end{cases}$$

The Gray map from $\mathbb{Z}_{2^s}$ to $\mathbb{F}_2^{2^{s-1}}$ for this weight function can be given simply as:

$$\begin{array}{lcl} 0 & \to & (000\cdots000), \\ 1 & \to & (100\cdots000), \\ 2 & \to & (110\cdots000), \\ & \cdot & \\ & \cdot & \\ 2^{s-1} & \to & (111\cdots111), \\ 2^{s-1}+1 & \to & (011\cdots111), \\ 2^{s-1}+2 & \to & (001\cdots111), \\ & \cdot & \\ & \cdot & \\ 2^s-2 & \to & (000\cdots011), \\ 2^s-1 & \to & (000\cdots001), \end{array}$$

which is introduced in [16] for $\mathbb{Z}_{2k}$-linear codes by Borges et al. Simply put 1' s in the first x coordinates and 0' s in the other coordinates for all $x \leq 2^{s-1}$, and if $x > 2^{s-1}$ then the Gray map takes x to $\overline{1} + \varphi_L(2^{s-1} - x)$, where φ_L is the Gray map for w_L. This map can be extended for a codeword $\overline{c} = (c_1, c_2, \ldots, c_n)$ as follows:

$$\varphi_L(\overline{c}) = (\varphi_L(c_1), \varphi_L(c_2), \ldots, \varphi_L(c_n)).$$

Note that φ_L is a (non-linear) isometry from ($\mathbb{Z}_{2^s}$, Lee weight) to ($\mathbb{F}_2^{2^{s-1}}$, Hamming weight).

3. The main lemma

We start with the following remarks:

Remark 1. *For any $x \in \mathbb{Z}_{2^s}$,*

$$w_L(x) + w_L(x + 2^{s-1}) = 2^{s-1}.$$

Remark 2. [11] *Let C be a linear code over $\mathbb{Z}_{2^s}$ of length j and type $(2^s)^{k_1}(2^{s-1})^{k_2}\cdots(2)^{k_s}$ with*

$$\begin{aligned}
\overline{a}_1, \overline{a}_2, \ldots, \overline{a}_{k_1} &\longrightarrow \text{ free generators,}\\
\overline{b}_1, \overline{b}_2, \ldots, \overline{b}_{k_2} &\longrightarrow \text{ generators in } 2\mathbb{Z}_{2^s},\\
&\cdot\\
&\cdot\\
&\cdot\\
\overline{c}_1, \overline{c}_2, \ldots, \overline{c}_{k_s} &\longrightarrow \text{ generators in } 2^{s-1}\mathbb{Z}_{2^s},
\end{aligned}$$

and let $\widetilde{C}$ be the linear code over $2^{s-1}\mathbb{Z}_{2^s}$ generated by

$$\begin{aligned}
&2^{s-1}\overline{a}_1, 2^{s-1}\overline{a}_2, \ldots, 2^{s-1}\overline{a}_{k_1},\\
&2^{s-2}\overline{b}_1, 2^{s-2}\overline{b}_2, \ldots, 2^{s-2}\overline{b}_{k_2},\\
&\cdot\\
&\cdot\\
&\cdot\\
&\overline{c}_1, \overline{c}_2, \ldots, \overline{c}_{k_s},
\end{aligned}$$

then $\widetilde{C}$ is a linear subcode of C and, moreover

$$C = \bigcup_{\overline{c}\in\mathbb{Z}_{2^s}^j} (\overline{c} + \widetilde{C}),$$

where $\overline{c}$'s are in $\mathbb{Z}_{2^s}^j$. The exact coset representatives can be found in [11].

For the rest of this paper S_C is defined as the following:

Definition 2. *For C, a subset of $\mathbb{Z}_{2^s}^j$ (in fact, C is either a subgroup or a coset of a subgroup) we define*

$$S_C(i_1, \cdots, i_j) := \sum_{(a_1,a_2,\ldots,a_j)\in C} \binom{w_L(a_1)}{i_1}\binom{w_L(a_2)}{i_2}\cdots\binom{w_L(a_j)}{i_j},$$

where $0 \le i_1, i_2, \cdots, i_j \le j$ such that

$$i_1 + i_2 + \cdots + i_j = j.$$

The following is the main result we would like to obtain.

