On Some $\mathbb{Z}_m$ Linear Goppa/BCH like Error Control Codes and Elementary Symmetric Functions*

Luca G. Tallini† and Bella Bose‡
†Dipartimento di Scienze della Comunicazione, Università degli Studi di Teramo, Teramo, Italy. E-mail: ltallini@unite.it
‡School of EECS, Oregon State University, Corvallis, OR, USA. E-mail: bose@eecs.orst.edu

2023 IEEE International Symposium on Information Theory (ISIT) | 978-1-6654-7554-9/23/$31.00 ©2023 IEEE | DOI: 10.1109/ISIT54713.2023.10206630

***Abstract*—Let $\mathbb{Z}_m \stackrel{\text{def}}{=} \{0,1,\ldots,(m-1)\}$ be the m-ary alphabet, $m \in \mathbb{N}$. This paper gives some new theory and designs of $\mathbb{Z}_m$ linear error control codes based on the elementary symmetric functions of m-ary words. Here, a $\mathbb{Z}_m$ linear code is a submodule of the module $(\mathbb{Z}_m^n, +\bmod m, \mathbb{Z}_m, \cdot \bmod m)$, $n \in \mathbb{N}$, and the errors are measured in the L_1 or Lee metric. Potentially, the alphabet size, m, can be any natural, however, the described code designs and decoding methods are solely based on fields and field operations. In particular, starting from a very general class of Goppa-like $\mathbb{Z}_m$ linear codes, given a field, K, of characteristic $p = char(K) \in \mathbb{N}$, we consider a generalization of the BCH codes to the m-ary alphabet for $m = p^l$, $l \in \mathbb{N}$. For these BCH-like codes we are able to prove a BCH-like bound with respect to both the L_1 and Lee distances. This enabled us to design a wide family of remarkable efficient codes. For example, an efficient design is given for $\mathbb{Z}_m$ linear codes with $m = 2^l, l \in \mathbb{N}$, length $n = m$, minimum Lee distance $d_{Lee} = m = n$ and the number of information m-ary digits $k = m/2 = n/2$.**

***Index Terms*—m-ary error control codes, elementary symmetric functions, σ-codes, asymmetric distance, L_1 and Lee distances, limited magnitude error channels, multi-level flash memories, m-PSK communication systems, sticky channels.**

I. Introduction

Error control codes for L_1 or Lee metrics are fundamental when the transmission channel follows the Varshamov error model where the error probability grows exponentially with the real distance between the sent and received erroneous symbol [16], [10]. Examples of Varshamov's channels are sticky channels (where $\mathbb{Z}_m = \mathbb{N}$) [15], [23], multi-level flash memories and/or limited magnitude error channels [7], [20], [5], m-PSK communication systems [14], [5], and so on.

The theories given in [8], [3], [4], [24], [22], [20], [21], [18], [17], [16], [15], show that some more information on the combinatorial properties of algebraic based codes may be obtained if one considers, as spectrum polynomial [2, p. 61] of a word, the sigma polynomial (defined below) whose coefficients are the elementary symmetric functions (instead of the power sums) of the elements in the word regarded as the multiset over an index set contained in a field. Here also, we base our investigation using this perspective. In particular, following the authors in [16], for $m = 2, 3\ldots$, let $\mathbb{Z}_m \stackrel{\text{def}}{=} \{0,1,\ldots,(m-1)\} \subseteq \mathbb{N} = \{0,1,2,\ldots\} \stackrel{\text{def}}{=} \mathbb{Z}_0$ be the m-ary alphabet order as $0 \leq 1 \leq 2 \leq \ldots$. For $m, n \in \mathbb{N}$, $X = x_0 x_1 \ldots x_{n-1} \in \mathbb{Z}_m^n$ and an index set $\partial S \stackrel{\text{def}}{=} \{a_0, a_1, \ldots, a_{n-1}\}$, let $x_{a_i} \stackrel{\text{def}}{=} x_i \in \mathbb{Z}_m$ indicate the i-th component of X or, equivalently, the multiplicity of $a_i \in X$, where X is also regarded as a multiset on the index set ∂S [16]. We identify words $X \in \mathbb{Z}_m^n$ with multisets on the index set ∂S which usually is a subset of a field. For example, if $m = 8$, $n = 4$ and $\partial S \stackrel{\text{def}}{=} \{a_0, a_1, a_2, a_3\}$ then $X = 3102 \equiv \{a_0, a_0, a_0, a_1, a_3, a_3\}$. Let the set

$$\partial X \stackrel{\text{def}}{=} \{i \in \partial S : x_{a_i} \neq 0\} \subseteq \partial S$$

be the set of indices where the word/multiset X is non-zero. Identifying the proper set ∂X with its incidence vector, we can regard ∂X as a binary vector in $\mathbb{Z}_2^n$. For example, if $X = 0401$ then $\partial X = 0101 = \{a_1, a_3\}$. So, the L_1 weight of X is its cardinality, $w_{L_1}(X) \stackrel{\text{def}}{=} |X| = \sum_{i \in \partial S} x_i$ (real sum), and the Hamming weight of X is $w_H(X) \stackrel{\text{def}}{=} |\partial X|$. Also, for all $x \in \mathbb{Z}_m$, let the Lee absolute value of x be $\lambda(x) \stackrel{\text{def}}{=} \lambda^{[m]}(x) \stackrel{\text{def}}{=} \min\{x, m-x\} \in \mathbb{Z}_{\lfloor m/2 \rfloor + 1}$, and note that it is a non decreasing function of m, for all $x \in \mathbb{Z}_{m+1}$. Let, $\lambda(X) \stackrel{\text{def}}{=} \lambda^{[m]}(X) \in \mathbb{Z}^n_{\lfloor m/2 \rfloor + 1}$, be the word obtained from $X \in \mathbb{Z}_m^n$ by applying λ to each x_i and the (m-ary) Lee weight of X is the cardinality of the multiset $\lambda(X)$, $w_{Lee}^{[m]}(X) \stackrel{\text{def}}{=} |\lambda^{[m]}(X)| = \sum_{i \in \partial S} \min\{x_i, m - x_i\}$. For example, $\lambda^{[5]}(10234) = 10221$ and so $w_{Lee}^{[5]}(10234) = |10221| = 6$. Let the natural subtraction be $x \dot{-} y = \max\{x - y, 0\}$, for all $x, y \in \mathbb{Z}_m$, and the word $X \dot{-} Y \in \mathbb{Z}_m^n$ be the componentwise natural subtraction of $X, Y \in \mathbb{Z}_m^n$. As in [20], [16], the following distances between m-ary words $X, Y \in \mathbb{Z}_m^n$ are considered to describe the combinatorial properties of the codes.

$$\begin{aligned}
&\text{asymmetric } L_1: && d_{L_1}^{as}(X,Y) \stackrel{\text{def}}{=} \max\{|Y \dot{-} X|, |X \dot{-} Y|\},\\
&\text{symmetric } L_1: && d_{L_1}^{sy}(X,Y) \stackrel{\text{def}}{=} |Y \dot{-} X| + |X \dot{-} Y|,\\
&\text{Lee:} && d_{Lee}(X,Y) \stackrel{\text{def}}{=} |\lambda(X \dot{-} Y)| + |\lambda(Y \dot{-} X)|,\\
&\text{Hamming:} && d_H(X,Y) \stackrel{\text{def}}{=} |\partial(X \dot{-} Y)| + |\partial(Y \dot{-} X)|.
\end{aligned}$$

For example, if $m = 5$, $n = 5$, $X = 10234$, $Y = 24212$ then $|X \dot{-} Y| = 4$, $|Y \dot{-} X| = 5$, $|\lambda(X \dot{-} Y)| = 4$, $|\lambda(Y \dot{-} X)| = 2$, $|\partial(X \dot{-} Y)| = 2$, $|\partial(Y \dot{-} X)| = 2$ and $d_{L_1}^{as}(X,Y) = \max\{4,5\} = 5$, $d_{L_1}^{sy}(X,Y) = 4 + 5 = 9$, $d_{Lee}(X,Y) = 4 + 2 = 6$ and $d_H(X,Y) = 2 + 2 = 4$.

