On the Properties of Error Patterns in the Constant Lee Weight Channel

Jessica Bariffi*†, Hannes Bartz*, Gianluigi Liva*, and Joachim Rosenthal†
*Institute of Communication and Navigation, German Aerospace Center, 82234 Wessling, Germany
Email:{jessica.bariffi,hannes.bartz,gianluigi.liva}@dlr.de
†Institute of Mathematics, University of Zurich, CH-8057 Zürich, Switzerland
Email: rosenthal@math.uzh.ch

***Abstract*—The problem of scalar multiplication applied to vectors is considered in the Lee metric. Unlike in other metrics, the Lee weight of a vector may be increased or decreased by the product with a nonzero, nontrivial scalar. This problem is of particular interest for cryptographic applications, like for example Lee metric code-based cryptosystems, since an attacker may use scalar multiplication to reduce the Lee weight of the error vector and thus to reduce the complexity of the corresponding generic decoder. The scalar multiplication problem is analyzed in the asymptotic regime. Furthermore, the construction of a vector with constant Lee weight using integer partitions is analyzed and an efficient method for drawing vectors of constant Lee weight uniformly at random from the set of all such vectors is given.**

I. Introduction

In the late 1950s, relating to transmitting symbols from a finite prime field $\mathbb{F}_q$, the Lee metric was introduced in [1], [2]. Error correcting codes endowed with the Lee metric (like BCH codes, dense error-correcting codes or codes with maximum Lee distance) were constructed and applied in various different manners [3]–[9]. Recently, the Lee metric was applied to DNA storage systems [10] and considered for cryptographic applications [11]. New families of error correcting codes endowed with the Lee metric together with an iterative decoding algorithm were proposed [12] while information set decoding (ISD) in the Lee metric has been analyzed [11], [13].

ISD is one way to solve the well-known generic (syndrome) decoding problem, which aims at decoding an arbitrary linear code efficiently without knowing or using the structure of the code. This problem is fundamental for code-based cryptography and was shown to be NP-complete in both the Hamming metric [14], [15] and the Lee metric [16]. The desirable feature of generic (syndrome) decoding is to succeed in correcting an error vector $\mathbf{e}$ as long as its corresponding weight is small, where small refers to the Gilbert-Varshamov bound [17], [18]. In fact, syndrome decoding has an exponential complexity in the weight of the error for both the Hamming and the Lee weight. From an adversarial point of view, the goal is to reduce the weight of the introduced error vector in order to make the generic (syndrome) decoding problem more feasible. In fact, while the Hamming weight of a vector with entries from a finite field is invariant under multiplication with a nonzero scalar, the Lee weight of a vector can be increased or decreased by the product with a scalar. Understanding under which conditions (and with what probability) the Lee weight on the error vector $\mathbf{e}$ is reduced represents a key preliminary step in the design of Lee metric code-based cryptosystems. We will refer to this problem as *scalar multiplication problem.*

In this paper, we consider an additive channel model that adds an error vector of a fixed Lee weight to the transmitted codeword. We will refer to this channel as the *constant Lee weight channel*. We present an algorithm that draws a vector of length n and fixed Lee weight t over the ring of integers $\mathbb{Z}_m$ modulo m uniformly at random from the set of vectors with the same parameters. Introducing errors uniformly at random is important from a cryptographic point of view in order to hide the structure of the error pattern. We will then derive the marginal distribution of the constant Lee weight channel in the limit of large block lengths n. This result enables to analyze how the Lee weight of a given error vector changes when multiplied by a random nonzero scalar, in the asymptotic regime. We show that, under certain conditions, the Lee weight of such an error vector will not decrease after scalar multiplication with high probability.

The paper is organized as follows. Section II provides the notations and preliminaries needed for the course of the paper. In Section III we introduce the constant Lee weight channel and provide a uniform construction of an error vector of given Lee weight among all possible vectors of the same Lee weight. The scalar multiplication problem is introduced in Section IV. We state the problem in a finite length setting and analyze it in the asymptotic regime. Conclusions are stated in Section V.

II. Notation and Preliminaries

We denote by $\mathbb{Z}_m$ the ring of integers modulo m, where m is a positive integer. To simplify the reading, vectors will be denoted by boldface lower-case letters.