Theorem 1. *Let C be a linear code over $\mathbb{Z}_{2^s}$ of type $(2^s)^{k_1}(2^{s-1})^{k_2}\cdots(2)^{k_s}$, then for any fixed $i_1, i_2, \ldots, i_j$ with $0 \le i_1, i_2, \ldots, i_j \le j$ and $i_1+i_2+\cdots+i_j = j$, we have*

$$S_C(i_1, \cdots, i_j) \equiv 0 \pmod{2^{2\cdot[k_1+k_2+\ldots+k_s]-j}}.$$

Note that by Remark 2, to prove the above theorem, it is enough to prove the following lemma:

Lemma 1. *Let C be a linear code over $2^{s-1}\mathbb{Z}_{2^s}$ of length j and dimension k. Then*

$$S_{\overline{a}+C}(i_1,\cdots,i_j)\equiv 0 \pmod{2^{2k-j}}$$

for any $\overline{a}\in\mathbb{Z}_{2^s}^j$ and $i_1,\cdots,i_j\in\mathbb{Z}_{2^s}$ such that $i_1+i_2+\cdots+i_j=j$.

Proof. The proof is by induction on j. Let $j=1$ and $k=1$. Then $C=\{(0),(2^{s-1})\}$. Hence

$$S_C(1)=\binom{w_L(0)}{1}+\binom{w_L(2^{n-1})}{1}=2^{s-1}\equiv 0 \pmod{2^{2.1-1}}$$

and if $a\in\mathbb{Z}_{2^s}$ is any coordinate, then

$$S_{\overline{a}+C}(1)=w_L(a)+w_L(a+2^{s-1})=2^{s-1}$$

by Remark 1. Assume that the induction hypothesis is true for $j-1$. It remains to show that the claim is true also for j. For the sake of simplicity, we drop $(i_1,\cdots,i_j)$ in the notation. There are two cases:
Case 1: Let $i_1=i_2=\cdots=i_j=1$ and $\overline{a}\in\mathbb{Z}_{2^s}^j$, $\overline{a}=(a_1,a_2,\ldots,a_j)$. Then

$$S_{\overline{a}+C}=w_L(a_1)\cdot S_{\dot{\overline{a}}+\dot{C}_0}+w_L(a_1+2^{s-1})\cdot S_{\dot{\overline{a}}+\dot{C}_{2^{s-1}}},$$

where C_ℓ is the set of codewords that have ℓ as their first coordinates ($\ell=0$ or 2^{s-1}), $\dot{C}_\ell$ is the set of codewords whose first coordinates, which are ℓ, are deleted and $\dot{\overline{a}}$ is the codeword that is obtained from $\overline{a}$ by deleting its first coordinate. Now when deleting a coordinate from C , there can be two situations. Either the dimension does not change or two copies of a code with dimensions decreased by one occur. In the first case, the following holds:

$$\begin{aligned}S_{\overline{a}+C}&=w_L(a_1)\cdot S_{\dot{\overline{a}}+\dot{C}_0}+(2^{s-1}-w_L(a_1))\cdot S_{\dot{\overline{a}}+\dot{C}_{2^{s-1}}}\\&=w_L(a_1)\cdot S_{\dot{\overline{a}}+\dot{C}_0}+w_L(a_1)\cdot S_{\dot{\overline{a}}+\dot{C}_{2^{s-1}}}\\&+(2^{s-1}-2\cdot w_L(a_1))\cdot S_{\dot{\overline{a}}+\dot{C}_{2^{s-1}}}\\&=w_L(a_1)\cdot S_{\dot{\overline{a}}+\dot{C}}+2\cdot\left[2^{s-2}-w_L(a_1)\right]\cdot S_{\dot{\overline{a}}+\dot{C}_{2^{s-1}}}\end{aligned}$$

Now by induction hypothesis,

$$S_{\dot{\overline{a}}+\dot{C}}\equiv 0 \pmod{2^{2k-(j-1)}},$$

and

$$S_{\dot{\overline{a}}+\dot{C}_{2^{s-1}}}\equiv 0 \pmod{2^{2(k-1)-(j-1)}}.$$

Hence

$$2\cdot\left[2^{s-2}-w_L(a_1)\right]\cdot S_{\dot{\overline{a}}+\dot{C}_{2^{s-1}}}\equiv 0 \pmod{2^{2k-j}}.$$

This proves that

$$S_{\overline{a}+C} \equiv 0 \pmod{2^{2k-j}},$$

which means $S_{\overline{a}+C}$ is divisible by 2^{2k-j}. Now in the second case, $C_0 = \dot{C}_{2^s-1}$ is a code of length $j-1$ and dimension $k-1$, then

$$\begin{aligned} S_{\overline{a}+C} &= w_L(a_1) \cdot S_{\dot{\overline{a}}+\dot{C}_0} + (2^{s-1} - w_L(a_1)) \cdot S_{\dot{\overline{a}}+\dot{C}_0} \\ &= 2^{s-1} \cdot S_{\dot{\overline{a}}+\dot{C}_0}. \end{aligned}$$

Hence,

$$S_{\overline{a}+C} \equiv 0 \pmod{2^{2k-j}},$$

since $S_{\dot{\overline{a}}+\dot{C}_0} \equiv 0 \pmod{2^{2k-j-1}}$.

