Lee-Metric BCH Codes and their Application to Constrained and Partial-Response Channels

Ron M. Roth* Paul H. Siegel†

Abstract

We show that each code in a certain class of BCH codes over $GF(p)$, specified by a code length $n \leq p^m - 1$ and a runlength $r \leq (p-1)/2$ of consecutive roots in $GF(p^m)$, has minimum Lee distance $\geq 2r$. For the very high-rate range these codes approach the sphere-packing bound on the minimum Lee distance. Furthermore, for a given r, the length range of these codes is twice as large as that attainable by Berlekamp's extended negacyclic codes. We present an efficient decoding procedure, based on Euclid's algorithm, for correcting up to $r-1$ errors and detecting r errors, that is, up to the number of Lee errors guaranteed by the designed minimum Lee distance $2r$. Bounds on the minimum Lee distance for $r \geq (p+1)/2$ are provided for the Reed-Solomon case i.e., when the BCH code roots are in $GF(p)$. We present two applications. First, Lee-metric BCH codes can be used for protecting against bitshift errors and synchronization errors caused by insertion and/or deletion of zeros in (d,k)-constrained channels. Second, the code construction with its decoding algorithm can be formulated over the integer ring, providing an algebraic approach to correcting errors in partial-response channels where matched spectral-null codes are used.

Key words: BCH codes; constrained channels; decoding; Lee metric; partial-response channels.

---

*Computer Science Department, Technion — Israel Institute of Technology, Haifa 32000, Israel. This work was done in part while the author was visiting IBM Research Division, Almaden Research Center, San Jose, CA 95120.

†IBM Research Division, Almaden Research Center K65/802, 650 Harry Road, San Jose, CA 95120.

1 Introduction

The Lee metric [14],[25] was developed as an alternative to the Hamming metric for transmission of non-binary signals (usually taken from $GF(p)$) over certain noisy channels. The Lee distance $d_{\mathcal{L}}(x, y)$ between two elements x, y in $GF(p)$ is the smallest absolute value of any integer congruent, modulo p, to the difference $x - y$. Therefore, the Lee metric is "circular" when applied to $GF(p)$, and, for this reason, has on occasion been proposed for use in the context of phase modulation [2, Section 8.2]. Codes for the Lee metric were described first by Lee [14] and Ulrich [25], but perhaps the most important and well-known codes for the Lee metric are the negacyclic codes introduced by Berlekamp [2, Ch. 9], for which there is an efficient decoding procedure. The core of the decoding procedure is the application of the Berlekamp-Massey algorithm to a polynomial congruence similar to the key equation for BCH codes in the Hamming metric. Later, Chang and Wolf [3] devised a family of cyclic codes, for odd codeword lengths, with Lee-metric properties very similar to those of the negacyclic codes. See also [6],[24],[1].

The definition of the Lee metric can be generalized in a straightforward manner also to integer rings. In [21], Nakamura obtained a construction of codes for the Lee metric over the ring of integers modulo 2^h that is capable of correcting up to two errors. A nonlinear construction over such rings for correcting any prescribed number of errors was described recently by Orlitsky [22]. His construction is based on dividing a codeword of a binary BCH code into nonoverlapping h-tuples and regarding the latter as the Gray-code representations of the integers between 0 and $2^h - 1$.

The Lee metric extends to symbols drawn from the alphabet of rational integers, where the Lee distance between symbols corresponds to the absolute value of their difference. Jinushi and Sakaniwa [10] recently reported a construction method for error-correcting codes over the integers that relies upon properties of generalized Hadamard matrices. (They use the term *absolute summation distance* to refer to the Lee distance in the context of the integer alphabet). Karabed and Siegel [11] observed that ensembles of integer sequences with higher-order nulls in the power spectral density at rational submultiples of the symbol frequency have substantial Lee-distance properties. The lower bound on the minimum Lee distance of such sequences generalizes a lower bound on the minimum Hamming distance for binary block codes with higher-order spectral density null at zero frequency, due to Immink

and Beenker [9].

As mentioned in [11], the appearance of Newton's identities in the proof of the lower bounds on the minimum Lee distance for integer spectral-null codes suggested the existence of efficient, iterative decoding algorithms akin to those developed for BCH and Goppa codes in the Hamming metric. The details of such a decoding algorithm for spectral-null codes will be presented in this paper, but in the broader context of a BCH class of error-correcting codes for the Lee metric over $GF(p)$, as we now describe.

Motivated by the similarity in form of the moment equations characterizing integer block codes with a higher-order spectral null and the parity-check equations of BCH codes, we define in Section 2 a class of BCH codes over $GF(p)$, with each code specified by a code length $n \leq p^m - 1$ and a runlength r of consecutive roots in $GF(p^m)$.

In Section 3, we prove that, for those codes in this class satisfying the constraint that $r \leq (p-1)/2$, the minimum Lee distance is bounded from below by $2r$. The performance of these codes is compared with that of the negacyclic codes and their generalizations. For a given r and redundancy, the length range of the Lee-metric BCH codes is shown to be twice as large as that achieved by the negacyclic code construction. Furthermore, for small values of r and for sufficiently large m, Lee-metric BCH codes of length $n = p^m - 1$ approach the sphere-packing upper bound on the minimum Lee distance.

Section 4 addresses extensions and improvements of the $2r$ lower bound in the base-field case, which corresponds to Reed-Solomon codes of lengths $n \leq p - 1$ over $GF(p)$. In Subsection 4.1 we first extend the $2r$ lower bound to all values $r \leq n \leq p - 1$. Then, in Subsection 4.2, we provide a refined bound that, for the low-dimension (high-redundancy) case, becomes quadratic (rather than linear) in r. For $r \geq \frac{6}{7}p$, this bound improves upon the $2r$ lower bound.

Section 5 addresses the issue of decoding Lee-metric BCH codes. We develop a modified 'key equation' and present a decoding procedure, based upon Euclid's algorithm, that can correct all error patterns up to Lee weight $r - 1$ and detects all error patterns of Lee weight r, for codes with designed minimum Lee distance $2r$. The time complexity of the decoding algorithm for the proposed codes is similar to that of the known Hamming-metric decoding algorithms for BCH codes, and the algorithm appears to be simpler than Berlekamp's Lee-

metric decoding algorithm for negacyclic codes [2, Algorithm 9.36].

Finally, in Section 6, we discuss two applications. First, in Subsection 6.1, we discuss the use of Lee-metric BCH codes to detect and/or correct synchronization errors, caused by insertion and/or deletion of zero symbols, in runlength-limited (d, k) channels, such as those found in digital recording. We also show that, with a slight modification of the decoding procedure, some of the Lee-metric BCH codes can be used to provide even more efficient protection against a special subset of synchronization errors known as bitshift errors that predominate in magnetic recording systems. The performance of these codes is compared to that of the recently published family of shift-error-correcting modulation (SECM) codes [7] that are based upon Hamming-metric BCH codes.

Then, in Subsection 6.2, completing the circle, we return to the application that prompted this work, and use the decoding algorithm of Section 5 to develop an algebraic approach to the demodulation of integer-valued, spectral-null codes when used as matched-spectral-null codes on noisy partial-response channels where the Lee metric pertains.

Another application of Lee-metric codes in the area of interactive communication is described in [22].