If X is a sent word and Y is received then $Y \dot{-} X$ is the positive error vector, $X \dot{-} Y$ is the negative error vector so that, $X = Y - (Y \dot{-} X) + (X \dot{-} Y)$. The following combinatorial characterizations are well known [1], [25], [16].

***Theorem** 1:* A code $\mathcal{C} \subseteq \mathbb{Z}_m^n$ can correct $t_+ \in \mathbb{N}$ or less positive errors and simultaneously $t_- \in \mathbb{N}$ or less negative errors (i. e., $\mathcal{C}$ is a (t_+, t_-)-EC code) measured in the L_1 metric if, and only if, the minimum asymmetric L_1 distance of $\mathcal{C}$ is $d_{L_1}^{as}(\mathcal{C}) > t_+ + t_-$. In addition (similar to the Lee and Hamming distances codes), $\mathcal{C}$ can correct $t \in \mathbb{N}$ or less symmetric errors (i. e., $\mathcal{C}$ is a t-SyEC code) in the L_1 metric if, and only if, $d_{L_1}^{sy}(\mathcal{C}) > 2t$.

*This work is supported by the NSF grants CCF-2006571.

Now, the sigma polynomial of a word is defined as follows. Given $m, n \in \mathbb{N}$, a field K and $\partial S \subseteq K$, with $|\partial S| = n$, the σ-polynomial associated with $X = x_0 x_1, \ldots, x_{n-1} \in \mathbb{Z}_m^n$ is defined as [20],

$$\sigma_X(z) \stackrel{\text{def}}{=} z^{x_0} \prod_{a \in \partial S \dot{-} \{0\}} (1 - az)^{x_a} = \sigma_0(X) + \sigma_1(X) z + \sigma_2(X) z^2 + \ldots \in K[z]. \quad (1)$$

For example, if $n = 4$, $a_0 \stackrel{\text{def}}{=} 0 \in \partial S$ and $X = 2102 = \{a_0, a_0, a_1, a_3, a_3\}$ then

$$\sigma_X(z) = z^2(1 - a_1 z)^1 (1 - a_3 z)^2 = z^2 - (a_1 + 2a_3) z^3 + (2a_1 a_3 + a_3^2) z^4 - (a_1 a_3^2) z^5.$$

Note that $\sigma_X(z)$ is a polynomial of degree $\deg(\sigma_X) = w_{L_1}(X) = |X|$ having $w_H(X) = |\partial X|$ distinct roots in K, each with multiplicity x_a, for $a \in \partial S$. In particular, X coincides with the multiset of all the roots of the "equivalent" σ-polynomial

$$\varrho_X(z) \stackrel{\text{def}}{=} z^{|X| - x_0} \sigma_X(1/z) = \prod_{a \in \partial S} (z - a)^{x_a},$$

and so the coefficients $\sigma_0(X)$, $\sigma_1(X)$, $\sigma_2(X)$, $\ldots \in K$ of $\sigma_X(z)$ are the elementary symmetric functions of the elements in the multiset X, ordered in increasing order of their degree.

Given Theorem 1, (t_+, t_-)-EC can be designed based on the following general key equation [16].

$$\sigma_X(z) \sigma_{Y \dot{-} X}(z) = \sigma_Y(z) \sigma_{X \dot{-} Y}(z), \text{ for all } X, Y \in \mathbb{Z}_m^n. \quad (2)$$

For any fixed $g(z) \in K[z]$ such that the $\gcd(\sigma_{\partial S}, g) = 1$, the following σ-codes were considered in [16] and these codes have the minimum asymmetric L_1 distance $d = \deg(g)$ capable of controlling $t = d - 1$ asymmetric L_1 errors (see Theorem 1).

$$\mathcal{C}_{g,\sigma} \stackrel{\text{def}}{=} \left\{ X \in \mathbb{Z}_m^n \;\middle|\; \begin{array}{l} \sigma_X(z) = c_X \cdot \sigma(z) \bmod g(z), \\ \text{for some } c_X \in K - \{0\} \end{array} \right\}, \quad (3)$$

where $\sigma(z) \in K[z]$. When $d \leq m = char(K) = p \in \mathbb{N}$ and $g(z) = z^d$, the codes $\mathcal{C}_{z^d,1}$ are linear m-ary BCH codes (eventually shortened); hence, easy to encode and decode. The authors in [16] extended these linear m-ary BCH σ-codes to efficient $\mathbb{Z}_m$ linear BCH σ-codes with minimum **asymmetric** (designated) L_1 distance $d \leq m/v = p^l$, $l, v \in \mathbb{N}$. In particular, they get a new class of $t = (d-1)$ asymmetric error correcting $\mathbb{Z}_m$ linear codes of length $n \leq |K| - 1$ whose redundancy is only $t \log_m |K|$. These codes have very efficient field based algebraic decoding algorithms to control t errors actually in the Lee distance. Here, we extend their results and get other remarkable families of efficient $\mathbb{Z}_m$ linear codes with good minimum **symmetric** Lee distance. In particular, in Section II, starting from a formal generalization of the codes in (3) (we let $c_X = [\tau_X(z)]^m \in K[z] - \{0\}$) we are able to define a very general class of Goppa-like $\mathbb{Z}_m$, $m \in \mathbb{N}$, linear codes. Then, given a field, K, of characteristic $p = char(K) \in \mathbb{N}$, in Section III we consider a natural generalization of the (eventually shortened) BCH codes to the m-ary alphabet for $m = p^l$, $l \in \mathbb{N}$. For these BCH-like codes we are able to prove a BCH-like bound with respect to both the L_1 and Lee distances. We note that no BCH bound for Lee-distance codes over $\mathbb{Z}_m$ seems to be known [2, p. 120]. In Section IV, we focus on the cyclic version of the BCH-like codes and relate these to the Galois ring based coding theory given in [2], [6], [11] and analyze some remarkable examples of a $\mathbb{Z}_m$ linear codes with simple field based decoding algorithm.

II. The $\mathbb{Z}_m$ linear Goppa-like codes

Let us recall the following as done in [16]. Let $m, n, k, h \in \mathbb{N}$ and $X, Y \in \mathbb{N}^n$. If $C = C(X, Y) = \lfloor (k \cdot X + h \cdot Y)/m \rfloor$ then

$$k \cdot X + h \cdot Y = m \cdot C + (k \cdot X + h \cdot Y) \bmod m; \quad (4)$$

where "$\cdot$", "/", "$\bmod m$", $\ldots$ operations are applied componentwise. For example, if $m = 4$, $n = 4$, $k = 2$, $h = 3$, $X = 0123$ and $Y = 1201$ then $k \cdot X + h \cdot Y = 3849$, $C = \lfloor (k \cdot X + h \cdot Y)/4 \rfloor = 0212$, $(k \cdot X + h \cdot Y) \bmod 4 = 3001$ and $3849 = 4(0212) + 3001$. Hence, for any $m \in \mathbb{N}$, field K and index set $\partial S \subseteq K$,

for all $k, h \in \mathbb{Z}_m$ and $X, Y \in \mathbb{Z}_m^n$,

$$[\sigma_X(z)]^k [\sigma_Y(z)]^h = \sigma_{k \cdot X + h \cdot Y}(z) = [\sigma_C(z)]^m \sigma_{(k \cdot X + h \cdot Y) \bmod m}(z), \quad (5)$$

where $C = C(X, Y) = \lfloor (k \cdot X + h \cdot Y)/m \rfloor \in \mathbb{N}^n$.