A. The Lee Metric

Definition 1. *The Lee weight of a scalar $a \in \mathbb{Z}_m$ is defined as*

$$\mathrm{wt}_{\mathsf{L}}(a) := \min(a, m-a).$$

The Lee weight of a vector $\mathbf{x} \in \mathbb{Z}_m^n$ of length n is defined as the sum of the Lee weights of its entries, i.e.

$$\mathrm{wt}_{\mathsf{L}}(\mathbf{x}) := \sum_{i=1}^{n} \mathrm{wt}_{\mathsf{L}}(x_i).$$

Note that the Lee weight of an element $a \in \mathbb{Z}_m$ is upper bounded by $\lfloor m/2 \rfloor$. Hence, the Lee weight of a length-n vector $\mathbf{x}$ over $\mathbb{Z}_m$ is at most $n \cdot \lfloor m/2 \rfloor$. To simplify the notation, we define

$$r := \lfloor m/2 \rfloor.$$

Furthermore, we observe that if $m \in \{2, 3\}$ the Lee weight is equivalent to the Hamming weight.

If we consider the elements of $\mathbb{Z}_m$ as points placed along a circle such that the circle is divided into m arcs of equal length, then the Lee distance between two distinct values a and b can be interpreted as the smallest number of arcs separating the two values. Therefore, the following property holds

$$\mathrm{wt}_{\mathsf{L}}(a) = \mathrm{wt}_{\mathsf{L}}(m-a) \quad \text{for every } a \in \{1, \dots, r\}. \tag{1}$$

The Lee distance between two vectors is defined as follows.

Definition 2. *Let $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_m^n$. The Lee distance between $\mathbf{x}$ and $\mathbf{y}$ is given by the Lee weight of their difference, i.e.*

$$\mathrm{d}_L(\mathbf{x}, \mathbf{y}) := \mathrm{wt}_{\mathsf{L}}(\mathbf{x} - \mathbf{y}).$$

It is well-known that the Lee distance indeed induces a metric.

B. Useful Results from Information Theory

Let X be a random variable over an alphabet $\mathcal{X}$ with probability distribution P, where $P(x) := \mathbb{P}(X = x)$ with $x \in \mathcal{X}$. The entropy $H(X)$ is defined as

$$H(X) := -\sum_{x \in \mathcal{X}} P(x) \log(P(x)).$$

The Kullback-Leibler divergence between two distributions Q and P is denoted as

$$D(Q \,||\, P) := \sum_{x \in \mathcal{X}} Q(x) \log\left(\frac{Q(x)}{P(x)}\right)$$

Theorem 1 (Conditional Limit Theorem [19, Theorem 11.6.2])**.** *Let E be a closed convex subset of probability distributions over a given alphabet $\mathcal{X}$ and let Q be a distribution not in E over the same alphabet $\mathcal{X}$. Consider $X_1, \dots, X_n$ to be discrete random variables drawn i.i.d. $\sim Q$ and let $P^\star = \arg\min_{P \in E} D(P \,||\, Q)$. Denote by X^n the random sequence $(X_1, \dots, X_n)$ and P_{X^n} its empirical distribution. Then for any $a \in \mathcal{X}$*

$$\mathbb{P}\left(X_1 = a \,|\, P_{X^n} \in E\right) \longrightarrow P^\star(a)$$

in probability as n grows large.

C. Combinatorics

Definition 3. *Let t and s be positive integers. An integer partition of t into s parts is an s-tuple $\lambda := (\lambda_1, \dots, \lambda_s)$ of positive integers satisfying the following two properties:*

i. $\lambda_1 + \ldots + \lambda_s = t$,

ii. $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_s$.

The elements λ_i are called parts and we say that s is the length of the partition λ.

Note that the order of the parts does not matter. This means that, for instance, the tuples $(1, 1, 2)$, $(1, 2, 1)$ and $(2, 1, 1)$ are all identical and represented only by $(2, 1, 1)$. We will denote by Π_λ the set of all permutations of an integer partition λ. Let n_i denote the number of occurrences of a positive integer i in an integer partition λ of t, where $i \in \{1, \dots, t\}$, then $|\Pi_\lambda| = \binom{t}{n_1, \dots, n_t} = \frac{t!}{n_1! \dots n_t!}$.
In the following, we use $\mathcal{P}(t)$ to denote the set of integer partitions of t. We write $\mathcal{P}_k(t)$ instead, if we restrict $\mathcal{P}(t)$ to those partitions with part sizes not exceeding some fixed nonnegative integer value k. Note that for any $\lambda \in \mathcal{P}_k(t)$ its length ℓ_λ is bounded by $\lceil \frac{t}{k} \rceil \leq \ell_\lambda \leq t$.