2 Definitions

Let $C(n, r, \boldsymbol{\alpha}; p)$ be the (shortened) BCH code of length n over $GF(p)$ whose parity-check matrix is

$$H(n, r, \boldsymbol{\alpha}; p) \stackrel{\Delta}{=} \begin{bmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_n^2 \\ \vdots & \vdots & \dots & \vdots \\ \alpha_1^{r-1} & \alpha_2^{r-1} & \dots & \alpha_n^{r-1} \end{bmatrix},$$

where $\boldsymbol{\alpha} = [\, \alpha_1 \, \alpha_2 \, \dots \, \alpha_n \,]$ is the *locator vector*, consisting of distinct nonzero elements of the smallest field $GF(p^m)$ of size greater than n. Hence, a word $\mathbf{c} = [\, c_1 \, c_2 \, \dots \, c_n \,] \in GF(p)^n$ is

in $C(n, r, \boldsymbol{\alpha}; p)$ if and only if it satisfies the following r parity-check equations over $GF(p^m)$:

$$\sum_{j=1}^{n} c_j \alpha_j^{\ell} \;=\; 0 \;, \quad \ell = 0, 1, \ldots, r-1 \;. \tag{1}$$

For $\ell \geq 1$, each parity-check equation in (1) translates into m equations over $GF(p)$. This gives the following well-known lower bound on the dimension k, or, rather, an upper bound on the redundancy $n-k$, of $C(n, r, \boldsymbol{\alpha}; p)$:

$$n - k \;\leq\; 1 \;+\; (r-1)\, m \;. \tag{2}$$

Furthermore, since the entries of $\mathbf{c}$ are in $GF(p)$, $\sum_{j=1}^{n} c_j \alpha_j^{\ell} = 0$ implies $\sum_{j=1}^{n} c_j \alpha_j^{p\,\ell} = 0$. Therefore, (2) can be improved to

$$n - k \;\leq\; 1 \;+\; \left\lceil \tfrac{p-1}{p}\,(r-1) \right\rceil \, m \;.$$

However, as we shall be mainly concentrating on values of r which are smaller than p, the bound (2) will be sufficient for our purposes.

The codes $C(n, r, \boldsymbol{\alpha}; p)$ for which $n = p^m - 1$ will be called *primitive*. In this case, $\boldsymbol{\alpha}$ is unique, up to permutation of coordinates, and, therefore, we shall sometimes use the short-hand notation $C(p^m - 1, r; p)$ for $C(p^m - 1, r, \boldsymbol{\alpha}; p)$. For primitive codes, the bound (2) becomes

$$n - k \;\leq\; 1 \;+\; (r-1) \log_p(n+1) \;. \tag{3}$$

Remark 1. The requirement that the α_j be nonzero elements of $GF(p^m)$ is not essential as long as $n \leq p^m - 1$. This is due to the fact that, by linear operations on the rows of $H(n, r, \boldsymbol{\alpha}; p)$, we can obtain another parity-check matrix

$$H(n, r, \tilde{\boldsymbol{\alpha}}; p) \;=\; \begin{bmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 - \beta & \alpha_2 - \beta & \ldots & \alpha_n - \beta \\ (\alpha_1 - \beta)^2 & (\alpha_2 - \beta)^2 & \ldots & (\alpha_n - \beta)^2 \\ \vdots & \vdots & \ldots & \vdots \\ (\alpha_1 - \beta)^{r-1} & (\alpha_2 - \beta)^{r-1} & \ldots & (\alpha_n - \beta)^{r-1} \end{bmatrix} \tag{4}$$

for $C(n, r, \boldsymbol{\alpha}; p)$ for any $\beta \in GF(p^m)$. Therefore, there is no loss of generality in assuming that the α_j are nonzero, and we shall indeed assume so throughout this paper. (In fact, the

code of length $n = p^m$, obtained by setting all the elements of $GF(p^m)$ as coordinates of $\boldsymbol{\alpha}$, can be regarded as a shortened code of $C(p^{2m}-1, r; p)$, and this is by setting β in (4) to be an element of $GF(p^{2m}) - GF(p^m)$. However, in this case we will treat the locator vector $\boldsymbol{\alpha}$ as a vector over $GF(p^{2m})$, rather than over $GF(p^m)$. This delicate observation will become significant when $m = 1$.) •

A special interesting case is the base-field case $m = 1$ which corresponds to (generalized) Reed-Solomon codes of length $n \leq p-1$ over $GF(p)$. In this case, the α_j are distinct nonzero elements of $GF(p)$, and the dimension of these codes is equal to $n-r$. The generator matrix of primitive base-field codes $C(p-1, r; p)$ has the form

$$G(p-1, r; p) \stackrel{\Delta}{=} \begin{bmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_{p-1} \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_{p-1}^2 \\ \vdots & \vdots & \dots & \vdots \\ \alpha_1^{p-r-1} & \alpha_2^{p-r-1} & \dots & \alpha_{p-1}^{p-r-1} \end{bmatrix} .$$

In the sequel we shall use the symbols $0, 1, 2, \dots, p-1$ both for elements of $GF(p)$ and for the first p nonnegative integers. In those cases where a distinction is necessary (say, to specify whether operations are taken over $GF(p)$ or over the integers), we shall overline the integer values. Hence, for an element $\alpha \in GF(p)$, we denote by $\overline{\alpha}$ the smallest nonnegative integer such that $\alpha = \overline{\alpha} \cdot 1$, where 1 stands for the multiplicative unity in $GF(p)$.

For an element $\alpha \in GF(p)$, we define the *Lee value* $|\alpha|$ by

$$|\alpha| \stackrel{\Delta}{=} \begin{cases} \overline{\alpha} & \text{when } 0 \leq \overline{\alpha} \leq (p-1)/2 \\ p - \overline{\alpha} & \text{when } (p+1)/2 \leq \overline{\alpha} \leq p-1 \end{cases} .$$

The elements $0, 1, \dots, (p-1)/2$ of $GF(p)$ will be referred to as the 'positive' elements of the field, for which $\overline{\alpha} = |\alpha|$. The rest of the elements are the 'negative' ones.

For a vector $\mathbf{c} = [\, c_1\, c_2\, \dots\, c_n\,]$ over $GF(p)$, we define the *Lee weight* by $\|\mathbf{c}\| \stackrel{\Delta}{=} \sum_{j=1}^{n} |c_j|$ (summation taken over the integers). The *Lee distance* between two vectors in $GF(p)^n$ is defined as the Lee weight of their difference. The *minimum Lee distance* of a subset X of $GF(p)^n$ is the minimum Lee distance between any pair of distinct vectors in X. Since $C(n, r, \boldsymbol{\alpha}; p)$ is an additive subgroup of $GF(p)^n$, the minimum Lee distance of

$C(n, r, \boldsymbol{\alpha}; p)$, denoted $d_{\mathcal{L}}(n, r, \boldsymbol{\alpha}; p)$, is also the minimum Lee weight of any nonzero codeword in $C(n, r, \boldsymbol{\alpha}; p)$.

Given a 'transmitted' word $\mathbf{c} \in GF(p)^n$ (say, a codeword in $C(n, r, \boldsymbol{\alpha}; p)$) and a 'received' word $\mathbf{y} \in GF(p)^n$, the error vector is defined by $\mathbf{e} \stackrel{\Delta}{=} \mathbf{y} - \mathbf{c}$. The number of *Lee errors* is given by $\|\mathbf{e}\|$; that is, the number of Lee errors is the smallest number of additions of ± 1 to the coordinates of the transmitted codeword $\mathbf{c}$ which yield the received word $\mathbf{y}$. Since the Lee weight satisfies the triangle inequality, using a code of minimum Lee distance $d_{\mathcal{L}}$ allows to correct any pattern of up to $(d_{\mathcal{L}} - 1)/2$ Lee errors.

One of the applications that motivated this work was analyzing the correction capability of matched-spectral-null trellis codes for partial-response channels [11]. These codes can be modeled as sets of vectors $\mathbf{c} = [\, c_1 \, c_2 \, \ldots \, c_n \,]$ over the integer ring $\mathcal{Z}$ that satisfy the set of constraints

$$\sum_{j=1}^{n} (j-1)^{\ell} \, c_j \;=\; 0 \,, \quad \ell = 0, 1, \ldots, r-1 \tag{5}$$

(where $0^0 \stackrel{\Delta}{=} 1$), for some prescribed order r of the spectral null at zero frequency. The constraints in (5) are equivalent, in turn, to

$$\sum_{j=1}^{n} j^{\ell} \, c_j \;=\; 0 \,, \quad \ell = 0, 1, \ldots, r-1$$

(compare with (4)). Hence, along with the codes $C(n, r, \boldsymbol{\alpha}; p)$, we shall be interested also in additive subgroups $C(n, r, \boldsymbol{\alpha})$ of $\mathcal{Z}^n$ consisting of words $\mathbf{c} \in \mathcal{Z}^n$ that satisfy the constraint $H(n, r, \boldsymbol{\alpha})\, \mathbf{c} \;=\; \mathbf{0}$, where $\boldsymbol{\alpha} = [\, \alpha_1 \, \alpha_2 \, \ldots \, \alpha_n \,]$ is a locator vector of distinct integers entries $0 < \alpha_1 < \alpha_2 < \ldots < \alpha_n$ and $H(n, r, \boldsymbol{\alpha}) \stackrel{\Delta}{=} \left[\alpha_j^{\ell} \right]_{\ell=0, j=1}^{r-1, n}$. When $\boldsymbol{\alpha} = [\, 1 \, 2 \, \ldots \, n \,]$ we shall use the shorter notation $C(n, r)$ for $C(n, r, \boldsymbol{\alpha})$.