The relations in (5) follow from (4) and the σ-polynomial definition (1). At this point, the $\mathbb{Z}_m$ linear Goppa-like codes are given in (6) below.

***Theorem** 2:* Let $u, v, m \stackrel{\text{def}}{=} uv, n \in \mathbb{N}$. Let K be any field, $\partial S = \{a_0, a_1, \ldots, a_{n-1}\} \subseteq K$, with $n \leq |K|$, and $g(z) \in K[z]$ be a polynomial such that $\gcd(\sigma_{\partial S}, g) = 1$. The code

$$\mathcal{C}_g \stackrel{\text{def}}{=} \left\{ X \in \mathbb{Z}_m^n \;\middle|\; \begin{array}{l} \sigma_X(z) = [\tau_X(z)]^v \bmod g(z), \\ \text{for some } \tau_X(z) \in K[z] - \{0\} \end{array} \right\} \quad (6)$$

is $\mathbb{Z}_m$ linear. In particular, if $\mathcal{G} \stackrel{\text{def}}{=} \{G_0, G_1, \ldots, G_b\} \subseteq \mathcal{C}_g \subseteq \mathbb{Z}_m^n$ then $(\mathcal{G}) \subseteq \mathcal{C}_g$, where

$$(\mathcal{G}) \stackrel{\text{def}}{=} \left\{ X \in \mathbb{Z}_m^n \;\middle|\; \begin{array}{l} X = \sum_{i=0}^b k_i \cdot G_i \bmod m, \text{ for} \\ \text{some } k_0, k_1, \ldots, k_b \in \mathbb{Z}_m \end{array} \right\}$$

indicates the $\mathbb{Z}_m$ linear code generated by $G_0, G_1, \ldots, G_b$.

Proof: Let $X, Y \in \mathcal{C}_g \subseteq \mathbb{Z}_m^n$ so that $\sigma_X(z) = [\tau_X(z)]^v \bmod g(z)$ and $\sigma_Y(z) = [\tau_Y(z)]^v \bmod g(z)$, for some $\tau_X(z), \tau_Y(z) \in K[z] - \{0\}$. Hence, from (5), there exists $C \in \mathbb{N}^n$ such that $\partial C \subseteq \partial S$ and

$$[\sigma_C(z)]^m \sigma_{(X+Y) \bmod m}(z) = \sigma_X(z) \sigma_Y(z) = [\tau_X(z) \tau_Y(z)]^v \bmod g(z). \quad (7)$$

Since $\gcd(\sigma_{\partial S}, g) = 1$ and $\partial C \subseteq \partial S$, we get $\gcd(\sigma_C, g) = 1$. This implies that there exists the inverse polynomial $\tilde{\sigma}_C(z) \stackrel{\text{def}}{=} 1/[\sigma_C(z)] \bmod g(z) \in K[z] - \{0\}$. Hence, from (7) and $m = uv$, it follows,

$$\sigma_{(X+Y) \bmod m}(z) = [\tilde{\sigma}_C(z)]^m [\tau_X(z) \tau_Y(z)]^v = [\tilde{\sigma}_C(z)^u \tau_X(z) \tau_Y(z)]^v = [\tau_{(X+Y) \bmod m}(z)]^v \bmod g(z);$$

where $\tau_{(X+Y) \bmod m}(z) \stackrel{\text{def}}{=} \tilde{\sigma}_C(z)^u \tau_X(z) \tau_Y(z) \in K[z] - \{0\}$. This implies $(X + Y) \bmod m \in \mathcal{C}_g$. ∎

We note that the cosets of the $\mathbb{Z}_m$ linear code $\mathcal{C}_g$ in (6) are the (possibly empty) codes

$$\mathcal{C}_{g,\sigma} \stackrel{\text{def}}{=} \left\{ X \in \mathbb{Z}_m^n \;\middle|\; \begin{array}{l} \sigma_X(z) = [\tau_X(z)]^v \sigma(z) \bmod g(z), \\ \text{for some } \tau_X(z) \in K[z] - \{0\} \end{array} \right\},$$

with $\sigma(z) \in K[z] - \{0\}$, where $\mathcal{C}_g = \mathcal{C}_{g,1}$.

III. The $\mathbb{Z}_m$ linear BCH-like codes and the BCH-like bound

The class of codes in (6) is so general that, for example, it contains the class of (eventually shortened) BCH codes when $g(z) = z^d$, $d \in \mathbb{N}$, and $m = v = p = char(K)$ (this can be easily shown, for example, with the aid of the Newton's Identity applied to $\sigma_X(z)$). Indeed, even if $m = v = p^l$, $l \in \mathbb{N}$, then some bounds can be given on the minimum L_1 and Lee distances of the codes given in (6) as stated in the following theorem whose proof is given in the Appendix.

***Theorem** 3:* Let $p, l, m = p^l, n \in \mathbb{N}$, K be any field of characteristic $p = char(K) \geq 0$, $\partial S = \{a_1, a_2, \ldots, a_n\} \subseteq K - \{0\}$, with $n \leq |K| - 1$. If $g(z) = z^d \in K[z]$ then the $\mathbb{Z}_m$ linear code in (6) becomes $\mathcal{C} = \mathcal{C}_{z^d,1} =$

$$\mathcal{C}(m, n, d) \stackrel{\text{def}}{=} \left\{ X \in \mathbb{Z}_m^n \,\middle|\, \begin{array}{l} \sigma_X(z) = [\tau_X(z)]^m \bmod z^d, \\ \text{with } \tau_X(z) \in 1 + zK[z] \end{array} \right\} \quad (8)$$

and the following BCH-like bound holds for the minimum symmetric L_1 and Lee distances:

$$d_{L_1}^{sy}(\mathcal{C}(m, n, d)) \geq d_{Lee}(\mathcal{C}(m, n, d)) \geq \deg\left(z^d\right) = d. \quad (9)$$

Also, for the minimum asymmetric L_1 distance:

$$d_{L_1}^{as}(\mathcal{C}(m, n, d)) \geq \begin{cases} \min\{d, m\} & \text{if } m > 0, \\ d & \text{if } m = 0. \end{cases} \quad (10)$$

Note that, even though the codes in (8) have a minimum Lee distance $d \in \mathbb{N}$, their minimum Hamming distance may be less. For example, if $p = 2$, $l = 2$, $m = 2^2 = 4$, $K = GF(4)$, $\partial S = K - \{0\}$ and $d = 2$ then the code in (8) is $\mathcal{C} = \mathcal{C}(4, 3, 2) = \{000, G_1 = 020, G_2 = 002, G_0 = 133, \ldots\}$ (the G_i's are the generators), $d_{Lee}(\mathcal{C}) = d = 2 > 1 = d_H(\mathcal{C})$. However, the code $\mathcal{C}$ can correct $t = 1$ asymmetric L_1 error because $d_{L_1}^{as}(\mathcal{C}) = d = t + 1 = 2$. Indeed, by using the key equation (14) in [16], $\mathcal{C}$ can even correct 1 asymmetric error in the Lee metric (and is perfect in doing so).