We will now introduce a definition describing vectors whose Lee weight decomposition is based on a given integer partition.

Definition 4. *For a positive integer n and a given partition $\lambda \in \mathcal{P}_r(t)$ of a positive integer t, we say that a length-n vector $\mathbf{x}$ has weight decomposition λ over $\mathbb{Z}_m$ if there is a one-to-one correspondence between the Lee weight of the nonzero entries of $\mathbf{x}$ and the parts of λ.*

Example 1. *Let $n = 5$ and let $\lambda = (2, 1, 1)$ be an integer partition of $t = 4$ over $\mathbb{Z}_7$. All vectors of length n over $\mathbb{Z}_7$ consisting of one element of Lee weight 2 and two elements of Lee weight 1 have weight decomposition λ.*

We will denote the set of all vectors of length n of the same weight decomposition $\lambda \in \mathcal{P}(t)$ by $\mathcal{V}_{t,\lambda}^{(n)}$.

III. The Constant Lee Weight Channel

Let us consider a channel

$$\mathbf{y} = \mathbf{x} + \mathbf{e},$$

where $\mathbf{y}, \mathbf{x}$ and $\mathbf{e}$ are length-n vectors over $\mathbb{Z}_m$ and the channel introduces the error vector $\mathbf{e}$ uniformly at random from the set $\mathcal{S}_{t,m}^{(n)}$ of all vectors in $\mathbb{Z}_m^n$ with a fixed Lee weight t, i.e.

$$\mathcal{S}_{t,m}^{(n)} := \{\mathbf{e} \in \mathbb{Z}_m^n \mid \mathrm{wt}_{\mathsf{L}}(\mathbf{e}) = t\}.$$

A. Marginal Channel Distribution

Since certain decoder types (e.g., iterative decoders employed for low-density parity-check codes defined over integer rings) require the knowledge of the channel's marginal conditional distribution, our goal is to describe the marginal distribution P_e, for a generic element E of the error.

Lemma 1. *The marginal distribution of a constant Lee weight channel over $\mathbb{Z}_m$ is given by*

$$P_e^\star = \frac{1}{\sum_{j=0}^{m-1} \exp(-\beta\, \mathrm{wt}_{\mathsf{L}}(j))} \exp\left(-\beta\, \mathrm{wt}_{\mathsf{L}}(e)\right),$$

for some constant $\beta > 0$.

Proof. Following [19, Ch. 12], we are looking for a distribution $\mathbf{P} = (P_0, \dots, P_{m-1})$ that maximizes the entropy function

$$\mathrm{H}_e(\mathbf{P}) := -\sum_{e=0, P_e \neq 0}^{m-1} P_e \log P_e$$

under the constraint that the Lee weight of the vector is t, or equivalently, that the normalized Lee weight of the error vector is $\delta := t/n$, i.e.

$$\sum_{e=0}^{m-1} \mathrm{wt}_{\mathsf{L}}(e) P_e = \delta.$$

Let us introduce a Lagrange multiplier $\beta > 0$, which is the solution to

$$\delta = \frac{(k-1)\mathrm{e}^{(k+1)\beta} - k\mathrm{e}^{k\beta} + \mathrm{e}^{\beta}}{(\mathrm{e}^{\beta k} - 1)(\mathrm{e}^{\beta} - 1)}$$

with $k = r + 1$. Then the optimization problem has the following solution

$$P_e^{\star} = \kappa \exp\left(-\beta\, \mathrm{wt}_{\mathsf{L}}(e)\right), \tag{2}$$

where κ is a normalization constant enforcing $\sum_e P_e^{\star} = 1$. □

The solution (2) is closely related to the problem in statistical mechanics of finding the distribution of the energy state of a given system [19]–[21]. Here, we may interpret the energy value of the particles as the Lee weight $\mathrm{wt}_{\mathsf{L}}(e)$ of an element $e \in \mathbb{Z}_m$. Note that for the channel law determined by Lemma 1, the optimum decoder will seek for the codeword at minimum Lee distance from the channel output $\mathbf{y}$.