Defining the Lee value of an integer as its (conventional) absolute value, the definition of the Lee weight of an integer vector, as well as the minimum Lee distance of any subset of $\mathcal{Z}^n$, is extended in a natural way. The minimum Lee distance of $C(n, r, \boldsymbol{\alpha})$ will be denoted by $d_{\mathcal{L}}(n, r, \boldsymbol{\alpha})$.

3 The $2r$ lower bound

In [11], a lower bound $d_{\mathcal{L}}(n,r) \geq 2r$ on the minimum Lee distance of $C(n,r)$ was derived. The proof was a slight generalization of an argument, based upon Newton's identities, that was used in [9] to bound from below the minimum Hamming distance of binary codes with rth order spectral null at zero frequency. In fact, the very same proof can be used to show the more general lower bound $d_{\mathcal{L}}(n,r,\boldsymbol{\alpha}) \geq 2r$. Our goal in this section is to show that the $2r$ lower bound, with certain necessary restrictions on r, applies also to $d_{\mathcal{L}}(n,r,\boldsymbol{\alpha};p)$. More specifically, we prove the following.

Theorem 1.

$$d_{\mathcal{L}}(n,r,\boldsymbol{\alpha};p) \;\geq\; \begin{cases} 2r & \text{for } r \leq (p-1)/2 \\ p & \text{for } (p+1)/2 \leq r < p \end{cases} .$$

This bound is, in a way, the analog of the BCH lower bound $r+1$ on the minimum Hamming distance of $C(n,r,\boldsymbol{\alpha};p)$, although the proof of the $2r$ lower bound is slightly more complicated. For $r \geq p$ we can bound $d_{\mathcal{L}}(n,r,\boldsymbol{\alpha};p)$ from below by the minimum Hamming distance $r+1$.

At this point, it is worthwhile comparing the performance of $C(n,r,\boldsymbol{\alpha};p)$ in the Lee space with that of negacyclic codes [2, Ch. 9]. The latter, or, rather, generalized versions thereof, are defined as codes of length $n \leq (p^m-1)/2$ over $GF(p)$ whose parity-check matrix is of the form

$$H_{\text{negacyclic}}(n,r,\boldsymbol{\alpha};p) \;\triangleq\; \begin{bmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \alpha_1^3 & \alpha_2^3 & \dots & \alpha_n^3 \\ \alpha_1^5 & \alpha_2^5 & \dots & \alpha_n^5 \\ \vdots & \vdots & \dots & \vdots \\ \alpha_1^{2r-3} & \alpha_2^{2r-3} & \dots & \alpha_n^{2r-3} \end{bmatrix} , \tag{6}$$

where $\boldsymbol{\alpha} = [\,\alpha_1\,\alpha_2\,\dots\,\alpha_n\,]$ consists of distinct nonzero elements $\alpha_j \in GF(p^m)$ such that $\alpha_j + \alpha_\ell \neq 0$ for all j and ℓ. For $r \leq (p-1)/2$, the known lower bound on the minimum Lee distance of negacyclic codes is $2r-1$ [2, Ch. 9], and this bound becomes $2r$ if we extend the codes by adding an all-one row to their parity-check matrix. The upper bound on the redundancy of these extended codes is equal to the corresponding bound (2) for

$C(n, r, \boldsymbol{\alpha}; p)$. However, given m (dictated by specifications on r and redundancy constraints), the maximum attainable length of extended negacyclic codes is only half the maximum length of $C(n, r, \boldsymbol{\alpha}; p)$. As we shall see in Section 5, the decoding algorithm of $C(n, r, \boldsymbol{\alpha}; p)$ appears to be simpler than Berlekamp's decoding algorithm for the negacyclic case.

We point out that the construction of [22] for length n and designed minimum distance $2r-1$ over the ring of integers modulo $q = 2^h$ has redundancy $(r-1)\lceil \log_q(nh) \rceil$, namely, similar to that of negacyclic codes.

Before getting into the proof of Theorem 1, we show that, for $(p+1)/2 \leq r < p$, the bound $d_{\mathcal{L}}(n, r, \boldsymbol{\alpha}; p) \geq p$ cannot be improved for certain choices of n and $\boldsymbol{\alpha}$, e.g., when $C(n, r, \boldsymbol{\alpha}; p)$ is primitive. Let the code length n be at least p, thus implying $m \geq 2$. In addition, assume that the first p elements of $\boldsymbol{\alpha}$ are given by $\alpha_j = \beta + j - 1$ for some $\beta \in GF(p^m) - GF(p)$. Now, the power sums $\sum_{j=1}^{p}(j-1)^\ell$, and therefore $\sum_{j=1}^{p} \alpha_j^\ell$, vanish for every $0 \leq \ell \leq p-2$. Hence, for any $r < p$, there is a codeword in $C(n, r, \boldsymbol{\alpha}; p)$ consisting of p ones followed by $n-p$ zeros, thus implying the upper bound $d_{\mathcal{L}}(n, r, \boldsymbol{\alpha}; p) \leq p$. Note that this proof does not hold in the base-field case $n \leq p-1$, in which case the set $GF(p^m) - GF(p)$ is empty. And, indeed, in Subsection 4.1 we show that, in the base-field case, the $2r$ lower bound applies also to the range $r \geq (p+1)/2$.

The following definition will be useful in our subsequent discussions: Given a locator vector $\boldsymbol{\alpha} = [\, \alpha_1 \, \alpha_2 \, \ldots \, \alpha_n \,]$ of a code $C(n, r, \boldsymbol{\alpha}; p)$ and a word $\mathbf{y} = [\, y_1 \, y_2 \, \ldots \, y_n \,] \in GF(p)^n$, define the *locator polynomial* associated with $\mathbf{y}$ as the polynomial $\sigma(x)$ over $GF(p^m)$ given by

$$\sigma(x) \stackrel{\Delta}{=} \prod_{j=1}^{n} (1 - \alpha_j x)^{|y_j|} \, .$$

The definition of locator polynomial extends easily to the integer ring as well.

Example 1. Let $p = 7$, $m = 1$, and $\alpha_j = j$. For $\mathbf{y} = [\, 0\, 2\, 5\, 0\, 3\, 6 \,]$ we have

$$\sigma(x) = (1-2x)^2(1-3x)^2(1-5x)^3(1-6x) \, . \qquad \bullet$$

Let $\sigma(x)$ be a polynomial over a field F of the form $\prod_{j=1}^{t}(1-\beta_j x)$, where β_j, $j = 1, 2, \ldots t$, are (not necessarily distinct) elements of F. For $\ell \geq 1$, we define the ℓth power sum, S_ℓ,

associated with $\sigma(x)$ by

$$S_\ell \;\triangleq\; \sum_{j=1}^{t} \beta_j^\ell \;. \tag{7}$$

The proof of Theorem 1 is based on the following lemma.

Lemma 1. (Newton's identities [16, Ch. 8]). *Let* $\sigma(x) = \sum_{i=0}^{\infty} \sigma_i x^i$ *be the following polynomial of finite degree* $\deg \sigma$,

$$\sigma(x) \;=\; 1 + \sum_{i=1}^{\deg \sigma} \sigma_i x^i \;=\; \prod_{j=1}^{\deg \sigma} (1 - \beta_j x) \;,$$

where β_j *are elements of a field* F. *For* $\ell \geq 1$, *let* S_ℓ *denote the* ℓ*th power sum as in (7). Then,*

$$\sum_{\ell=0}^{i-1} \sigma_\ell S_{i-\ell} + i\sigma_i \;=\; 0 \quad \textit{for all} \quad i \geq 1 \;. \tag{8}$$

In particular, by (8) we have

$$\sum_{\ell=0}^{i-1} \sigma_\ell S_{i-\ell} \;=\; 0 \quad \text{for all} \quad i > \deg \sigma \;.$$

The latter equations are the basis for Massey's decoding algorithm for BCH codes in the Hamming metric [18].