IV. The $\mathbb{Z}_m$ linear cyclic codes

Particularly interesting is the case $g(z) = z^d$ where the index set ∂S is composed by the n-th roots of unity. In this case, the codes in (6) become cyclic as shown in the following theorem.

***Theorem** 4:* Let $m, v, n, d \in \mathbb{N}$, K be any field and $\partial S = \{\alpha^0, \alpha^1, \ldots, \alpha^{n-1}\} \subseteq K - \{0\}$; α being a (primitive) n-th root of unity, with $n \leq |K| - 1$. If $g(z) = z^d \in K[z]$ then the code in (6), $\mathcal{C}(m, n, d, v) \stackrel{\text{def}}{=}$

$$\mathcal{C} \stackrel{\text{def}}{=} \left\{ X \in \mathbb{Z}_m^n \,\middle|\, \begin{array}{l} \sigma_X(z) = [\tau_X(z)]^v \bmod z^d, \\ \text{with } \tau_X(z) \in 1 + zK[z] \end{array} \right\} \quad (11)$$

is an m-ary cyclic code of length n. Furthermore, if $m = uv$ with $u \in \mathbb{N}$ then the code in (11) is also $\mathbb{Z}_m$ linear and, in general, $d_{Lee}(\mathcal{C}) \geq \min\{d, v\}$.

Proof: Given $X = x_0 x_1 \ldots x_{n-2} x_{n-1} \in \mathbb{Z}_m^n$ let $X^{\rightarrow} = x_{n-1} x_0 x_1 \ldots x_{n-2} \in \mathbb{Z}_m^n$ indicate the word obtained from X due to a right cyclic shift. From $\sigma_X(z) = \prod_{i=0}^{n-1} \left(1 - \alpha^i z\right)^{x_i}$ and $\alpha^n = \alpha^0 = 1$, it follows $\sigma_X(\alpha z) = \sigma_{X^{\rightarrow}}(z)$. Now, if $X \in \mathcal{C}$ then, for some $k(z) \in K[z]$ and $\tau_X(z) \in 1 + zK[z]$,

$$\begin{array}{l} \sigma_X(z) = [\tau_X(z)]^v \bmod z^d \implies \\ \sigma_X(z) = [\tau_X(z)]^v + k(z) z^d \implies \\ \sigma_X(\alpha z) = [\tau_X(\alpha z)]^v + k(\alpha z) \alpha^d z^d \implies \\ \sigma_{X^{\rightarrow}}(z) = \sigma_X(\alpha z) = [\tau_{X^{\rightarrow}}(z)]^v \bmod z^d, \end{array}$$

with $\tau_{X^{\rightarrow}}(z) \stackrel{\text{def}}{=} \tau_X(\alpha z) \in 1 + zK[z]$. So $X^{\rightarrow} \in \mathcal{C}$. The $\mathbb{Z}_m$ linearity of $\mathcal{C}$ comes from Theorem 2. With regards to the minimum Lee distance of $\mathcal{C}$, note that if $X \in \mathcal{C} - \{0\}$ then either a) $X = v \cdot \partial X$ with $\partial X \neq 0$, or b) $0 \neq X \neq v \cdot \partial X$. If a) holds then, simply, $w_{Lee}^{[m]}(X) = |\lambda^{[m]}(X)| \geq v |\partial(X)| \geq v$. If b) holds then, from Theorem 3 applied to the v-ary code ($\mathcal{C} \bmod v$), the word $(X \bmod v) \in (\mathcal{C} \bmod v) - \{0\}$ and $|\lambda^{[v]}(X)| \geq d$. Since $\lambda^{[m]}$ is non increasing, $|\lambda^{[m]}(X)| \geq |\lambda^{[v]}(X)| \geq d$. ■

Let us focus on the case $m = uv = p^l$, $p = char(K) = 2, 3, 5, 7, \ldots$ prime, $\partial S = \{\alpha^0, \alpha^1, \ldots, \alpha^{n-1}\} \subseteq K - \{0\}$; α being a (primitive) n-th root of unity, with $n \in \mathbb{N}$, $n \leq |K| - 1$. In this case the codes in (11),

$$\begin{array}{l} \mathcal{C} \stackrel{\text{def}}{=} \mathcal{C}(m, n, d, v) \stackrel{\text{def}}{=} \\ \left\{ X \in \mathbb{Z}_m^n \,\middle|\, \begin{array}{l} \sigma_X(z) = [\tau_X(z)]^v \bmod z^d, \\ \text{with } \tau_X(z) \in 1 + zK[z] \end{array} \right\} = \\ \left\{ X \in \mathbb{Z}_m^n \,\middle|\, \begin{array}{l} \sigma_0(X) = 1 \text{ and } \sigma_i(X) = 0 \text{ for any} \\ \text{integer } i \in [1, d-1] \text{ such that } i \neq 0 \bmod v \end{array} \right\} \end{array} \quad (12)$$

are $\mathbb{Z}_m$ linear cyclic codes of length n. Note that, when $m = p^l$, p prime, then all the theories on the m-ary cyclic codes given in [11], [6] and [2] hold. In particular, if any codeword $X \in \mathbb{Z}_m^n$ is represented by the codeword polynomial [2, p. 61] in the variable t,

$$X(t) \stackrel{\text{def}}{=} x_0 + x_1 t + x_2 t^2 + \ldots + x_{n-1} t^{n-1} \in \mathbb{Z}_m[t], \quad (13)$$

then the codes in (12) are ideals of the principal ideal ring $\mathcal{R} \stackrel{\text{def}}{=} \mathbb{Z}_m[t]/(t^n - 1)$ and, for them, the minimum distance properties in Theorem 3 hold. In particular, if $(F_1, F_2, \ldots)$ indicates the ideal generated by $F_1, F_2, \ldots \in \mathcal{R}$ then Theorem 6 and its Corollary in [6] say that any ideal in $\mathcal{R}$ has the forms $(G) = (F_0, pF_1, p^2 F_2, \ldots, p^{l-1} F_{l-1}) \subseteq \mathbb{Z}_m[t]$ where the $F_i(z)$'s are divisors of $t^n - 1 \in \mathbb{Z}_m[t]$ satisfying

$$\begin{array}{l} F_{l-1} | F_{l-2} | \cdots | F_1 | F_0 \text{ and} \\ G(t) \stackrel{\text{def}}{=} g_0 + g_1 t + \ldots + g_{n-1} t^{n-1} = \\ \quad F_0(t) + pF_1(t) + p^2 F_2(t) + \ldots + p^{l-1} F_{l-1}(t) \in \mathbb{Z}_m[t]. \end{array} \quad (14)$$

Starting from the factorization of $t^n - 1 \in \mathbb{Z}_p[t]$ it is possible to find the Hensel lift factorization of $t^n - 1 \in \mathbb{Z}_{m=p^l}[t]$ into basic irreducible polynomials. Now, say, as done in Example 5 of [6], from this factorization it is possible to classify all cyclic codes each of which is identified by a generator of the form in (14). Now, if $G(t)$ is any one of these generators and $G = g_0 g_1 \ldots g_{n-1} \in \mathcal{C} \subseteq \mathbb{Z}_m^n$ then the minimum distances of the code $(G) = \mathcal{C}$ can be lower-bounded with Theorem 3. In other words, the σ-polynomial of the generators of a cyclic code give some information on the minimum L_1 and Lee distances of the code.