B. Error Pattern Construction

In the following we will present an algorithm that draws a vector uniformly at random from $\mathcal{S}_{t,m}^{(n)}$ for given parameters n, t and m. The idea is inspired by the algorithm presented in [12]. We start from partitioning the desired Lee weight t into integer parts of size at most r, since the Lee weight of any $a \in \mathbb{Z}_m$ is at most r. The main difference to the algorithm presented in [12, Lemmas 2 and 3], and crucial to design the vector uniformly at random from $\mathcal{S}_{t,m}^{(n)}$, is that the integer partition of t is not chosen uniformly at random from the set of all integer partitions $\mathcal{P}_r(t)$ of t. In fact, picking a partition uniformly at random from $\mathcal{P}_r(t)$ yields that some of the vectors in $\mathcal{S}_{t,m}^{(n)}$ are more probable than others. Therefore, we need to understand the number of vectors with weight decomposition λ, for a fixed partition $\lambda \in \mathcal{P}_r(t)$. The following result gives an answer to this question.

Lemma 2. *Let n, m and t be positive integers with $t \leq n$ and consider the set of partitions $\mathcal{P}_r(t)$ of t with part sizes not exceeding r. For any $\lambda \in \mathcal{P}_r(t)$ the number of vectors of length n over $\mathbb{Z}_m$ with weight decomposition λ is given by*

$$\left|\mathcal{V}_{t,\lambda}^{(n)}\right| = \begin{cases} 2^{\ell_\lambda} \left|\Pi_\lambda\right| \binom{n}{\ell_\lambda} & \text{if } m \text{ is odd,} \\ 2^{\ell_\lambda - c_{r,\lambda}} \left|\Pi_\lambda\right| \binom{n}{\ell_\lambda} & \text{else} \end{cases}$$

where $c_{r,\lambda} = |\{i \in \{1, \ldots, \ell_\lambda\} \mid \lambda_i = r\}|$.

Proof. Recall from Definition 4 that $\mathcal{V}_{t,\lambda}^{(n)}$ consists of all length n vectors $\mathbf{x}$ whose nonzero entries are in one-to-one correspondence with the parts of λ. Let $x_{i_1}, \ldots, x_{i_{\ell_\lambda}}$ denote the nonzero positions of $\mathbf{x}$ and let us first consider the case where

$$\mathrm{wt}_{\mathsf{L}}(x_{i_1}) = \lambda_1, \ \ldots, \ \mathrm{wt}_{\mathsf{L}}(x_{i_{\ell_\lambda}}) = \lambda_{\ell_\lambda}. \tag{3}$$

Finding the number of such vectors relies on the "selection with repetition" problem [22, Section 1.2], which implies that this number is exactly $\binom{\text{number of zeros } + \text{ free spaces } - 1}{\text{free spaces } - 1}$, i.e.

$$\binom{(n - \ell_\lambda) \ + \ (\ell_\lambda + 1) \ - \ 1}{(\ell_\lambda + 1) \ - \ 1} = \binom{n}{\ell_\lambda},$$

where with "free spaces" we mean all the possible gaps in front, between and at the end of the parts of λ.
If m is odd, the number n_i of elements in $\mathbb{Z}_m$ having a nonzero Lee weight i is always 2 for every possible Lee weight $i \in \{1, \ldots, r\}$. Hence, there are $2^{\ell_\lambda}\binom{n}{\ell_\lambda}$ vectors satisfying (3). On the other hand, if m is even, then $n_i = 2$ for $i \in \{1, \ldots, r-1\}$ and $n_r = 1$. If we define $c_{r,\lambda} = |\{i \in \{1, \ldots, \ell_\lambda\} \mid \lambda_i = r\}|$ to be the number of parts of λ equal to r, then the number of parts of λ that can be flipped is $2^{\ell_\lambda - c_{r,\lambda}}$. Hence, the number of vectors satisfying (3) is $2^{\ell_\lambda - c_{r,\lambda}}\binom{n}{\ell_\lambda}$.
Finally, since the ordering of the nonzero elements of $\mathbf{x}$ is not necessarily the same as the order of the parts of λ, we multiply $\binom{n}{\ell_\lambda}$ by the number of permutations $|\Pi_\lambda|$ of λ and obtain the desired result. □

Finally, the actual vector construction over $\mathbb{Z}_m$, described in Algorithm 1, mainly consists of picking a partition $\lambda \in \mathcal{P}_r(t)$ of the Lee weight t with part sizes not exceeding r. The probability of $\mathbf{x} \in \mathcal{S}_{t,m}^{(n)}$ with weight decomposition $\lambda \in \mathcal{P}_r(t)$ is given by

$$p_\lambda := \frac{\left|\mathcal{V}_{t,\lambda}^{(n)}\right|}{\sum_{\tilde{\lambda} \in \mathcal{P}_r(t)} \left|\mathcal{V}_{t,\tilde{\lambda}}^{(n)}\right|}.$$