Using the notation $S(x)$ for the formal power-sum series $\sum_{\ell=1}^{\infty} S_\ell x^\ell$, we can rewrite (8) as

$$\sigma(x)\, S(x) \;+\; x\, \sigma'(x) \;=\; 0 \;,$$

where $\sigma'(x)$ is the formal derivative $\sum_{i \geq 1} i\, \sigma_i x^{i-1}$ of $\sigma(x)$.

Remark 2. Given r and the values S_ℓ for $1 \leq \ell \leq r-1$, the coefficients σ_i, $0 \leq i \leq r-1$, are uniquely defined by (8) when F has characteristic zero: simply solve iteratively for σ_i, starting with $\sigma_0 = 1$ and continuing with

$$\sigma_i \;=\; -\frac{1}{i} \sum_{\ell=0}^{i-1} \sigma_\ell S_{i-\ell} \;. \tag{9}$$

When the characteristic of F is p, we can apply (9) over F for values i which are smaller than p. Hence, over such fields F, the values σ_i are uniquely defined for $0 \leq i \leq \min\{r, p\} - 1$. •

Proof of Theorem 1. The proof is very similar to the one presented in [11]. For the sake of completeness, and for future reference in this paper, we repeat the proof here.

Assume that $\mathbf{c}$ is a codeword of $C(n, r, \boldsymbol{\alpha}; p)$ of Lee weight $< 2r$. We show that either $\|\mathbf{c}\| \geq p$ or $\mathbf{c} = \mathbf{0}$. Let $\mathbf{c}^+ = [\, c_1^+ \, c_2^+ \, \ldots \, c_n^+ \,]$ be the word defined by

$$c_j^+ \;=\; \begin{cases} c_j & \text{if } c_j \in \{1, 2, \ldots, (p-1)/2\} \\ 0 & \text{otherwise} \end{cases}$$

and let $\mathbf{c}^- \stackrel{\Delta}{=} \mathbf{c}^+ - \mathbf{c}$. That is, $\mathbf{c}^+$ is equal to $\mathbf{c}$ at the latter's 'positive' entries, and is zero otherwise, whereas the entries of $\mathbf{c}^-$ take the Lee values of the 'negative' entries of $\mathbf{c}$, leaving the other locations zero. Let $\sigma^+(x)$ and $\sigma^-(x)$ denote the locator polynomials of $\mathbf{c}^+$ and $\mathbf{c}^-$, respectively, and let $S^+(x) = \sum_{\ell=1}^{\infty} S_\ell^+ x^\ell$ and $S^-(x) = \sum_{\ell=1}^{\infty} S_\ell^- x^\ell$ be the formal power-sum series over $GF(p^m)$ associated with $\sigma^+(x)$ and $\sigma^-(x)$, as defined in (7). From $H(n, r, \boldsymbol{\alpha}; p)\, \mathbf{c} = \mathbf{0}$ we deduce the following r equations

$$H(n, r, \boldsymbol{\alpha}; p)\, \mathbf{c}^+ \;=\; H(n, r, \boldsymbol{\alpha}; p)\, \mathbf{c}^- \tag{10}$$

over $GF(p^m)$. The first equation in (10) reads

$$\|\mathbf{c}^+\| \;\equiv\; \|\mathbf{c}^-\| \pmod{p}\,, \tag{11}$$

whereas the other $r-1$ equation can be rewritten as

$$S_\ell^+ = S_\ell^-\,, \quad \ell = 1, 2, \ldots, r-1\,,$$

or, equivalently,

$$S^+(x) \;\equiv\; S^-(x) \pmod{x^r}\,. \tag{12}$$

Therefore, by Remark 2 we obtain

$$\sigma^+(x) \;\equiv\; \sigma^-(x) \pmod{x^r}\,. \tag{13}$$

Assume first that $\|\mathbf{c}^+\| \neq \|\mathbf{c}^-\|$. By (11) we must have $\|\mathbf{c}^+\| = \|\mathbf{c}^-\| \pm \ell \cdot p$ for some $\ell \neq 0$ and, hence, $\|\mathbf{c}\| = \|\mathbf{c}^+\| + \|\mathbf{c}^-\| \geq p$ (note that this may happen only when $r \geq (p+1)/2$). On the other hand, if $\|\mathbf{c}^+\| = \|\mathbf{c}^-\| = \frac{1}{2}\|\mathbf{c}\|$, then,

$$\deg \sigma^+ \;=\; \|\mathbf{c}^+\| \;=\; \|\mathbf{c}^-\| \;= \deg\, \sigma^- \;\leq r-1\,,$$

in which case (13) implies the equality $\sigma^+(x) = \sigma^-(x)$. However, since the supports of $\mathbf{c}^+$ and $\mathbf{c}^-$ are disjoint, the polynomials $\sigma^+(x)$ and $\sigma^-(x)$ are relatively prime. Therefore, we must have $\sigma^+(x) = \sigma^-(x) = 1$, yielding $\mathbf{c} = \mathbf{0}$. □

We end this section by exhibiting the near-optimality of the primitive codes $C(p^m-1, r; p)$ for sufficiently small values of r.

Lemma 2. (Sphere-packing bound, Golomb and Welch [5],[6]). *A code over $GF(p)$ of length n, size p^k, and minimum Lee distance $\geq 2r-1$ for some $r \leq (p+1)/2$ must satisfy the inequality*

$$\sum_{i=0}^{r-1} 2^i \binom{n}{i} \binom{r-1}{i} \;\leq\; p^{n-k} \,. \tag{14}$$

Theorem 2. *A code over $GF(p)$ of length n, size p^k, and minimum Lee distance $\geq 2r-1$ for some $r \leq (p+1)/2$ must satisfy the inequality*

$$(r-1)\Big(\log_p(n-r+2) - \log_p(r-1)\Big) \;\leq\; n-k \,.$$

Proof. By Lemma 2 we have

$$\frac{(n-r+2)^{r-1}}{(r-1)^{r-1}} \cdot 2^{r-1} \;\leq\; p^{n-k} \,.$$

The theorem now follows by taking the logarithm to base p of both sides of the latter inequality. □

Return now to the code $C(p^m-1, r; p)$ where, for $r \leq (p-1)/2$, we have $d_{\mathcal{L}}(p^m-1, r; p) \geq 2r-1$, thus conforming to the definition of r in Theorem 2. It is easy to verify that the lower bound of Theorem 2 on the redundancy $n-k$ approaches the upper bound on $n-k$ given in (3) when $\log_p r$ is much smaller than $m = \log_p(n+1)$. This would be the case when, for instance, we keep p, and therefore the range of r, fixed and let $n = p^m - 1$ go to infinity.

4 Lower bounds for the base-field case

Among the finite-field codes $C(n, r, \boldsymbol{\alpha}; p)$, the base-field codes are of some special interest in that they allow us to obtain bounds on the integer codes $C(n, r, \boldsymbol{\alpha})$ as well. In particular,

for any code $C(n, r, \boldsymbol{\alpha})$ with $\boldsymbol{\alpha} = [\,\alpha_1\,\alpha_2\,\ldots\,\alpha_n\,]$, $0 < \alpha_1 < \alpha_2 < \ldots < \alpha_n$, and for every prime $p > \alpha_n \geq n$, we have $d_{\mathcal{L}}(n, r, \boldsymbol{\alpha}) \geq d_{\mathcal{L}}(n, r, \boldsymbol{\alpha}; p)$. This is due to the fact that any nonzero codeword $\mathbf{c} \in C(n, r, \boldsymbol{\alpha})$ of minimum Lee weight must have at least one entry which is not divisible by p, and reducing such a codeword modulo p results in a nonzero codeword of $C(n, r, \boldsymbol{\alpha}; p)$ whose Lee weight is at most $\|\mathbf{c}\|$. Hence, any lower bound on $d_{\mathcal{L}}(n, r, \boldsymbol{\alpha}; p)$ implies one for $d_{\mathcal{L}}(n, r, \boldsymbol{\alpha})$. The converse, of course, is not necessarily true.