Case 2: Assume that one of i_k' s is greater than 1, where $1 \leq k \leq j$. Then, since $i_1 + i_2 + \cdots + i_j = j$ must hold, at least one of them should be 0. Supposing that one of the i_k's is r, with $r \geq 2$, this implies at least $r-1$ of i_k' s are 0. Without loss of generality $i_1 = 0, i_2 = 0, \ldots, i_{r-1} = 0, i_r = r$ may be assumed. Now,

$$S_C = \sum_{(a_1,a_2,\cdots,a_r,\cdots,a_j)\in C} \binom{w_L(a_1)}{0}\binom{w_L(a_2)}{0}\cdots\binom{w_L(a_r)}{r}\cdots\binom{w_L(a_j)}{i_j}.$$

Let $\overline{C}$ be the code that is obtained by deleting the first r coordinates of C. Then,

$$S_C = \sum_{a_r}\binom{w_L(a_r)}{r} \cdot \sum_{(a_{r+1},\cdots,a_j)\in\overline{C}} \binom{w_L(a_{r+1})}{i_{r+1}}\cdots\binom{w_L(a_j)}{i_j}.$$

So, $\overline{C}$ is either of the same dimension of C or 2^ℓ copies of a $k-\ell$ dimensional code for some $\ell \in \mathbb{N}$, where $\ell \leq r$. Then by induction hypothesis $S_{\overline{C}}$ is divisible by

$$2^{\ell+2(k-\ell)-(j-r)} = 2^{2k+r-\ell-j}.$$

But we know that $r \geq \ell$, so

$$\sum_{a_r}\binom{w_L(a_r)}{r} \cdot \sum_{(a_{r+1},\cdots,a_j)\in\overline{C}} \binom{w_L(a_{r+1})}{i_{r+1}}\cdots\binom{w_L(a_j)}{i_j} \equiv 0 \pmod{2^{2k-j}},$$

which means S_C is divisible by 2^{2k-j}. ∎

4. Linear codes over $\mathbb{Z}_{2^s}$ of type $(2^s)^k$

In this section, the results in [10] will be specialized to the extended Lee weight enumerators of codes over $\mathbb{Z}_{2^s}$ by using the same techniques and tools in [10] that are introduced in the proof of the following lemma.

Lemma 2. [10] *Let p be a prime, and e and m positive integers. Let f be an integer-valued function on the integers that is periodic of period p^e. There exists a polynomial*

$$w(x) = c_0 + c_1 x + c_2 \binom{x}{2} + \cdots + c_d \binom{x}{d}$$

of degree $d \leq (m(p-1)+1)p^{e-1} - 1$ so that

$$w(t) \equiv f(t) \pmod{p^m}$$

for all integers t. The coefficients c_i are integers and, moreover,

$$c_i \equiv 0 \pmod{p^\ell},$$

whenever $i \geq (\ell(p-1)+1)p^{e-1}$.

The following is the main theorem we would like to prove:

Theorem 2. *Suppose C is a linear code of type $(2^s)^k$ over $\mathbb{Z}_{2^s}$. If we denote by $N_C(j, 2^e)$ the number of codewords in C that have Lee weights congruent to j modulo 2^e, then we have*

$$N_C(j, 2^e) \equiv 0 \pmod{2^{\left\lfloor \frac{sk - 2^{e-1}(s-1)}{2^{e-1}(s-1)} \right\rfloor}},$$

where $j = 0, 1, 2, \ldots, 2^e - 1$. Here $\lfloor \cdot \rfloor$ denotes the floor function.