The idea is to choose the integer partition according to the probability mass function $\mathcal{X}_{t,m}^{(n)}$ defined by the probabilities p_λ, for $\lambda \in \mathcal{P}_r(t)$. We will denote this procedure by

$$\lambda \xleftarrow{\mathcal{X}_{t,m}^{(n)}} \mathcal{P}_r(t).$$

We then randomly flip the elements of the partition modulo m and assign these values to randomly chosen positions of the error vector. Choosing an element a uniformly at random from a given set $\mathcal{A}$ will be denoted by $a \xleftarrow{\$} \mathcal{A}$. We want to emphasize at this point that for fixed parameters n, t and m the computation of $\mathcal{X}_{t,m}^{(n)}$ needs to be done only once at the beginning, since the distribution is only dependent on these parameters and does not change anymore.

Theorem 2. *Let n, m and t be positive integers. Algorithm 1 draws a vector uniformly at random among $\mathcal{S}_{t,m}^{(n)}$.*

Proof. First note that $\mathcal{S}_{t,m}^{(n)} = \bigsqcup_{\lambda \in \mathcal{P}_r(t)} \mathcal{V}_{t,\lambda}^{(n)}$, where $\bigsqcup$ denotes the disjoint union of sets. Hence, we want to pick $\lambda \in \mathcal{P}_r(t)$ such that all the vectors in $\mathcal{S}_{t,m}^{(n)}$ are equally probable to be drawn. The choice of λ is decisive for the set $\mathcal{V}_{t,\lambda}^{(n)}$. Since

Algorithm 1 Drawing a vector uniformly at random from $\mathcal{S}_{t,m}^{(n)}$

```
Require: $n, m, t \in \mathbb{N}_{>0}$, distribution $\mathcal{X}_{t,m}^{(n)}$
Ensure: $\mathbf{e} \overset{\$}{\leftarrow} \mathcal{S}_{t,m}^{(n)}$
$\lambda \xleftarrow{\mathcal{X}_{t,m}^{(n)}} \mathcal{P}_r(t)$
$F = \{f_1, \dots, f_{\ell_\lambda}\} \overset{\$}{\leftarrow} \{\pm 1\}^{\ell_\lambda}$
$\operatorname{supp}(\mathbf{e}) \overset{\$}{\leftarrow} \{S \subset \{1, \dots, n\} \,:\, |S| = \ell_\lambda\}$
for $i = 1, \dots, n$ do
    if $i \in \operatorname{supp}(\mathbf{e})$ then
        $e_i \leftarrow f_i \cdot \lambda_i$
    else
        $e_i = 0$
    end if
end for
return random_permutation($\mathbf{e}$)
```

$\left|\mathcal{V}_{t,\lambda}^{(n)}\right|$ changes with λ, we pick λ according to distribution p_λ from $\mathcal{X}_{t,m}^{(n)}$ using Lemma 2 and the result follows. □

IV. Scalar Multiplication Problem

While we know that the Hamming weight of a vector over a finite field is invariant under multiplication with a nonzero scalar, the Lee weight can possibly change. In this section, we analyze the behavior of the Lee weight of a vector when multiplied by a scalar. Recalling that the Lee metric coincides with the Hamming metric over $\mathbb{Z}_2$ and $\mathbb{Z}_3$, in the following we will focus only on the case where the Lee weight is different from the Hamming weight, i.e. we focus on $\mathbb{Z}_m$ with $m > 3$.

Remark 1. *Even though we will not discuss the following, we want to emphasize at this point that the Hamming weight is* not *invariant under multiplication with a nonzero scalar when working over a finite integer ring that is not a field.*

A. Problem Statement

We now establish bounds on the probability of reducing the Lee weight of a random vector by multiplying it with a random nonzero scalar.

Problem 1. *Consider the ring of integers $\mathbb{Z}_m$, with $m > 3$. Given a random vector $\mathbf{x} \in \mathbb{Z}_m^n$ with Lee weight $\operatorname{wt_L}(\mathbf{x}) = t$ uniformly distributed in $\mathcal{S}_{t,m}^{(n)}$. Let a be chosen uniformly at random from $\mathbb{Z}_m \backslash \{0\}$. Find the probability that the Lee weight of $a \cdot x$ is less than the Lee weight t of x, i.e.*