Example 2. The code $C(4, 3)$ consists of all integer vectors $\mathbf{c} \in \mathcal{Z}^4$ which satisfy the equality $H\,\mathbf{c} = \mathbf{0}$, where

$$H = H(4, 3, [\,1\,2\,3\,4\,]) \;=\; \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \\ 1 & 4 & 9 & 16 \end{bmatrix} .$$

It thus follows that $C(4, 3)$ consists of all integer multiples of the vector $[\,1\,{-3}\,3\,{-1}\,]$ and, therefore, $d_{\mathcal{L}}(4, 3, [\,1\,2\,3\,4]) = 8$. Taking each entry of every codeword of $C(4, 3)$ modulo 5, we obtain the base-field code $C(4, 3; 5)$, whose minimum Lee distance is 6. •

4.1 Extending the $2r$ lower bound for the base-field case

As we pointed out in Section 3, the $2r$ lower bound does not hold in general for all values of r for any code $C(n, r, \boldsymbol{\alpha}; p)$; however, it does hold for all r in the base-field case $n \leq p - 1$. We remark that for fairly large values of r, say, $r \geq (p + 1)/2$, we believe that the true value of $d_{\mathcal{L}}(n, r, \boldsymbol{\alpha}; p)$ is much greater than $2r$. Our conjecture is based on the lower bounds on $d_{\mathcal{L}}(n, r, \boldsymbol{\alpha}; p)$ given in the next subsection, where we show that in the high-redundancy range, the lower bound on $d_{\mathcal{L}}(n, r, \boldsymbol{\alpha}; p)$ becomes quadratic, rather than linear, in r. Still, $2r$ is the best lower bound we have for values of r up to around $\frac{6}{7}p$. Furthermore, although we present a substantial improvement on the $2r$ lower bound for the high-redundancy range, we have yet to find an efficient way to decode the number of correctable errors guaranteed by that bound.

The $2r$ lower bound for the base-field case takes the following form.

Theorem 3. *For $r \leq n \leq p - 1$,*

$$d_{\mathcal{L}}(n, r, \boldsymbol{\alpha}; p) \;\geq\; 2r \;.$$

Proof. Throughout the proof we assume that $r \geq (p+1)/2$, as the range of smaller r is covered by Theorem 1. Following the notations and line of proof of Theorem 1, by (11) we have $\|\mathbf{c}^+\| = \|\mathbf{c}^-\| \pm \ell \cdot p$ for some integer ℓ. The case $\ell = 0$ yields the desired $2r$ lower bound also when $r \geq (p+1)/2$, the same way it did in the proof of Theorem 1. Also, when $|\ell| \geq 2$ we have $\|\mathbf{c}\| = \|\mathbf{c}^+\| + \|\mathbf{c}^-\| \geq 2p > 2r$ and so we are done. Hence, it remains to consider the case $\ell = \pm 1$. Thus, we assume that $\ell = 1$ (or else apply the proof on $-\mathbf{c}$), $\deg \sigma^- = s$, and $\deg \sigma^+ = p + s$ with $p + 2s < 2r$, and we wish to show that $\mathbf{c} = \mathbf{0}$.

Define the *locator ratio* $\rho(x)$ by

$$\rho(x) \ \triangleq \ \frac{\sigma^+(x)}{\sigma^-(x)} \ .$$

A similar ratio will play in the decoding algorithm of Section 5 the role of the error-locator polynomial used in the Hamming-metric BCH decoding algorithm. Since $\sigma^-(0) \neq 0$, we can write $\rho(x)$ also as an infinite formal series $\rho(x) = 1 + \sum_{i=1}^{\infty} \rho_i x^i$. Noting that (12), and therefore (13), still hold, we have,

$$\sigma^+(x) \ = \ \sigma^-(x) \ + \ x^r \tau(x) \ ,$$

where $\deg \tau = p + s - r \leq p + 2s - r < r$. Hence,

$$\rho(x) \ = \ 1 + \sum_{i=1}^{\infty} \rho_i x^i \ = \ 1 + x^r \, \frac{\tau(x)}{\sigma^-(x)} \ , \tag{15}$$

implying that $\rho_i = 0$ for $1 \leq i \leq r-1$, or that

$$\rho(x) \ \equiv \ 1 \pmod{x^r} \ . \tag{16}$$

Our next step is to show that $\rho_i = 0$ also for $i = p-1$ and $p+1 \leq i \leq 2r-1$.

Newton's identities for $S^+(x)$ and $S^-(x)$ take the form

$$\sigma^+(x) \, S^+(x) \ + \ x \left(\sigma^+(x)\right)' \ = \ 0 \tag{17}$$

and

$$\sigma^-(x) \, S^-(x) \ + \ x \left(\sigma^-(x)\right)' \ = \ 0 \ . \tag{18}$$

Now, multiply (17) by $\sigma^-(x)$ and (18) by $\sigma^+(x)$, and subtract one from the other to obtain

$$\sigma^+(x)\sigma^-(x)\Big(S^+(x) - S^-(x)\Big) \ + \ x \left[\sigma^-(x)\Big(\sigma^+(x)\Big)' \ - \ \sigma^+(x)\Big(\sigma^-(x)\Big)'\right] \ = \ 0 \ . \tag{19}$$

Let $S(x) = \sum_{\ell=1}^{\infty} S_\ell x^\ell$ denote the difference $S^+(x) - S^-(x)$ and let $S_0 \triangleq S_0^+ - S_0^-$. Using this notation, we can rewrite (19) as

$$\rho(x)\, S(x) \;+\; x\, \rho'(x) \;=\; 0\;. \tag{20}$$

In addition, by (12) we have $S(x) \equiv 0 \pmod{x^r}$ which, with (16), yields

$$\rho(x)\, S(x) \;\equiv\; S(x) \pmod{x^{2r}}$$

and, therefore, by (20),

$$S(x) \;+\; x\, \rho'(x) \;\equiv\; 0 \pmod{x^{2r}}\;. \tag{21}$$

We now make use of the fact that the code is a base-field code. In this case we have $\alpha_j^{p-1} = 1$ and, therefore,

$$S^{\pm}_{\ell+p-1} = \sum_{j=1}^{n} c_j^{\pm} \alpha_j^{\ell+p-1} = \sum_{j=1}^{n} c_j^{\pm} \alpha_j^{\ell} = S_\ell^{\pm}$$

i.e., the sequences $\{S_\ell^{\pm}\}_{\ell=0}^{\infty}$, and, therefore, $\{S_\ell\}_{\ell=0}^{\infty}$, have period $p-1$. In particular, this implies that $S_\ell = 0$ for $p-1 \le \ell \le p+r-2$, which, with (21), leads to

$$i\, \rho_i \;=\; 0 \quad \text{for} \quad p-1 \le i \le 2r-1\;,$$

or,

$$\rho_i \;=\; 0 \quad \text{for} \quad i = p-1 \quad \text{and} \quad p+1 \le i \le 2r-1\;, \tag{22}$$

as desired.

Let $\eta(x)$ be the polynomial of degree $\le r-1$ defined by

$$\eta(x) \;\equiv\; \frac{\tau(x)}{\sigma^-(x)} \pmod{x^r}\;.$$

Comparing with (15) we have $\eta(x) = \sum_{i=0}^{r-1} \rho_{i+r} x^i$ and, therefore, by (22), $\deg \eta \le p-r$. We now use this bound on $\deg \eta$ to show that $\sigma^-(x) = 1$.

By definition of $\eta(x)$ we have

$$\sigma^-(x)\, \eta(x) \;\equiv\; \tau(x) \pmod{x^r}\;. \tag{23}$$

Now,

$$\deg \sigma^- \;+\; \deg \eta \;\le\; s + (p-r) \;\le\; p + 2s - r \;<\; r\;,$$

and, as pointed out before, the same upper bound applies to $\deg \tau$. Hence, (23) can be rewritten simply as

$$\sigma^-(x)\,\eta(x) \;=\; \tau(x)\;. \tag{24}$$

However, since σ^+ and σ^- are relatively prime, so are τ and σ^-. Therefore, by (24) we conclude that σ^- is constant i.e., $\sigma^-(x) = 1$ and $\eta(x) = \tau(x)$.