***Example** 1:* Let $p = 2$, $l = 3$, $m = 8$, $h = 4$, $K = GF(2^h) = \mathbb{Z}_2[z]/(z^4 + z + 1)$, ∂S be the ordered set $\partial S = (\alpha^0, \alpha^1, \ldots, \alpha^{14}) = K - \{0\}$ and $n = |\partial S| = 15$. Considering K as a vector space over $\mathbb{Z}_2$, define the words $F_0 = 11111\,11111\,11111 = \mathcal{L}(\alpha^0, \alpha^1, \alpha^2, \alpha^3) - \{0\}$, $2F_1 = 22202\,20020\,20000 = 2(\mathcal{L}(\alpha^0, \alpha^1, \alpha^2) - \{0\})$, $4F_2 =$

$44004\,00000\,00000 = 4(\mathcal{L}(\alpha^0,\alpha^1)-\{0\})$ and $G = F_0+2F_1+4F_2$; where $\mathcal{L}(p_1,p_2,\ldots,p_\delta) \le K$ is the linear closures of the multiset $\{p_1,p_2,\ldots,p_\delta\}$. From equation (7) in [21] and (5), we have that $\sigma_{2^iF_i}(z) = 1 + c_i z^8 \bmod z^{12}$, with $c_i \in K$, $i = 0,1,2$. From Theorem 3 with $d = m + m/2 = 12$, $\mathcal{C} \stackrel{\text{def}}{=} (G) \le \mathcal{C}(m=8,n=15,d=12)$ has $d_{Lee}(\mathcal{C}) \ge 12$ and $d^{as}_{L_1}(\mathcal{C}) \ge 8$ (but, note that $4F_2 \in \mathcal{C}$ and so $3 \ge d_H(\mathcal{C})$). Indeed, $\mathcal{C}$ is of type $1^1 2^4 4^6$ (with the notation in [6]) and so it is a $\mathbb{Z}_8$ linear code with $k = \log_8(8^1 4^4 2^6) = 17/3 = 5.\bar{6}$ information digits and length $n = 15$. With an abuse of notation, a generator matrix is,

$$G \stackrel{\text{def}}{=} \left[\begin{array}{cccccccccccccc|c}
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\ \hline
0&2&2&2&0&2&2&0&0&2&0&2&0&0&0\\
0&0&2&2&2&0&2&2&0&0&2&0&2&0&0\\
0&0&0&2&2&2&0&2&2&0&0&2&0&2&0\\
0&0&0&0&2&2&2&0&2&2&0&0&2&0&2\\ \hline
0&0&0&0&0&4&4&0&0&4&0&0&0&0&0\\
0&0&0&0&0&0&4&4&0&0&4&0&0&0&0\\
0&0&0&0&0&0&0&4&4&0&0&4&0&0&0\\
0&0&0&0&0&0&0&0&4&4&0&0&4&0&0\\
0&0&0&0&0&0&0&0&0&4&4&0&0&4&0\\
0&0&0&0&0&0&0&0&0&0&4&4&0&0&4
\end{array}\right].$$

Now, let $RM(\rho,h)$ be the binary ρ-th order Reed-Muller code of length $n+1 = 2^h$, dimension $k = 1 + \binom{h}{1} + \binom{h}{2} + \ldots + \binom{h}{\rho}$ and minimum Hamming distance $d_H = 2^{h-\rho}$ (see [12, pages 370–385]). By adding the parity check symbol $x_\infty = -|X| \bmod 8$ for $X \in \mathcal{C}$ a code $\mathcal{C}^+ = \mathcal{C}^+(m = 8, n = 16, k = 5.\bar{6}, d_{Lee} \ge 16)$ can be obtained. The minimum distance is $d_{Lee}(\mathcal{C}^+) \ge 16$ because of the following. For any $n,h,m = 2^h \in \mathbb{N}$ and $X \in \mathbb{Z}_m^n$, let $B_\rho(X) \stackrel{\text{def}}{=} [\lfloor X/2^\rho \rfloor \bmod 2] \in \mathbb{Z}_2^n$, for all $\rho = 0,1,2$, note that $|X| = |B_0(X)| + 2|B_1(X)| + 4|B_2(X)| \ge |B_0(X)|$ and $B_\rho(x_\infty) = |B_\rho(X)| \bmod 2 = |B_0(X/2^\rho)| \bmod 2$ when $X \in (2^\rho)\cdot\mathbb{Z}^n$. So, if $X \in [(2^\rho)\cdot\mathbb{Z}^n] \cap \mathcal{C}^+$ then $B_0(X/2^\rho) \in RM(\rho,h)$. Also, note that $B_0(X) - B_0(\lambda^{[m]}(X)) = X - \lambda^{[m]}(X) = 0 \bmod 2$ and $\lambda^{[m]}(2X) = 2\lambda^{[m/2]}(X)$. Now, assume $X \in \mathcal{C}^+ - \{0\}$. If $B_0(X) \in (\mathcal{C}^+ \bmod 2) - \{0\}$ then, from above, $B_0(X) \in RM(\rho,h)$, $B_0(\lambda^{[m]}(X)) = B_0(X)$ and so, $|\lambda^{[m]}(X)| \ge |B_0(\lambda^{[m]}(X))| = |B_0(X)| \ge 2^{h-\rho} = 2^{4-0} = 16$. Otherwise, if $B_0(X) = 0$ and $B_1(X) \in [(\mathcal{C}^+/2) \bmod 2] - \{0\}$ then, from above, $X \in 2\mathbb{Z}^n_{m/2}$, $B_0(X/2) \in RM(1,h)$, $B_0(\lambda^{[m/2]}(X/2)) = B_0(X/2)$ and so, $|\lambda^{[m]}(X)| = |\lambda^{[m]}(2(X/2))| = 2|\lambda^{[m/2]}(X/2)| \ge 2|B_0(\lambda^{[m/2]}(X/2))| = 2|B_0(X/2)| \ge 2\cdot 2^{h-\rho} = 2\cdot 2^{4-1} = 16$. Finally, if $B_0(X) = B_1(X) = 0$ then, from above, $B_2(X) \in [(\mathcal{C}^+/4) \bmod 2] - \{0\}$, $X \in 4\mathbb{Z}^n_{m/4}$, $B_0(X/4) \in RM(2,h)$, $B_0(\lambda^{[m/4]}(X/4)) = B_0(X/4)$ and so, $|\lambda^{[m]}(X)| = |\lambda^{[m]}(4(X/4))| = 4|\lambda^{[m/4]}(X/4)| \ge 4|B_0(\lambda^{[m/4]}(X/4))| = 4|B_0(X/4)| \ge 4\cdot 2^{h-\rho} = 16$. Now, not many error correcting $\mathbb{Z}_m$ linear codes are known in the literature, however it is known that the Gray mapping sets a contraction between the metric space $(\mathbb{Z}_{2^l}, d_{Lee})$ and $(\mathbb{Z}_2^l, d_H)$ (which is an isometry for $l = 2$ [11]) [14, p. 321]. This implies that the minimum Hamming distance, d, of the binary codes of length ln gives the minimum Lee distance of at least d with length n over $\mathbb{Z}_{2^l}$. Given this, the extended code $\mathcal{C}^+ = (G)^+$ may be considered equivalent to a linear $(m = 2, n = 3\cdot 16 = 48, k = 3\cdot 5.\bar{6} = 17, d_H \ge 16)$ code which has not been discovered yet and the closer code to this is a linear $(m = 2, n = 51, k = 3\cdot 5.\bar{6} = 17, d_H \ge 16)$ code [9], [13]. So, this example code is rather remarkable. It can be considered a $\mathbb{Z}_8 - RM(2,4)$ code and can be generalized to any $m = 2^l, l, h \in \mathbb{N}$ to get $\mathbb{Z}_m - RM(\rho = h-2, h)$ codes of length $n = 2^h = |K|$, Lee distance $d_{Lee} \ge 2m$ with $k = \log_m|\mathcal{C}^+| = \sum_{i=0}^{l-1}\binom{h}{i} - (1/l)\sum_{i=h-l}^{l-1} i\binom{h}{i}$ data digits.