$$\mathbb{P}\left(\operatorname{wt_L}(a \cdot x) < t\right).$$

For simplicity, let us define the following event

$$F := \{\operatorname{wt_L}(a \cdot \mathbf{x}) < t\}.$$

We denote by $Q_{\mathbf{x}}$ the empirical distribution of the entries of $\mathbf{x}$. Recall the distribution $P^\star$ defined in (2). We will rewrite $\mathbb{P}(F)$ by distinguishing between vectors $\mathbf{x}$ with $Q_{\mathbf{x}}$ close to $P^\star$ and all others, where by "close" we mean with respect to the Kullback-Leibler divergence, i.e. $Q_{\mathbf{x}}$ satisfies $D(Q_{\mathbf{x}} \,||\, P^\star) < \varepsilon$ for some $\varepsilon > 0$ small. We have that

$$\begin{aligned} \mathbb{P}(F) \leq\, & \mathbb{P}\left(\operatorname{wt_L}(a \cdot \mathbf{x}) < t \,|\, D(Q_{\mathbf{x}} \,||\, P^\star) < \varepsilon\right) \\ & + \mathbb{P}\left(D(Q_{\mathbf{x}} \,||\, P^\star) \geq \varepsilon\right). \end{aligned} \tag{4}$$

Note that the probability $\mathbb{P}(F)$ is dependent on three parameters: the length n of the constructed vector $\mathbf{x}$, the size m of the integer ring and the given Lee weight t of $\mathbf{x}$. The evaluation of the bound (4) is challenging for $m > 3$, finite n and generic t. In the following subsection we will describe how to attack the problem for n large.

B. Asymptotic Analysis

Let us focus now on the asymptotic regime, i.e. where the block length n tends to infinity. Note here that we let $\operatorname{wt_L}(\mathbf{x}) = t$ grow linearly with n. Let us denote by $U(\mathbb{Z}_m)$ the uniform distribution over $\mathbb{Z}_m$ and let E be the set of probability distributions over $\mathbb{Z}_m$ with an average Lee weight $\delta := t/n$, i.e.

$$E := \left\{ p = (p_0, \dots, p_{m-1}) \,\middle|\, \sum_{i=0}^{m-1} p_i = 1 \text{ and } \sum_{i=0}^{m-1} p_i \operatorname{wt_L}(i) = \delta \right\}$$

Hence, a straightforward application of Theorem 1 yields the following corollary.

Corollary 1. *Let $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{Z}_m^n$ a random vector drawn uniformly from $\mathcal{S}_{\delta n,m}^{(n)}$. Then, for every $\varepsilon > 0$ it holds*

$$\mathbb{P}\left(D(Q_{\mathbf{x}} \,||\, P^\star) \geq \varepsilon\right) \longrightarrow 0 \textit{ as } n \longrightarrow \infty.$$

Proof. Let $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{Z}_m^n$ be a random vector whose entries are independent and uniformly distributed in $\mathbb{Z}_m$. The distribution of $\mathbf{x}$ is uniform on $\mathbb{Z}_m^n$, and hence on $\mathcal{S}_{\delta n,m}^{(n)}$. We have that

$$P^\star = \arg\min_{P \in E} D(P \,||\, U(\mathbb{Z}_m)).$$

Then, by Theorem 1, we obtain the desired result. □

In fact, Theorem 1 allows to assume that the entries of a sequence $\mathbf{x}$ drawn uniformly in $\mathcal{S}_{\delta n,m}^{(n)}$ are distributed according to $P^\star$ as n grows large. Hence, in the asymptotic regime, Problem 1 reduces to estimating the probability $\mathbb{P}\left(\operatorname{wt_L}(a \cdot \mathbf{x}) \leq \operatorname{wt_L}(\mathbf{x}) \,|\, D(Q_{\mathbf{x}} \,||\, P^\star) < \varepsilon\right)$. In that case, we apply Definition 1 for the Lee weight of a vector $\mathbf{x}$. Then the assumption that the entries of $\mathbf{x}$ are distributed as in (2) yields, in the limit of n large, the following equivalent description of the desired probability

$$\begin{aligned} \lim_{n \longrightarrow \infty} \mathbb{P}(F) = \mathbb{P}\Big(& \sum_{i=1}^{m-1} \mathrm{e}^{-\beta \operatorname{wt_L}(i)} \operatorname{wt_L}([a \cdot i]_m) \\ & < \sum_{i=1}^{m-1} \mathrm{e}^{-\beta \operatorname{wt_L}(i)} \operatorname{wt_L}(i) \Big) \end{aligned} \tag{5}$$