Proof. For any nonnegative integers t and m, let $d = (m+1)2^{e-1} - 1$, and let

$$W_t(x) = \sum_{i=0}^{d} c_i \binom{x}{i}$$

be a polynomial of degree $\leq d$ so that

$$W_t(j) \equiv \begin{cases} 1 \pmod{2^m} & \text{if } j \equiv t \pmod{2^e}, \\ 0 \pmod{2^m} & \text{otherwise,} \end{cases}$$

where $c_i \equiv 0 \pmod{2^\ell}$ for $i \geq (\ell+1)2^{e-1}$. The existence of this polynomial is guaranteed by the proof of Lemma 2. Then we have

$$N_C(j, 2^e) \equiv \sum_{\overline{a} \in C} W_t(w_L(\overline{a})) \equiv \sum_{j=0}^{d} c_j \sum_{\overline{a} \in C} \binom{w_L(\overline{a})}{j} \pmod{2^m}.$$

Given j, choose an integer ℓ such that

$$(\ell+1)2^{e-1} \leq j \leq (\ell+2)2^{e-1} - 1.$$

Then $c_j \equiv 0 \pmod{2^\ell}$. Consider

$$\begin{aligned} T_j \ :\ &= \sum_{\overline{a}\in C} \binom{w_L(\overline{a})}{j} \\ &= \sum_{(a_1,a_2,\ldots,a_n)\in C} \binom{w_L(a_1)+w_L(a_2)+\cdots+w_L(a_n)}{j} \\ &= \sum_{\substack{i_1+i_2+\cdots+i_n=j \\ i_1,i_2,\ldots,i_n\geq 0}} \sum_{(a_1,a_2,\ldots,a_n)\in C} \binom{w_L(a_1)}{i_1}\binom{w_L(a_2)}{i_2}\cdots\binom{w_L(a_n)}{i_n}. \end{aligned}$$

For fixed nonnegative $i_1, i_2, \ldots, i_n$ summing to j, at most j of indices i_v are non-zero. For notational convenience we might assume $i_t = 0$ for $t > j$. Then

$$\begin{aligned} &\sum_{\bar{a}\in C} \binom{w_L(a_1)}{i_1}\binom{w_L(a_2)}{i_2}\cdots\binom{w_L(a_n)}{i_n} \\ &= \sum_{(b_1,b_2,\ldots,b_j)\in\mathbb{Z}_{2^s}^j} \Phi(b_1,b_2,\cdots,b_j)\binom{w_L(b_1)}{i_1}\cdots\binom{w_L(b_j)}{i_j}, \end{aligned}$$

where $\Phi(b_1, b_2, \ldots, b_j)$ is the number of $\overline{a} \in C$ with first j coordinates $b_1, b_2, \ldots, b_j$ in that order. The set of such $\overline{a}$'s is either empty or is a coset of the kernel K of the group homomorphism $C \to \mathbb{Z}_{2^s}^j$ that projects onto the first j coordinates, which is of order 2^t where $t = sk - (sj - r)$. There are two cases:

Case 1: Suppose the image of this projection has size 2^{sj-r}, where $r > j$. Then K has order 2^t where $t = sk - (sj - r) > sk - (s - 1)j$.

Case 2: If the image of the homomorphism has size 2^{sj-r} with $r \leq j$, then we get

$$\begin{aligned} (4.1)\qquad &\sum_{\overline{a}\in C} \binom{w_L(a_1)}{i_1}\binom{w_L(a_2)}{i_2}\cdots\binom{w_L(a_n)}{i_n} \\ &= 2^{sk-sj+r} \sum_{(b_1,b_2,\ldots,b_j)\in H} \binom{w_L(b_1)}{i_1}\binom{w_L(b_2)}{i_2}\cdots\binom{w_L(b_j)}{i_j}, \end{aligned}$$

where H is the image of the homomorphism, and as such, is a subgroup of $\mathbb{Z}_{2^s}^j$. Here H can be seen as a code over $\mathbb{Z}_{2^s}$ of length j. Then by Theorem 1

$$\sum_{(b_1,b_2,\ldots,b_j)\in H} \binom{w_L(b_1)}{i_1}\binom{w_L(b_2)}{i_2}\cdots\binom{w_L(b_j)}{i_j}$$

is divisible by $2^{2j-j} = 2^j > 2^{j-r}$. Putting these in equation (4.1), we see that the sum in (4.1) is divisible by $2^{sk-(s-1)j}$.

This means that in both cases, which are investigated above,

$$\sum_{\overline{a}\in C} \binom{w_L(a_1)}{i_1}\binom{w_L(a_2)}{i_2}\cdots\binom{w_L(a_n)}{i_n}$$

is divisible by $2^{sk-(s-1)j}$.