***Example** 2:* Here the parameters are as in Example 1 but $m = 16$ (i. e., m is doubled). In this case, it is possible to add the word $8F_3 = 80000\,00000\,00000 = 8(\mathcal{L}(\alpha^0) - \{0\})$ as a generator because $\sigma_{8F_3}(z) = 1 + 1\cdot z^8 \bmod z^{12}$. From Theorem 4 with $v = m/2 = 8$ and $d = m/2 + m/4 = 12$, $\mathcal{C} \stackrel{\text{def}}{=} (G) \le \mathcal{C}(m=16,n=15,d=8)$ has $d_{Lee}(\mathcal{C}) \ge v = 8$ and $d^{as}_{L_1}(\mathcal{C}) \ge 8$ (so, it can correct 7 asymmetric errors). The code $\mathcal{C}$ is a $\mathbb{Z}_{16}$ linear code with $k = \log_{16}(16^1 8^4 4^6 2^4) = 32/4 = 8$ information digits and length $n = 15$ which, as in Example 1, can be extended by adding the parity check symbol $x_\infty = -|X| \bmod 16$ for $X \in \mathcal{C}$. In this way, a code $\mathcal{C}^+ = \mathcal{C}^+(m = 16, n = 16, k = 8, d_{Lee} \ge 16)$ can be obtained. It can be considered a $\mathbb{Z}_{16} - RM(3,4)$ code and can be generalized to any $m = 2^l, l \in \mathbb{N}$ to get $\mathbb{Z}_m - RM(\rho = l-1, l)$ codes of length $n = 2^l = |K| = m$, Lee distance $d_{Lee} \ge m$ and $k = \log_m|\mathcal{C}^+| = \log_m \prod_{i=0}^{h}(m/2^i)^{\binom{h}{i}} = m/2$ data digits.

Note that the generator matrices of permutation equivalent codes to all these codes can be constructed as done for $m = 4$ in Subsection II.G of [11].

With regard to decoding, the general T-SyEC/D-SyED Algorithm 2 in [16] is an efficient $GF(2^h)$ field based algebraic decoding algorithm. It relies on solving the general key equation (14) in [16], which is the Lee distance analogous to equation (2) for the L_1 distance [19]. In particular, the above specific examples for $m = 8, 16$ can be used to correct 7 and detect (at least) 8 symmetric Lee errors.

We note that equation (7) in [21] and the Theorems given here are so general that efficient generalizations for any values of the prime p may be possible.

Appendix

For $m,n \in \mathbb{N}$, $X = x_0x_1\ldots x_{n-1} \in \mathbb{Z}_m^n$ and an index set $\partial S \stackrel{\text{def}}{=} \{a_0,a_1,\ldots,a_{n-1}\}$ let $\mu_X(a_i) \stackrel{\text{def}}{=} x_{a_i} \stackrel{\text{def}}{=} x_i \in \mathbb{Z}_m$ be the i-th component of X or, equivalently, the multiplicity of $a_i \in X$.

Proof of Theorem 3: Let us prove (9) first. The leftmost relation comes from $d^{sy}_{L_1}(X,Y) \ge d_{Lee}(X,Y)$, for all $X,Y \in \mathbb{Z}_m^n$. So, let us prove $d_{Lee}(\mathcal{C}(m,n,d)) \ge d$. For any vector $X \in \mathbb{Z}_m^n$, let us write $X = B_0 + B_1p + B_2p^2 + \ldots + B_{l-1}p^{l-1} \in \mathbb{Z}_{p^l}^n = \mathbb{Z}_m^n$, where $B_j \in \mathbb{Z}_p^n$, for all integer $j \in [0, l-1]$. In this way, any component $x_i \in \mathbb{Z}_{p^l}$ of X can be written in the base p number system as $x_i = \mu_X(a_i) = \mu_{B_0}(a_i) + \mu_{B_1}(a_i)p + \ldots + \mu_{B_{l-1}}(a_i)p^{l-1}$ where each component $\mu_{B_j}(a_i)$ of the word/multiset $B_j \in \mathbb{Z}_p^n$ is such that $\mu_{B_j}(a_i) \in \mathbb{Z}_p$, for all integer $i \in [1,n]$ and $j \in [0, l-1]$. Note that, from (5) and (8),

$$X \in \mathcal{C} \iff \sigma_X(z) = \sigma_{B_0}(z)\,[\sigma_{B_1}(z)]^p\,[\sigma_{B_2}(z)]^{p^2}\ldots \ldots\,\big[\sigma_{B_{l-1}}(z)\big]^{p^{l-1}} = [\tau_X(z)]^{p^l} \bmod z^d.$$

Assume $X \in \mathcal{C} - \{0\}$. Then, let $s \in [0, l-1]$ be such that

$$B_0 = B_1 = \ldots = B_{s-1} = 0 \in \mathbb{Z}_p^n \text{ and } B_s \ne 0. \qquad (15)$$

Note that such s exists. For such $X \in \mathcal{C} - \{0\}$ we have

$$\sigma_X(z) = [\sigma_{B_s}(z)]^{p^s} \left[\sigma_{B_{s+1}}(z)\right]^{p^{s+1}} \cdots \left[\sigma_{B_{l-1}}(z)\right]^{p^{l-1}} = [\tau_X(z)]^{p^l} \bmod z^d. \quad (16)$$

Now, for all $j \in [0, l-1]$, $\gcd(\sigma_{\partial S}, z^d) = 1$ and $\partial B_j \subseteq \partial S$ imply $\gcd(\sigma_{B_j}, z^d) = 1$; so, there exists $\left[\sigma_{B_j}(z)\right]^{-1} \bmod z^d$. Hence, from (16) and $s+1 \leq l$, there exists $\tau_{B_s}(z) \in K[z]$ such that $[\sigma_{B_s}(z)]^{p^s} = [\tau_{B_s}(z)]^{p^{s+1}} = \{[\tau_{B_s}(z)]^p\}^{p^s} \bmod z^d$. Since $char(K) = p$, the application $x \to x^{p^s}$ is a (Frobenius) automorphism of K, for all $s \in \mathbb{N}$. So the above relation is equivalent to the polynomial equation

$$k(z)z^d = [\sigma_{B_s}(z) - [\tau_{B_s}(z)]^p]^{p^s} = [\sigma_{B_s}(z)]^{p^s} - \{[\tau_{B_s}(z)]^p\}^{p^s} \quad (17)$$