By Property (1), we can run the sum only up to r. Nevertheless we need to distinguish between even or odd ring order m. In particular, for m odd we rewrite (5) as

$$\lim_{n \longrightarrow \infty} \mathbb{P}(F) = \mathbb{P}\Big(0 < \sum_{i=1}^{r} \mathrm{e}^{-\beta i} (i - \operatorname{wt_L}([a \cdot i]_m)) \Big) \tag{6}$$

whereas for m even (5) is equivalent to

$$\lim_{n\longrightarrow\infty}\mathbb{P}(F)=\mathbb{P}\Big(0<\sum_{i=1}^{r-1}2\mathrm{e}^{-\beta i}(i-\mathrm{wt}_{\mathsf{L}}([a\cdot i]_m)) + \mathrm{e}^{-\beta r}(r-\mathrm{wt}_{\mathsf{L}}([a\cdot r]_m))\Big) \quad (7)$$

where $[a\cdot i]_m$ denotes the reduction of $a\cdot i \mod m$.

Since we want $\mathbb{P}(F)$ to be small (or equal to zero), we need to understand under which circumstances the sums in (6) and (7) are non-positive. Note that both $\sum_{i=1}^{r}\mathrm{e}^{-\beta i}(i-\mathrm{wt}_{\mathsf{L}}([a\cdot i]_m))$ and $\sum_{i=1}^{r-1}2\mathrm{e}^{-\beta i}(i-\mathrm{wt}_{\mathsf{L}}([a\cdot i]_m))+\mathrm{e}^{-\beta r}(r-\mathrm{wt}_{\mathsf{L}}([a\cdot r]_m)$ are dependent on m and β, where β depends on δ. If we fix these parameters, we are able to compute the sum and hence (5). We therefore fix m and evaluate the two expressions for different values of δ. Let $\delta^\star$ denote the largest normalized Lee weight such that (6) or rather (7) are equal to zero for every $\delta<\delta^\star$. Table I shows the values of the threshold $\delta^\star$ for different ring orders m.

TABLE I
MAXIMAL NORMALIZED LEE WEIGHT $\delta^\star$ OVER $\mathbb{Z}_m$ SUCH THAT $\mathbb{P}(F)=0$ AS $n\longrightarrow\infty$, FOR SOME VALUES OF m COMPARED TO THE MAXIMAL POSSIBLE NORMALIZED LEE WEIGHT r.

m	5	7	8	9	11	15	16	31	32	53
r	2	3	4	4	5	7	8	15	16	26
$\delta^\star$	1.2	1.714	2	1.962	2.727	3.310	4	7.741	8	13.245

Observe from Table I that for m an odd prime power and for $\delta^\star=(m^2-1)/4m$ (i.e. the average Lee weight when choosing an element uniformly from $\mathbb{Z}_m$ [23]) the Lee weight of a vector $\mathbf{x}\in\mathbb{Z}_m^n$ can never be reduced when multiplied by a nonzero scalar. This fact can be established by observing that the multiplication of a random variable X in $\mathbb{Z}_m$ by $a\in\mathbb{Z}_m\setminus\{0\}$ induces a permutation of the distribution. Moreover, if X is distributed according to $P^\star$ with $\beta>0$, the permutation that maximizes $\mathbb{E}(\mathrm{wt}_{\mathsf{L}}(aX))$ is the identity, i.e., $a=1$. On the contrary, if $\beta<0$, the identity permutation ($a=1$) minimizes $\mathbb{E}(\mathrm{wt}_{\mathsf{L}}(aX))$. The result follows by observing that $\beta>0$ implies that the average Lee weight is $\delta<(m^2-1)/4m$.

Note that the same result follows for any m if $a\in\mathbb{Z}_m^\times$ is a unit modulo m. Moreover, if m is a power of 2, the threshold is

$$\delta^\star=m/4.$$

V. Conclusions

In this work we have introduced an algorithm for the construction of error patterns over $\mathbb{Z}_m^n$ of a fixed Lee weight. The algorithm is efficient compared to straightforward approaches, which are more involved in terms of computation and memory. The proposed algorithm is based on the idea of subdividing the tasks into subtasks, which are more or less easy to solve. The procedure is dominated by the computation of the distribution used to choose the underlying integer partition of a vector's Lee weight decomposition. For a fixed Lee weight t, this distribution can be pre-computed. We have shown that the presented algorithm draws a vector uniformly at random among all vectors of the same length and Lee weight. This property is important for cryptographic applications in the context of Lee metric code-based cryptography in order to avoid information leakage on the structure of the error pattern. Additionally, the results on the constant-weight Lee channel together with the random construction of sequences of fixed Lee weight were used to derive the probability of reducing the Lee weight of a vector over $\mathbb{Z}_m^n$ when multiplying it by a random nonzero element of $\mathbb{Z}_m$, for the limit case where the sequence length grows large. An open problem is to characterize this probability in the finite sequence length regime.