Now suppose $k \geq \frac{2(s-1)}{s}(m+1)2^{e-2}$. Then we have

$$\begin{aligned} sk-(s-1)j &\geq 2(s-1)(m+1)2^{e-2} - (s-1)\left[2^{e-1}(\ell+2)-1\right] \\ &= (s-1)\left[(m+1-\ell-2)\,2^{e-1}+1\right] \\ &\geq (m-\ell-1)2^{e-1}+1 \geq (m-\ell-1)+1 = m-\ell. \end{aligned}$$

This means that the inner sum of the equation is divisible by $2^{m-\ell}$, and since by choice, c_j is divisible by 2^ℓ, so

$$N_C(j,2^e) \equiv 0 \pmod{2^m},$$

where $k \geq \frac{2(s-1)}{s}(m+1)2^{e-2}$ which means

$$N_C(j,2^e) \equiv 0 \pmod{2^{\left\lfloor \frac{sk-2^{e-1}(s-1)}{2^{e-1}(s-1)} \right\rfloor}},$$

$j = 0,1,2,\ldots,2^e-1$. Finally, if we choose $k < \frac{2(s-1)}{s}(m+1)2^{e-2}$ then $\frac{sk-2^{e-1}(s-1)}{2^{e-1}(s-1)}$, the corresponding m value, is negative, which does not make sense in congruences. ∎

Note that everything done in this proof is still valid if a linear code C is replaced by a coset $A = \overline{a}+C$ of C. Hence the more general result follows:

Theorem 3. *Suppose C is a linear code of type $(2^s)^k$ over $\mathbb{Z}_{2^s}$ and let $A = \overline{a}+C$ be a coset of C. If we denote by $N_A(j,2^e)$ the number of codewords in A, that have Lee weights congruent to j modulo 2^e, then we have*

$$N_A(j,2^e) \equiv 0 \pmod{2^{\left\lfloor \frac{sk-2^{e-1}(s-1)}{2^{e-1}(s-1)} \right\rfloor}}, \tag{4.2}$$

$j = 0,1,2,\ldots,2^e-1$.

Also note that when $s=2$, (4.2) is transformed into (4.3) in the following theorem:

Theorem 4. [6] *Suppose C is a linear $\mathbb{Z}_4$-code of type $(4)^k$ and let $A = \overline{a}+C$ be a coset of C. If we denote by $N_A(j,2^e)$ the number of codewords in A, that have Lee weights congruent to j modulo 2^e, then we have*

$$N_A(j,2^e) \equiv 0 \pmod{2^{\left\lfloor \frac{k-2^{e-2}}{2^{e-2}} \right\rfloor}}, \tag{4.3}$$

where $j = 0,1,\ldots,2^e-1$.

This shows that the results in this paper and in [6] are consistent. The following theorem from [10] holds for any weight function:

Theorem 5. [10] *Let G be a group of order p^s, p prime, let C be a subgroup of $G^n = G \times G \times \cdots \times G$, and let A be a coset of C in G^n. Suppose $|A| = |C| = p^k$. Let μ be a mapping from G into integers and define for $\overline{a} = (a_1, \ldots, a_n) \in G^n$, $\mu(\overline{a}) = \sum_{i=1}^{n} \mu(a_i)$. If $k > s((m(p-1)+1)p^{e-1}-1)$, then for any integer t, the number N of solutions $\overline{a} \in A$ to the equation $\mu(\overline{a}) \equiv t \pmod{p^e}$ is divisible by p^m.*

Thus for a linear code over $\mathbb{Z}_{2^s}$ of type $(2^s)^k$ [10] leads to

$$N_A(j, 2^e) \equiv 0 \pmod{2^{\lfloor \frac{k-2^{e-1}}{2^{e-1}} \rfloor}}, \tag{4.4}$$

(4.2) and (4.4) can be compared by expanding (4.4) by $(s-1)$:

$$\left\lfloor \frac{sk - 2^{e-1}(s-1)}{2^{e-1}(s-1)} \right\rfloor \geq \left\lfloor \frac{(s-1)k - 2^{e-1}(s-1)}{2^{e-1}(s-1)} \right\rfloor .$$

The above inequality is strict in many cases. For example, when $s = 2$, the power obtained in our case is more than twice the power obtained in [10].

5. The extended Lee weight distribution of the trivial code over $\mathbb{Z}_{2^s}$

The trivial code was used in [11] to prove that the results obtained were best possible. Hence to get an idea about how close to the trivial code one can get, the extended Lee weight distribution of the trivial code will be found. The aim here is to get information about the divisibility of the extended Lee weight enumerators of codes of type $(2^s)^{k_1}(2^{s-1})^{k_2}\cdots(2)^{k_s}$. The weight distribution polynomial of these codes is a good point to start.