being true for some $k(z) \in K[z]$ such that $k(z)z^d \in K[z]$ is the p^s-th power of a polynomial. Now, given $q(z) \in K[z]$ let $q^{[r]}(z) \in K[z]$ indicate the polynomial containing only the monomials, say $q_i z^i$, of $q(z)$ such that $i = r \bmod p^s$. From (17), we have

$$k(z)z^d = k^{[(p^s-d) \bmod p^s]}(z)z^d = \left(k^{[(p^s-d) \bmod p^s]}(z)/z^{(p^s-d) \bmod p^s}\right) z^{(p^s-d) \bmod p^s} z^d = [h(z)]^{p^s} \left[z^{\lceil d/p^s \rceil}\right]^{p^s} = \left[h(z)z^{\lceil d/p^s \rceil}\right]^{p^s}$$

where $k^{[(p^s-d) \bmod p^s]}(z)/z^{(p^s-d) \bmod p^s} = [h(z)]^{p^s} \in K[z]$ for some $h(z) \in K[z]$. So, the above relation and (17) give

$$[\sigma_{B_s}(z) - [\tau_{B_s}(z)]^p]^{p^s} = \left[h(z)z^{\lceil d/p^s \rceil}\right]^{p^s}$$

which, by taking the inverse of the Frobenius automorphism, gives $\sigma_{B_s}(z) - [\tau_{B_s}(z)]^p = h(z)z^{\lceil d/p^s \rceil}$, and hence,

$$\sigma_{B_s}(z) = [\tau_{B_s}(z)]^p \bmod z^{\lceil d/p^s \rceil}, \text{ with } B_s \in \mathbb{Z}_p^n - \{0\}.$$

At this point we take the derivative and, since $char(K) = p$, obtain

$$\sigma'_{B_s}(z) = 0 \bmod z^{\lceil d/p^s \rceil - 1}, \text{ with } B_s \in \mathbb{Z}_p^n - \{0\}. \quad (18)$$

Let $\epsilon_{B_s}(z) \in K[z]$ be the evaluator polynomial associated with B_s. From Lemma 1–b) given below with $Y = B_s$, we have $\sigma'_{B_s}(z) = \epsilon_{B_s}(z)\sigma_{B_s \dot{-} \partial B_s}(z)$. Substituting this in (18), we get $\sigma'_{B_s}(z) = \epsilon_{B_s}(z)\sigma_{B_s \dot{-} \partial B_s}(z) = 0 \bmod z^{\lceil d/p^s \rceil - 1}$. So, from $\gcd\left(\sigma_{\partial S}, z^{\lceil d/p^s \rceil - 1}\right) = 1$ and $\partial(B_s \dot{-} \partial B_s) \subseteq \partial B_s \subseteq \partial S$, it follows $\gcd\left(\sigma_{B_s \dot{-} \partial B_s}, z^{\lceil d/p^s \rceil - 1}\right) = 1$; and so,

$$\epsilon_{B_s}(z) = 0 \bmod z^{\lceil d/p^s \rceil - 1} \text{ with } B_s \in \mathbb{Z}_p^n - \{0\}. \quad (19)$$

Since $B_s \in \mathbb{Z}_p^n - \{0\}$, $\epsilon_{B_s}(z) = k(z)z^{\lceil d/p^s \rceil - 1}$ for some $k(z) \in K[z] - \{0\}$. This, $char(K) = p$ and Lemma 1–c) with $Y = B_s$, imply, $|\partial B_s| - 1 \geq \deg(\epsilon_{B_s}) \geq \deg\left(z^{\lceil d/p^s \rceil - 1}\right) = \lceil d/p^s \rceil - 1$. So, from $\partial X \supseteq \partial B_s$, it follows $|\partial X| \geq |\partial B_s| \geq \lceil d/p^s \rceil$. However, from Lemma 2 given below, (15) implies $w_{Lee}(X) \geq p^s |\partial X|$, and so $w_{Lee}(X) \geq p^s |\partial X| \geq p^s \lceil d/p^s \rceil \geq d$. In conclusion, we have shown that either $X = 0 \in \mathcal{C}$ or $w_{Lee}(X) \geq d$. This means that $d_{Lee}(\mathcal{C}(m,n,d)) \geq d$ and (9) is proved.

Let us prove (10) when $m > 0$. Note that if $X \in \mathcal{C}$ then $\sigma_X(z) = [\tau_X(z)]^m \bmod z^d$, with $\tau_X(z) \stackrel{\text{def}}{=} 1 + \tau_1 z + \tau_2 z^2 + \ldots \in K[z] - \{0\}$. Since $char(K) = p$ and $m = p^l$, the application $x \to x^m$ is a Frobenius automorphism of K. Hence,

$$\sigma_X(z) = \prod_{a \in \partial S} (1 - az)^{\mu_X(a)} = 1 + \sigma_1(X)z + \sigma_2(X)z^2 + \ldots = [\tau_X(z)]^m = 1 + \tau_1^m z^m + \tau_2^m z^{2m} + \ldots \bmod z^d$$

implies that $\sigma_i(X) = 0$ for any integer $i \in [1, d-1]$ such that $i \neq 0 \bmod m$ and vice-versa. That is,

$$X \in \mathcal{C} \iff \sigma_i(X) = 0 \text{ for any integer } i \in [1, d-1] \text{ such that } i \neq 0 \bmod m.$$

Let $\delta \stackrel{\text{def}}{=} \min\{d, m\}$. In any case, if $X \in \mathcal{C}$ then $\sigma_i(X) = 0$ for any integer $i \in [1, \delta - 1]$, and so $\mathcal{C}$ is a subset of the σ-code

$$\mathcal{C}_{z^\delta, 1} = \left\{X \in \mathbb{Z}_m^n : \ \sigma_X(z) = 1 \bmod z^\delta\right\},$$

whose minimum asymmetric L_1 distance is δ [20]. Finally, if $m = 0$ then the code $\mathcal{C}$ in (8) itself becomes a σ-code,

$$\mathcal{C} = \mathcal{C}_{z^d, 1} = \left\{X \in \mathbb{N}^n : \ \sigma_X(z) = 1 \bmod z^d\right\}$$

and, again, the minimum asymmetric L_1 distance is d. ■

Lemma 1 (see [22]): Let $m, n \in \mathbb{N}$, K be any field and $\partial S \subseteq K - \{0\}$. For any $Y \in \mathbb{Z}_m^n$ let

$$\lambda_Y(z) = \sigma_{\partial Y}(z) = \prod_{a \in \partial S} (1 - az)^{\mu_{\partial Y}(a)} \in K[z]$$

be the locator polynomial of Y and

$$\epsilon_Y(z) = -\sum_{a \in \partial S} \mu_Y(a) a \prod_{b \in \partial S \dot{-} \{a\}} (1 - bz)^{\mu_{\partial Y}(b)} \in K[z]$$

be the evaluator polynomial of Y. For all $Y \in \mathbb{Z}_m^n$, the following relations hold.

a) $\sigma_Y(z) = \lambda_Y(z)\sigma_{Y \dot{-} \partial Y}(z)$,
b) $\sigma'_Y(z) = \epsilon_Y(z)\sigma_{Y \dot{-} \partial Y}(z)$ and
c) if $m = char(K)$ then Hamming weight of Y satisfies $w_H(Y) = |\partial Y| = \deg(\lambda_Y) \geq \deg(\epsilon_Y) + 1$.