At this point we have established that $S^-(x) = 0$; therefore, $S^+(x) = S(x)$ and $\sigma^+(x) = \rho(x)$ with $\deg \sigma^+ = p + s = p$. Equation (21) thus reads

$$S^+(x) \;+\; x\left(\sigma^+(x)\right)' \;\equiv\; 0 \pmod{x^{2r}}\;. \tag{25}$$

Now, if $S^+(x) = 0$, we are done. Otherwise, let t be the smallest integer ℓ such that $S^+_\ell \neq 0$. Hence, by periodicity we have $S^+_{p-1} = S^+_p = \ldots = S^+_{p+t-2} = 0$, and (25) becomes

$$S^+(x) \;+\; x\left(\sigma^+(x)\right)' \;\equiv\; 0 \pmod{x^{p+t-1}} \tag{26}$$

which, with (17), yields

$$\sigma^+(x)\,S^+(x) \;\equiv\; S^+(x) \pmod{x^{p+t-1}}\;.$$

However, we assume that $S^+(x) \not\equiv 0 \pmod{x^{t+1}}$, thus forcing the congruence $\sigma^+(x) \equiv 1 \pmod{x^{p-1}}$. Recalling that $\sigma^+_{p-1} = \rho_{p-1} = 0$, this leaves us with $\sigma^+(x) = 1 + \sigma^+_p x^p = (1 + \sigma^+_p x)^p$. But this is absurd, since the multiplicity of a root in $\sigma^+(x)$ cannot be greater than $(p-1)/2$. Therefore, $S^+(x)$ cannot have a nonzero coefficient S^+_t, implying that $S(x) = S^+(x) = S^-(x) = 0$. □

4.2 The low-dimension case

We turn now to improve the $2r$ lower bound for base-field codes in the low-dimension range. Since each base-field code $C(n, r, \boldsymbol{\alpha}; p)$ is a shortened code of $C(p-1, r; p)$, it suffices to consider only the primitive base-field case, bearing in mind that for $n \leq p-1$, $d_{\mathcal{L}}(n, r, \boldsymbol{\alpha}; p) \geq d_{\mathcal{L}}(p-1, r; p)$.

Theorem 4.

$$d_{\mathcal{L}}(p-1, p-1-k; p) \;\geq\; \frac{p^2 - k^2}{4k}\;.$$

Proof. The proof is based on the fact that, up to permutation of coordinates, each nonzero codeword $\mathbf{c} \in C(p-1, p-1-k; p)$ has the form

$$\mathbf{c} \;=\; [\, u_1\, u_2\, \ldots\, u_n\,]\, G(p-1, p-1-k; p) \;=\; [\, u(1)\; u(2)\; \ldots\; u(p-1)\,]$$

for some nonzero polynomial $u(x) = u_1 x + u_2 x^2 + \cdots + u_k x^k$ over $GF(p)$. Now, since $u(x)$ is of degree $\leq k$, the function $x \mapsto u(x)$, defined over $GF(p)$, may take the same value of $GF(p)$ at most k times. Hence, an element of $GF(p)$ may appear with multiplicity at most k in $\mathbf{c}$; furthermore, since $u(0) = 0$, the zero element may appear in $\mathbf{c}$ with multiplicity not greater than $k-1$. Let $M \triangleq \lfloor (p-k)/(2k) \rfloor$ and $N \triangleq p - k - 2kM$; that is, N is the remainder of dividing $p-k$ by $2k$. We now construct a 'worst-case' word $\mathbf{a} \in GF(p)^{p-1}$ with $\|\mathbf{c}\| \geq \|\mathbf{a}\|$ in the following manner: The zero element appears in $\mathbf{a}$ with multiplicity $k-1$; each one of the $2M$ elements $\pm 1, \pm 2, \ldots, \pm M$ appears with multiplicity k; and the remaining N coordinates, if any, are filled with $\pm(M+1)$. Clearly, the Lee weight of $\mathbf{a}$ under-estimates the Lee weight of any nonzero $\mathbf{c} \in C(p-1, p-1-k; p)$. Now,

$$\|\mathbf{a}\| \;\geq\; 2k \sum_{i=1}^{M} i \;+\; N(M+1) \;=\; kM(M+1) + N(M+1) \;=\; (kM+N)(M+1)\,.$$

Let $\mu \triangleq (p-k)/(2k)$ and $\gamma \triangleq N/(2k)$. Then, $M = \mu - \gamma$ and

$$\begin{aligned} \|\mathbf{a}\| \;&\geq\; \Big(k(\mu-\gamma) + 2k\gamma\Big)(\mu - \gamma + 1) \;=\; k(\mu+\gamma)(\mu-\gamma+1) \\ &=\; k(\mu^2 - \gamma^2 + \mu + \gamma) \;\geq\; k\mu(\mu+1)\,, \end{aligned}$$

where the last inequality follows from γ being smaller than 1. Substituting $\mu = (p-k)/(2k)$ we obtain,

$$d_{\mathcal{L}}(p-1, p-1-k; p) \;\geq\; \|\mathbf{a}\| \;\geq\; k \cdot \frac{p-k}{2k} \cdot \frac{p+k}{2k} \;=\; \frac{p^2-k^2}{4k}\,,$$

as claimed. □

Note that the lower bound of Theorem 4 is tight for $k = 1$: the entries of any nonzero codeword in $C(p-1, p-2; p)$ exhaust all nonzero elements of $GF(p)$ and, therefore, the minimum Lee distance of $C(p-1, p-2; p)$ is

$$d_{\mathcal{L}}(p-1, p-2; p) \;=\; 2 \sum_{j=1}^{(p-1)/2} j \;=\; \frac{p^2-1}{4}\,.$$

Substituting $k = p - 1 - r$ in Theorem 4 we obtain the following bound which holds for the nonprimitive base-field case as well.

Corollary 1. *For $n \leq p - 1$,*

$$d_{\mathcal{L}}(n, r, \boldsymbol{\alpha}; p) \;\geq\; \frac{r+1}{2} \;+\; \frac{(r+1)^2}{4(p-1-r)} \,.$$

It is easy to check that the bound of Corollary 1 supersedes the $2r$ lower bound for $r \geq \frac{6}{7}p$. Furthermore, when $r = p - O(1)$, the lower bound of Corollary 1 becomes quadratic in r.

The following theorem, due to Mazur [19], improves on Corollary 1 for the *very* low dimension case.

Theorem 5. (Mazur [19]).

$$d_{\mathcal{L}}(p-1, p-1-k; p) \;\geq\; \frac{p^2-1}{4} \;-\; \frac{1}{4}\,(k-1)\cdot p^{3/2} \,.$$

In particular, Theorem 5 yields a quadratic lower bound for $r = p - O(\sqrt{p})$. The proof of Theorem 5 makes use of Weil's Theorem for character sums. While in the proof of Theorem 4 we under-estimated $d_{\mathcal{L}}(p-1, p-1-k; p)$ by the Lee weight of some worst-case word, Weil's Theorem is used to show that, in fact, $C(p-1, p-1-k; p)$ cannot have such worst-case codewords: For sufficiently small k, elements of $GF(p)$ with small Lee values cannot appear with too-large multiplicity in any nonzero codeword of $C(p-1, p-1-k; p)$.

5 Decoding algorithm

In this section, we present a decoding procedure for $C(n, r, \boldsymbol{\alpha}; p)$, based upon Euclid's algorithm, that will correct all errors up to Lee weight $r - 1$ and detect all errors of Lee weight r whenever the $2r$ lower bound applies (that is, when $r \leq (p-1)/2$ or when $r \leq n \leq p - 1$). It is straightforward to adapt this algorithm to the integer codes $C(n, r, \boldsymbol{\alpha})$.

We first establish some notation. Let $\mathbf{c} = [\, c_1\, c_2\, \ldots\, c_n\,]$ denote the 'transmitted' codeword and $\mathbf{y} = [\, y_1\, y_2\, \ldots\, y_n\,]$ denote the 'received' word, with the error vector given by

$\mathbf{e} = [\, e_1\, e_2\, \ldots\, e_n\,] \triangleq \mathbf{y} - \mathbf{c}$. The corresponding 'positive' error vector $\mathbf{e}^+ = [\, e_1^+\, e_2^+\, \ldots\, e_n^+\,]$, is defined by setting $e_j^+ = e_j$ if $e_j \in \{0, 1, \ldots, (p-1)/2\}$ and $e_j^+ = 0$ otherwise. Similarly, we define the 'negative' error vector $\mathbf{e}^- = [\, e_1^-\, e_2^-\, \ldots\, e_n^-\,]$, with $e_j^- = |e_j|$ if $e_j \in \{(p+1)/2, (p+3)/2, \ldots, p-1\}$ and $e_j^- = 0$ otherwise. The error vector can then be decomposed as $\mathbf{e} = \mathbf{e}^+ - \mathbf{e}^-$.