Theorem 6. *Let C be the trivial code of type $(2^s)^k$ over $\mathbb{Z}_{2^s}$ where s is any integer, i.e. $C = (\mathbb{Z}_{2^s})^k$. Then the extended Lee weight distribution of this code is given by the polynomial*

$$w_{\mathbb{Z}_{2^s}^k}(x) = (1 + 2x + \cdots + 2x^{2^{s-1}-1} + x^{2^{s-1}})^k. \tag{5.1}$$

Proof. The proof is by induction on k. Let $k = 1$. Then

$$w_{\mathbb{Z}_{2^s}}(x) = (1 + 2x + \cdots + 2x^{2^{s-1}-1} + x^{2^{s-1}}).$$

Now assume that the extended Lee weight distribution of $\mathbb{Z}_{2^s}^{k-1}$ is

$$w_{\mathbb{Z}_{2^s}^{k-1}}(x) = (1 + 2x + \cdots + 2x^{2^{s-1}-1} + x^{2^{s-1}})^{k-1}.$$

Denote the trivial code over $\mathbb{Z}_{2^s}$ of type $(2^s)^k$ as C_k. Then

$$C_k = (C_{k-1} \cup \{0\}) \cup (C_{k-1} \cup \{1\}) \cup \cdots \cup (C_{k-1} \cup \{2^s - 1\}),$$

where $C_{k-1} \cup \{i\}$'s are the set of codewords that is obtained by adding i as a coordinate to the trivial code of type $(2^s)^{k-1}$. Then the extended Lee weight distribution of C_k is

$$\begin{aligned} w_{\mathbb{Z}_{2^s}^k}(x) = \; & x^{w_L(0)}.w_{\mathbb{Z}_{2^s}^{k-1}}(x) && + \; x^{w_L(1)}.w_{\mathbb{Z}_{2^s}^{k-1}}(x) \\ & \vdots && \quad \vdots \\ & +x^{w_L(2^s-2)}.w_{\mathbb{Z}_{2^s}^{k-1}}(x) && + \; x^{w_L(2^s-1)}.w_{\mathbb{Z}_{2^s}^{k-1}}(x). \end{aligned}$$

After plugging the generalized Lee weights into the equation and adding the terms with the same weights (5.1) is accomplished. ∎

The previous result is extended in a similar way for the case of trivial codes of arbitrary types as follows:

Theorem 7. *Let C be the trivial code of type $(2^s)^{k_1}(2^{s-1})^{k_2}\cdots(2^{s-i})^{k_i}\cdots(2)^{k_s}$ over $\mathbb{Z}_{2^s}$, i.e. $C = (\mathbb{Z}_{2^s})^{k_1} \times (2\mathbb{Z}_{2^s})^{k_2} \times \cdots \times (2^{s-1}\mathbb{Z}_{2^s})^{k_s}$. Then the extended Lee weight distribution of this code is given by the polynomial*

$$\begin{aligned} w_C(x) \;=\; & (1+2x+2x^2+\cdots+2x^{2^{s-1}-1}+x^{2^{s-1}})^{k_1} \\ & \cdot(1+2x^2+\cdots+2x^{2^{s-1}-2}+x^{2^{s-1}})^{k_2}\cdots \\ & \cdot(1+2x^{2^i}+\cdots+2x^{2^{s-1}-2^i}+x^{2^{s-1}})^{k_i}\cdots \\ & \cdot(1+x^{2^{s-1}})^{k_s}. \end{aligned} \tag{5.2}$$

Before proving the main result in this section a corollary of a theorem mentioned in [11] is needed.

Theorem 8. [11] *Suppose*

$$(1+(p-1)x^{p^{(\ell-1)m}})^k \equiv A_0 + A_1x + \cdots + A_{p^e-1}x^{p^e-1} \pmod{x^{p^e}-1},$$

then

$$\min\{v_p(A_i) \mid i = 0,1,\ldots,p^e-1\} = \left\lfloor \frac{k-p^{e-(\ell-1)m-1}}{(p-1)p^{e-(\ell-1)m-1}} \right\rfloor$$

for $e \geq (\ell-1)m+1$, where $v_p(k)$ denotes the highest power of a prime p that divides a non-negative integer k.

For the case in this paper, i.e. when $p = 2$, the below corollary follows:

Corollary 1. *Suppose*

$$(1+x)^k \equiv A_0 + A_1x + \cdots + A_{2^e-1}x^{2^e-1} \pmod{x^{2^e}-1},$$

then

$$\min\{v_2(A_i) \mid i = 0, 1, \cdots, 2^e - 1\} = \left\lfloor \frac{k - 2^{e-1}}{2^{e-1}} \right\rfloor$$

for $e \geq 1$.