Lemma 2: Let $n, p, h, m = p^l \in \mathbb{N}$, and

$$X \stackrel{\text{def}}{=} B_0 + B_1 p + B_2 p^2 + \ldots + B_{l-1} p^{l-1} \in \mathbb{Z}_m^n;$$

where $B_j \in \mathbb{Z}_p^n$, for all integer $j \in [0, l-1]$. If $s \in [0, l]$ is an integer such that $B_0 = B_1 = \ldots = B_{s-1} = 0$ then the m-ary Lee weight of X is such that $w_{Lee}^{[m]}(X) \geq p^s |\partial X|$.

Proof: If $m = 0$ then the Lee weight is equal to the L_1 weight and the theorem is true because $p^s = 0^0 = 1$. Assume $m > 0$. For all $i \in \partial S \stackrel{\text{def}}{=} [1, n]$, let $x_i = \mu_X(i) \stackrel{\text{def}}{=} p^s y_i \in \mathbb{Z}_{p^l}$ with $y_i = x_i/p^s \in \mathbb{Z}_{m/p^s} = \{0, 1, \ldots, p^{l-s} - 1\}$. This is possible because $B_j = 0$, for all $j \in [0, s-1]$. So, $Y \stackrel{\text{def}}{=} y_1 y_2 \ldots y_n \in \mathbb{Z}_{m/p^s}^n$ and

$$w_{Lee}^{[m]}(X) = \sum_{i \in \partial S} \gamma^{[m]}(x_i) = \sum_{i \in \partial S} \min\{x_i, m - x_i\} = \sum_{i \in \partial S} \min\{p^s y_i, m - p^s y_i\} = \sum_{i \in \partial S} p^s \min\{y_i, (m/p^s) - y_i\} = p^s \sum_{i \in \partial S} \min\{y_i, (m/p^s) - y_i\} = p^s w_{Lee}^{[(m/p^s)]}(Y) \geq p^s |\partial Y|.$$

Since $|\partial Y| = |\partial X|$ the statement follows. ■

REFERENCES

[1] E. R. Berlekamp, *Algebraic Coding Theory* - Revised 1984 Edition, Aegean Park Press, 1984.

[2] Richard E. Blahut, *Algebraic Codes on Lines, Planes, and Curves: An Engineering Approach*, Cambridge University Press, 2008.

[3] B. Bose and S. Cunningham, "Systematic and Multiple Asymmetric Error Codes", *IEEE International Symposium on Information Theory*, Ste. Jovite, Quebec, Canada, 25-29 September 1983.

[4] B. Bose and S. Cunningham, "Asymmetric Error Correcting Codes", *Sequences II: Combinatorics, Compression, Security, and Transmission*, Springer-Verlag (Editors: R. Capocelli, A. De Santis and U. Vaccaro), pp. 24-35, 1993.

[5] B. Bose, N. Elarief and L. G. Tallini, "On Codes Achieving Zero Error Capacities in Limited Magnitude Error Channels", *IEEE Transactions on Information Theory*, vol. 64, no. 1, pp. 257-273, January 2018.

[6] A. R. Calderbank and N. J. A. Sloane, "Modular and p-adic Cyclic Codes", *Designs, Codes and Cryptography*, Vol. 6, no. 1, pp. 21-35. July 1995. Also at http://arxiv.org/abs/math/0311319v1.

[7] Y. Cassuto, M. Schwartz, V. Bohossian and J. Bruck, "Codes for Asymmetric Limited-Magnitude Errors with Application to Multilevel Flash Memories", *IEEE Transactions on Information Theory*, vol. 56, no. 4, pp. 1582-1595, April 2010.

[8] R. Graham and N. Sloane, "Lower Bounds for Constant Weight Codes", *IEEE Transactions on Information Theory*, vol. 26, no. 1, pp. 37-43, January 1980.

[9] M. Grassl, "Bounds on the Minimum Distance of Linear Codes and Quantum Codes", Online available at http://www.codetables.de.

[10] S. Elmougy, L. Pezza, L. G. Tallini, A. Al-Dhelaan and B. Bose, "Diversity Combining Type I-Hybrid ARQ Protocol over m-ary Asymmetric Varshamov Channels", *Computers & Electrical Engineering*, vol. 77, pp. 389-397, July 2019.

[11] A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane and P. Solé, "The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and Related Codes", *IEEE Transactions on Information Theory*, vol. 40, no. 2, pp. 301-319. March 1994.

[12] F. J. MacWilliam and N. J. A. Slone, *The Theory of Error Correcting Codes*, North-Holland, 1977.

[13] "MinT – the Online Database for Optimal Parameters of (t, m, s)-Nets, (t, s)-Sequences, Orthogonal Arrays, Linear Codes, and OOAs", at http://mint.sbg.ac.at/.

[14] R. M. Roth, *Introduction to Coding Theory*, Cambridge Univ. Press, Cambridge, United Kingdom, 2006.

[15] L. G. Tallini, N. Alqwaifly and B. Bose, "Deletions and Insertions of the Symbol "0" and Asymmetric/Unidirectional Error Control Codes for the L_1 Metric", *IEEE Transactions on Information Theory*, vol. 69, no. 1, pp. 86-106, January 2023.

[16] L. G. Tallini and B. Bose, "On Some New $\mathbb{Z}_m$ Linear Codes Based on Elementary Symmetric Functions", *2018 IEEE International Symposium on Information Theory*, pp. 1665-1669, June 2018.

[17] L. G. Tallini and B. Bose, "On L_1 Metric Asymmetric/Unidirectional Error Control Codes, Constrained Weight Codes and σ-codes", *2013 IEEE International Symposium on Information Theory*, pp. 694-698, July 2013.

[18] L. G. Tallini, B. Bose, "On Symmetric L_1 Distance Error Control Codes and Elementary Symmetric Functions", *2012 IEEE International Symposium on Information Theory*, pp. 741-745, July 2012.

[19] L. G. Tallini and B. Bose, "On Symmetric/Asymmetric Lee Distance Error Control Codes and Elementary Symmetric Functions", *2012 IEEE International Symposium on Information Theory*, pp. 746-750, July 2012.

[20] L. G. Tallini and B. Bose, "On L_1-Distance Error Control Codes", *2011 IEEE International Symposium on Information Theory*, pp. 1026-1030, July/August 2011.

[21] L. G. Tallini and B. Bose, "Reed-Muller codes, Elementary Symmetric Functions and Asymmetric Error Correction", *2011 IEEE International Symposium on Information Theory*, pp. 1016-1020, July/August 2011.

[22] L. G. Tallini and B. Bose, "On Decoding Some Error Control Codes using the Elementary Symmetric Functions". In *Trends in Incidence and Galois Geometries: a Tribute to Giuseppe Tallini - Quaderni di Matematica*, F. Mazzocca, N. Melone and D. Olanda Ed.. vol. 19, p. 265-297, Caserta, Dipartimento di Matematica, Seconda Università di Napoli, 2010.

[23] L. G. Tallini, N. Elarief and B. Bose, "On Efficient Repetition Error Correcting Codes", *2010 IEEE International Symposium on Information Theory*, pp. 1012-1016, June 2010.

[24] L. G. Tallini and B. Bose, "On a New Class of Error Control Codes and Symmetric Functions", *2008 IEEE International Symposium on Information Theory*, pp.980-984, July 2008.

[25] J. H. Weber, C. de Vroedt, D. E. Boekee, "Necessary and Sufficient Conditions on Block Codes Correcting/Detecting Errors of Various Types", *IEEE Transactions on Computers*, vol. 41, no. 9, pp. 1189-1193, September 1992.