Given a locator vector $\boldsymbol{\alpha} = [\, \alpha_1\, \alpha_2\, \ldots\, \alpha_n\,]$, over $GF(p^m)$, we define the syndrome values S_ℓ of an error vector $\mathbf{e} = [\, e_1\, e_2\, \ldots\, e_n\,]$ in the standard way,

$$S_\ell = \sum_{j=1}^{n} e_j \alpha_j^\ell \,, \qquad 0 \le \ell < \infty \,.$$

The formal syndrome series $S(x)$ is then defined as

$$S(x) = \sum_{\ell=1}^{\infty} S_\ell x^\ell \,.$$

(Note that the constant term corresponding to S_0 is excluded from $S(x)$.)

When the transmitted word $\mathbf{c}$ belongs to $C(n, r, \boldsymbol{\alpha}; p)$, the first r syndrome values S_ℓ can be determined from the received vector $\mathbf{y}$. Specifically,

$$S_\ell \;=\; \sum_{j=1}^{n} e_j \alpha_j^\ell \;=\; \sum_{j=1}^{n} y_j \alpha_j^\ell \,, \qquad 0 \le \ell < r \,.$$

Therefore, when $\mathbf{c} \in C(n, r, \boldsymbol{\alpha}; p)$, the formal syndrome series $S(x)$ is in effect known modulo x^r.

It will be convenient to define the positive syndrome values S_ℓ^+ and the negative syndrome values S_ℓ^- of the error vector $\mathbf{e}$ by

$$S_\ell^+ \;=\; \sum_{j=1}^{n} e_j^+ \alpha_j^\ell \qquad \text{and} \qquad S_\ell^- \;=\; \sum_{j=1}^{n} e_j^- \alpha_j^\ell \,, \qquad 0 \le \ell < \infty \,,$$

with the associated formal syndrome series

$$S^+(x) \;=\; \sum_{\ell=1}^{\infty} S_\ell^+ x^\ell \qquad \text{and} \qquad S^-(x) \;=\; \sum_{\ell=1}^{\infty} S_\ell^- x^\ell \,.$$

Similarly, we define the positive and negative error-locator polynomials $\sigma^+(x)$ and $\sigma^-(x)$ by

$$\sigma^+(x) \;=\; \prod_{j=1}^{n} (1 - \alpha_j x)^{e_j^+} \qquad \text{and} \qquad \sigma^-(x) \;=\; \prod_{j=1}^{n} (1 - \alpha_j x)^{e_j^-} \,.$$

Note that, by definition, $S^+(x)$ and $S^-(x)$ are the formal power-sum series associated with $\sigma^+(x)$ and $\sigma^-(x)$, respectively.

Finally, as in Subsection 4.1, we introduce the error-locator ratio,

$$\rho(x) \;=\; 1 + \sum_{i=1}^{\infty} \rho_i x^i \;=\; \frac{\sigma^+(x)}{\sigma^-(x)} \; .$$

Recalling that the formal syndrome series $S(x)$ is equal to $S^+(x) - S^-(x)$, we can apply Newton's identities to $S^+(x)$ and $S^-(x)$, as in Equations (17)–(20), to obtain the following relation between the error-locator ratio $\rho(x)$ and the formal syndrome series $S(x)$:

$$\rho(x)\, S(x) \;+\; x\, \rho'(x) \;=\; 0 \; . \tag{27}$$

Let $\phi(x)$ be the polynomial over $GF(p^m)$ defined by $\phi(x) = 1 + \sum_{i=1}^{r-1} \rho_i x^i$; that is, $\phi(x)$ is the unique polynomial of degree less than r satisfying

$$\phi(x) \;\equiv\; \rho(x) \pmod{x^r} \; .$$

From (27) we obtain

$$\phi(x)\, S(x) \;+\; x\, \phi'(x) \;\equiv\; 0 \pmod{x^r} \; , \tag{28}$$

which, in turn, can be rewritten explicitly as

$$S_i \;+\; \sum_{\ell=1}^{i-1} \rho_\ell\, S_{i-\ell} \;+\; i\, \rho_i \;=\; 0 \; , \qquad 1 \le i < r \; . \tag{29}$$

Knowing the syndrome values $S_1, S_2, \ldots, S_{r-1}$ from the received word $\mathbf{y}$, and noting that, for $r \le p$, the index i in (29) ranges over invertible integers modulo p, we can apply Equation (29) iteratively to solve (uniquely) for the values ρ_i for $i = 1, 2, \ldots, r-1$. Furthermore, the mapping $[\, S_1\, S_2\, \ldots\, S_{r-1}\,] \mapsto [\, \rho_1\, \rho_2\, \ldots\, \rho_{r-1}\,]$, induced by (29), is one-to-one. Hence, when the $2r$ lower bound applies, distinct error vectors $\mathbf{e}$ of Lee weight smaller than r correspond to distinct syndrome vectors $[\, S_0\, S_1\, S_2\, \ldots\, S_{r-1}\,]$ and, therefore, to distinct pairs $(S_0, \phi(x))$.

The following theorem summarizes a few properties of the error-locator polynomials $\sigma^+(x)$ and $\sigma^-(x)$. Recall that $\overline{S_0}$ stands for the smallest nonnegative integer such that $S_0 = \overline{S_0} \cdot 1$ over $GF(p)$.

Theorem 6. *Given a code $C(n, r, \boldsymbol{\alpha}; p)$ and an error vector $\mathbf{e}$ of Lee weight smaller than r, let $\sigma^+(x)$ and $\sigma^-(x)$ be the positive and negative error-locator polynomials, respectively, associated with $\mathbf{e}$, and let $\phi(x)$ be the polynomial defined by (28) for the syndrome vector $[\, S_0\, S_1\, \ldots\, S_{r-1}\,]^T = H(n, r, \boldsymbol{\alpha}; p)\, \mathbf{e}$. Then,*

$$\begin{aligned} &\textit{(i)} && \sigma^-(x)\,\phi(x) \;\equiv\; \sigma^+(x) \pmod{x^r}\;; \\ &\textit{(ii)} && \deg\sigma^+ \;+\; \deg\sigma^- \;<\; r\;; \\ &\textit{(iii)} && \gcd(\sigma^+, \sigma^-) \;=\; 1\;; \\ &\textit{and —} && \\ &\textit{(iv)} && \deg\sigma^+ \;-\; \deg\sigma^- \;\equiv\; \overline{S_0} \pmod{p}\;. \end{aligned}$$

Properties (i)–(iv) will serve as the 'key equations' for our decoding algorithm. We now aim at stating a result which is somewhat of a converse to Theorem 6 and which will allow us to use these key equations to compute the error-locator polynomials $\sigma^+(x)$ and $\sigma^-(x)$ in an efficient way by application of Euclid's algorithm. Euclid's algorithm has also been used to decode BCH codes and Goppa codes in the Hamming metric, as described in [16, Ch. 12],[20, Ch. 8]. For the sake of completeness, we now review certain properties of Euclid's algorithm that are also relevant to our decoding problem.

Let $A(x)$ and $B(x)$ be nonzero polynomials over a field F. Define the polynomials $R_i(x)$ and $Q_i(x)$ as the intermediate remainders and quotients while executing Euclid's algorithm to determine the greatest common divisor of $A(x)$ and $B(x)$. That is, $R_{-1}(x) \triangleq A(x)$, $R_0(x) \triangleq B(x)$, and, for $i \geq 1$, $Q_i(x)$ and $R_i(x)$ are the quotient and remainder, respectively, when $R_{i-2}(x)$ is divided by $R_{i-1}(x)$. Note that for $i \geq 0$, $\deg R_i$ strictly decreases with i, until we reach the largest index $i_{\max}$ for which $R_i(x) \neq 0$. At that point, $R_{i_{\max}}(x) = \gcd(A(x), B(x))$.