Using Theorem 7 we get the following theorem:

Theorem 9. *Suppose C is the trivial code of type $(2^s)^{k_1}(2^{s-1})^{k_2} \cdots (2)^{k_s}$ over $\mathbb{Z}_{2^s}$. Then*

$$N_C(j, 2^e) \equiv 0 \pmod{2^{\left\lfloor \frac{(k_1+k_2+\cdots+k_s)-2^{e-s}}{2^{e-s}} \right\rfloor}},$$

where $j = 0, 1, \ldots, 2^e - 1$.

Proof. The weight distribution polynomial of such type of a code is given by (5.2). Since all the components of this product contain $x^{2^{s-1}}$ as the leading term, we can write each of them in terms of $(1+x)^{2^{s-1}}$ as follows,

$$= \left[(1+x)^{2^{s-1}} - Q_1(x)\right]^{k_1} \cdot \left[(1+x)^{2^{s-1}} - Q_2(x)\right]^{k_2} \cdots \left[(1+x)^{2^{s-1}} - Q_s(x)\right]^{k_s}.$$

All coefficients of $(1+x)^{2^{s-1}} - x^{2^{s-1}} - 1$ are even, since

$$2 \mid \binom{2^{s-1}}{i},$$

where $i = 2, \ldots, 2^{s-1} - 1$. So coefficients of $Q_i(x)$'s are even. Hence there exists $q_i(x) \in \mathbb{Z}[X]$ for each i such that

$$Q_i(x) = 2q_i(x).$$

After replacing $Q_i(x)$'s by $2q_i(x)$'s weight distribution polynomial becomes

$$w_C(x) = \left[(1+x)^{2^{s-1}} - 2q_1(x)\right]^{k_1} \cdots \left[(1+x)^{2^{s-1}} - 2q_s(x)\right]^{k_s}.$$

Now, using Binomial Theorem to expand each component,

$$(5.3) \qquad w_C(x) = \left[\sum_{i_1=0}^{k_1} \binom{k_1}{i_1}(1+x)^{2^{s-1}(k_1-i_1)}(-2q_1(x))^{i_1}\right] \cdot$$

$$\vdots$$

$$\left[\sum_{i_s=0}^{k_s} \binom{k_s}{i_s}(1+x)^{2^{s-1}(k_s-i_s)}(-2q_s(x))^{i_s}\right].$$

After expanding (5.3), we see that a typical term in the expansionis of the form

$$(1+x)^{2^{s-1}(k_1++\cdots+k_s-i_1-\cdots-i_s)}\, 2^{i_1+\cdots+i_s} A(x),$$

where $A(x)$ is a polynomial with integer coefficients. By using Corollary 1, the coefficients of (5.3) reduced modulo $(x^{2^e}-1)$ are all divisible by

$$\begin{aligned}
&\left\lfloor \frac{[2^{s-1}(k_1-i_1)+\cdots+2^{s-1}(k_s-i_s)]-2^{e-1}}{2^{e-1}} \right\rfloor + i_1+\cdots+i_s \\
=\ &\left\lfloor \frac{2^{s-1}(k_1+\cdots+k_s)+(2^{e-1}-2^{s-1})(i_1+\cdots+i_s)-2^{e-1}}{2^{e-1}} \right\rfloor, \\
\geq\ &\left\lfloor \frac{2^{s-1}(k_1+\cdots+k_s)-2^{e-1}}{2^{e-1}} \right\rfloor = \left\lfloor \frac{(k_1+\cdots+k_s)-2^{e-1+1-s}}{2^{e-1+1-s}} \right\rfloor \\
=\ &\left\lfloor \frac{(k_1+\cdots+k_s)-2^{e-s}}{2^{e-s}} \right\rfloor .
\end{aligned}$$

Then

$$N_C(j,2^e) \equiv 0 \pmod{2^{\left\lfloor \frac{(k_1+k_2+\cdots+k_s)-2^{e-s}}{2^{e-s}} \right\rfloor}},$$

where $j=0,1,\ldots,2^e-1$. ∎

For comparison with the result in [10] given by (3) and the result given by Theorem 9, let $k_1=k, k_i=0$ for all $i=2,3,\ldots,s$. Then $N_C(j,2^e)$ is divisible by $2^{\left\lfloor \frac{k-2^{e-s}}{2^{e-s}} \right\rfloor} = 2^{\left\lfloor \frac{2^{s-1}k-2^{e-1}}{2^{e-1}} \right\rfloor}$. But $2^{s-1}>1$ for $s\geq 1$, which means the theorem improves the result in [10], which is $2^{\left\lfloor \frac{k-2^{e-1}}{2^{e-1}} \right\rfloor}$, quite considerably.

Acknowledgement : We wish to thank the anonymous referees for their helpful remarks and comments.