References

[1] W. Ulrich, "Non-binary error correction codes," *The Bell System Technical Journal*, vol. 36, no. 6, pp. 1341–1388, 1957.

[2] C. Lee, "Some properties of nonbinary error-correcting codes," *IRE Trans. Inf. Theory*, vol. 4, no. 2, pp. 77–82, 1958.

[3] E. Prange, "The use of coset equivalene in the analysis and decoding of group codes," Air Force Cambridge Research Labs, Tech. Rep., 1959.

[4] E. R. Berlekamp, "Negacyclic codes for the Lee metric," North Carolina State University. Dept. of Statistics, Tech. Rep., 1966.

[5] S. W. Golomb and L. R. Welch, "Algebraic coding and the Lee metric," *Error Correcting Codes*, pp. 175–194, 1968.

[6] J. C.-Y. Chiang and J. K. Wolf, "On channels and codes for the Lee metric," *Information and Control*, vol. 19, no. 2, pp. 159–173, 1971.

[7] R. M. Roth and P. H. Siegel, "Lee-metric BCH codes and their application to constrained and partial-response channels," *IEEE Trans. Inf. Theory*, vol. 40, no. 4, pp. 1083–1096, Apr. 1994.

[8] T. Etzion, A. Vardy, and E. Yaakobi, "Dense error-correcting codes in the Lee metric," in *Proc. IEEE Information Theory Workshop*, Sep. 2010.

[9] T. L. Alderson and S. Huntemann, "On maximum Lee distance codes," *Journal of Discrete Mathematics*, 2013.

[10] R. Gabrys, H. M. Kiah, and O. Milenkovic, "Asymmetric Lee distance codes for DNA-based storage," *IEEE Trans. Inf. Theory*, vol. 63, no. 8, pp. 4982–4995, Aug. 2017.

[11] A.-L. Horlemann-Trautmann and V. Weger, "Information set decoding in the Lee metric with applications to cryptography," *arXiv preprint arXiv:1903.07692*, 2019.

[12] P. Santini, M. Battaglioni, F. Chiaraluce, M. Baldi, and E. Persichetti, "Low-Lee-Density Parity-Check Codes," in *Proc. 2020 IEEE International Conference on Communications (ICC)*, June 2020.

[13] V. Weger, M. Battaglioni, P. Santini, F. Chiaraluce, M. Baldi, and E. Persichetti, "Information set decoding of Lee-metric codes over finite rings," *arXiv preprint arXiv:2001.08425*, 2020.

[14] S. Barg, "Some new NP-complete coding problems," *Problemy Peredachi Informatsii*, vol. 30, no. 3, pp. 23–28, 1994.

[15] E. Berlekamp, R. McEliece, and H. Van Tilborg, "On the inherent intractability of certain coding problems (corresp.)," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 384–386, 1978.

[16] V. Weger, M. Battaglioni, P. Santini, A.-L. Horlemann-Trautmann, and E. Persichetti, "On the hardness of the Lee syndrome decoding problem," *arXiv e-prints*, 2020.

[17] E. N. Gilbert, "A comparison of signalling alphabets," *The Bell System Technical Journal*, vol. 31, no. 3, pp. 504–522, 1952.

[18] R. R. Varshamov, "Estimate of the number of signals in error correcting codes," *Docklady Akad. Nauk, SSSR*, vol. 117, pp. 739–741, 1957.

[19] T. M. Cover and J. A. Thomas, *Elements of information theory*, 2nd ed. New York: Wiley, 2006.

[20] L. Boltzmann, "Studien über das Gleichgewicht der lebendigen Kraft zwischen bewegten materiellen Punkten (studies of the equilibrium and the life force between material points)," *Wien. Ber*, vol. 58, p. 517, 1868.

[21] J. W. Gibbs, *Elementary principles in statistical mechanics: developed with special reference to the rational foundation of thermodynamics*. Dover Publications, 1902.

[22] S. Jukna, *Extremal combinatorics: with applications in computer science*. Springer Science & Business Media, 2011.

[23] A. D. Wyner and R. L. Graham, "An upper bound on minimum distance for a k-ary code," *Inf. Control.*, vol. 13, no. 1, pp. 46–52, 1968.