6. Conclusion

In this work, the extended Lee weight was considered for linear codes over $\mathbb{Z}_{2^s}$ together with its Gray map. The divisibility properties of Lee weight enumerators of linear codes over $\mathbb{Z}_{2^s}$ of type $(2^s)^k$ were established in a similar way to what was done in [10] and [6]. Later, the divisibility of the extended Lee weight enumerators of the trivial code was examined.

Comparing these results with Wilson's results in [10] and the results about homogeneous weight obtained in [11], we see the results that are introduced here, improve Wilson's results but the powers are not as high as the ones for homogeneous weight. This is natural to expect since the homogeneous weight of every coordinate in $\mathbb{Z}_{2^s}$ is already divisible by 2^{s-2}. The only non zero weights in the homogenous weight of $\mathbb{Z}_{2^s}$-codes are 2^{s-2} and 2^{s-1}. However, the extended Lee weight takes on every value from 1 to 2^{s-1}.

Possible direction for future research will be to reach the divisibility results for the generalized Lee weight enumerators of an arbitrary type of code, as done for free type of codes, and to obtain the tightest bounds possible for codes over $\mathbb{Z}_{2^s}$.

REFERENCES

[1] A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, P. Solé, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes, IEEE Trans. Inform. Theory 40 (1994) 301-319.

[2] I. Constantinescu, T. Heise, A metric for codes over residue class rings of integers, Problemy Peredachi Informatsii 33 (1997) 22-28.

[3] P.V. Kumar, T. Helleseth, A.R. Calderbank, An upperbound for Weil exponential sums over Galois rings and applications, IEEE Trans. Inform. Theory 41 (1995) 456-468.

[4] S. Ling, F. Özbudak, An improvement on the bounds of Weil exponential sums over Galois rings with some applications, IEEE Trans. Inform. Theory 50 (2004) 2529-2539.

[5] B. Yıldız, A combinatorial construction of the Gray map over Galois rings, Discrete Mathematics 309(10) (2009) 3408-3412.

[6] B. Yıldız, A lemma on binomial coefficients and applications to Lee weights modulo 2^e of codes over $\mathbb{Z}_4$, Designs, Codes and Cryptography (2011) (online). DOI: 10.1007/s10623-011-9512-2.

[7] C. Carlet, $\mathbb{Z}_{2^k}$-linear codes, IEEE Trans. Inform. Theory 44 (1998) 1543-1547.

[8] S.T. Dougherty, C. Fernández-Córdoba, Codes over $\mathbb{Z}_{2^k}$, gray map and self-dual codes, Adv. Math. Comm, Vol 5, (2011), 571–588.

[9] V. Pless, Constraints on weights in binary codes, Appl. Algebr. Eng. Comm., Vol 8, (1997), 411–414.

[10] R.M. Wilson, A lemma on polynomials modulo p^m and applications to Coding Theory, Discrete Mathematics 306 (2006) 3154-3165.

[11] B. Yıldız, Weights modulo p^e of linear codes over rings, Designs, Codes and Cryptography 43 (2007) 147-165.

[12] S. Ling, J.T. Blackford, $\mathbb{Z}_{p^{k+1}}$-linear codes, IEEE Trans. Inform. Theory 48 (2002) 2592-2605.

[13] M. Greferath, S.E. Schmidt, Gray isometries for finite chain rings and nonlinear ternary $(36, 3^{12}, 15)$ code, IEEE Trans. Inform. Theory 45 (1999) 2522-2524.

[14] W.C. Huffman, Decompositions and extremal Type II codes over $\mathbb{Z}_4$, IEEE Trans. Inform. Theory 44 (1998) 800-809.

[15] B. Yıldız, Z. Ödemiş Özger, Linear codes over $\mathbb{Z}_{2^s}$ with the extended Lee weight, AIP Conf. Proc. 1389 (2011) 621-624. DOI:10.1063/1.3636807.

[16] J.Borges, C.Fernández and J. Rifà, Propelinear structure of$\mathbb{Z}_{2^k}$-linear codes, Technical Report Arxiv:0907.5287,2009.

(B. Yıldız) DEPARTMENT OF MATHEMATICS, FATİH UNIVERSITY 34500 İSTANBUL, TURKEY

E-mail address, B. Yıldız: byildiz@fatih.edu.tr

(Z. Ödemiş Özger) DEPARTMENT OF ENGINEERING SCIENCES, İZMIR KÂTİP ÇELEBİ UNIVERSITY, 35620 İZMIR, TURKEY

E-mail address, Z. Ödemiş Özger: zeynep.odemis.ozger@ikc.edu.tr