We shall also need the auxiliary polynomials $T_i(x)$ which are defined as follows: $T_{-1}(x) \triangleq 0$, $T_0(x) \triangleq 1$, and, for $1 \leq i \leq i_{\max}$,

$$T_i(x) \;\triangleq\; T_{i-2}(x) - Q_i(x) T_{i-1}(x)\;.$$

The next two lemmas summarize properties of Euclid's algorithm that we shall need in the sequel.

Lemma 3. [20, p. 177]. *Suppose that $T(x)$ and $R(x)$ are nonzero polynomials satisfying the following three conditions:*

$$\begin{aligned} &\textit{(i)} \quad T(x)\,B(x) \;\equiv\; R(x) \pmod{A(x)}\,; \\ &\textit{(ii)} \quad \deg T \;+\; \deg R \;<\; \deg A\,; \\ &\textit{(iii)} \quad \gcd(T,R) \;=\; 1\,. \end{aligned}$$

Then, there exist a unique index s, $0 \le s \le i_{\max}$, and a constant $c \neq 0$ such that $T(x) = c \cdot T_s(x)$ and $R(x) = c \cdot R_s(x)$.

Lemma 4. [20, p. 176, Table 8.2]. *For $0 \le i \le i_{\max}$,*

$$\deg T_i + \deg R_{i-1} = \deg A$$

and, therefore, for that range of i, $\deg R_i - \deg T_i$ strictly decreases with i.

The following converse to Theorem 6 provides the foundation for the decoding algorithm for the case $r \le (p-1)/2$.

Theorem 7. *Given a code $C(n, r, \boldsymbol{\alpha}; p)$ with $r \le (p-1)/2$ and with $\boldsymbol{\alpha}$ over $GF(p^m)$, let $\mathbf{e}$ be an error vector of Lee weight smaller than r and let S_0 and $\phi(x)$ be as in Theorem 6.*

(a) There is a unique (up to scalar normalization) pair of polynomials $\sigma^+(x)$ and $\sigma^-(x)$ over $GF(p^m)$ which satisfy properties (i)–(iv) of Theorem 6.

(b) With the proper scaling, the polynomials in (a) are the positive and negative error-locator polynomials, respectively, associated with $\mathbf{e}$.

(c) The polynomials $\sigma^+(x)$ and $\sigma^-(x)$ are given by

$$\sigma^+(x) = c \cdot R_s(x) \quad \text{and} \quad \sigma^-(x) = c \cdot T_s(x)\,,$$

where $R_i(x)$ and $T_i(x)$ are obtained from the application of Euclid's algorithm to the polynomials $A(x) = x^r$ and $B(x) = \phi(x)$, and s is the unique index i for which

$$\deg R_s - \deg T_s \;=\; \begin{cases} \overline{S_0} & \text{if } \; 0 \le \overline{S_0} < r \\ \overline{S_0} - p & \text{if } \; p - r < \overline{S_0} \le p-1 \end{cases}\,. \tag{30}$$

Proof. Let $\sigma^+(x)$ and $\sigma^-(x)$ be a pair of polynomials over $GF(p^m)$ that satisfy properties (i)–(iv) of Theorem 6. If we set $A(x) = x^r$, $B(x) = \phi(x)$, $R(x) = \sigma^+(x)$, and $T(x) = \sigma^-(x)$, then the three properties (i)–(iii) of Theorem 6 coincide with the three conditions (i)–(iii) of Lemma 3. Therefore, there exist a unique index i and a constant $c \neq 0$ such that $\sigma^+(x) = c \cdot R_i(x)$ and $\sigma^-(x) = c \cdot T_i(x)$. Now, since $r \leq (p-1)/2$, properties (ii) and (iv) of Theorem 6 imply the equality

$$\deg \sigma^+ - \deg \sigma^- \;=\; \deg R_i - \deg T_i \;=\; \begin{cases} \overline{S_0} & \text{if } \; 0 \leq \overline{S_0} < r \\ \overline{S_0} - p & \text{if } \; p - r < \overline{S_0} \leq p-1 \end{cases}$$

which, with Lemma 4, leaves only one possible value for i. This proves parts (a) and (c) of the theorem. Part (b) is now a consequence of Theorem 6. □

Note that when $r \leq (p-1)/2$, there is a nonempty range of values of $\overline{S_0}$, namely, $r \leq \overline{S_0} \leq p-r$, which corresponds to detectable but uncorrectable error patterns. Uncorrectable errors are detected also when the unique polynomials $\sigma^+(x)$ and $\sigma^-(x)$, if any, obtained by Theorem 7(c), violate the degree property (ii) of Theorem 6, or when these polynomials do not factor into linear terms $1 - \alpha_j x$ for elements α_j in the locator vector $\boldsymbol{\alpha}$. Uncorrectable errors will always be detected when the Lee weight of the error vector is exactly r.

It is worth pointing out that when r is much smaller than $(p-1)/2$, and $p-r < \overline{S_0} \leq p-1$, there is an algorithmic shortcut to Theorem 7(c): re-compute the polynomial $\phi(x)$ associated with the negated syndrome values $-S_1, -S_2, \ldots, -S_{r-1}$, then apply the stopping rule

$$\deg R_s - \deg T_s \;=\; |S_0| \;,$$

in lieu of (30), and, finally, set the error-locator polynomials to

$$\sigma^+(x) = c \cdot T_s(x) \quad \text{and} \quad \sigma^-(x) = c \cdot R_s(x) \;.$$

This corresponds to applying Theorem 7 on $-\mathbf{e}$, that is, on a negated copy of the received word $\mathbf{y}$.

Having determined the error-locator polynomials $\sigma^+(x)$ and $\sigma^-(x)$ by Theorem 7(c), we can now solve for the error vector $\mathbf{e} = [\, e_1 \, e_2 \, \ldots \, e_n \,]$ using the following modified Chien search (compare with [2, Algorithm 9.36]). For $j = 1, 2, \ldots, n$ we set $e_j = a$ (respectively, $e_j = -a$), where $\overline{a}$ is the smallest integer $i \geq 0$ for which the ith order formal derivative

$$\Big(\sigma^+(x)\Big)^{(i)} \;=\; \sum_{\ell \geq i} \ell(\ell-1)\cdots(\ell-i+1)\,\sigma_\ell^+ x^{\ell-i}$$

of $\sigma^+(x)$ (respectively, of $\sigma^-(x)$) does not vanish at $x = \alpha_j^{-1}$. (Since we expect to have multiplicities not greater than $(p-1)/2$ in the correct error-locator polynomials, the above test, using formal derivatives, does indeed provide the correct multiplicity. See [15, pp. 303–305].)

We now turn to the base-field case and the range $r \geq (p+1)/2$. The complication in this case arises from the fact that the stopping rule (30) might become ambiguous. In fact, part (a) of Theorem 7 no longer holds.

We illustrate this in the following example.

Example 3. Consider the code $C(p-1, r; p)$ with $p = 7$, $r = 5$, and $\alpha_1 = 1$ and assume $\mathbf{e} = [\,4\,0\,0\,0\,0\,0]$. Then, $S_\ell = 4$ for $\ell = 0, 1, 2, 3, 4$, and $\phi(x) = 1 + 3x + 6x^2 + 3x^3 + x^4$. Now, stopping rule (30) in Theorem 7(c) is satisfied at $s = 0$, yielding

$$\sigma_1^+(x) = R_0(x) = 1 + 3x + 6x^2 + 3x^3 + x^4 = (1-x)^4 \qquad \text{and} \qquad \sigma_1^-(x) = T_0(x) = 1\ ,$$

and also at $s = 4$, yielding

$$\sigma_2^+(x) = 4 \cdot R_4(x) = 1 \qquad \text{and} \qquad \sigma_2^-(x) = 4 \cdot T_4(x) = 1 + 4x + 3x^2 + 6x^3 = (1-x)^3\ .$$

Both pairs of polynomials, (σ_1^+, σ_1^-) and (σ_2^+, σ_2^-), satisfy all four properties of Theorem 6. However, the multiplicity 4 of $1 - x$ in the decomposition of $\sigma_1^+(x)$ is not a valid Lee value. Disregarding this inconsistency, both pairs of error-locator polynomials correspond to the same true error vector. •

Theorem 7 for the base-field case takes the following form.

Theorem 8. *Given a base-field code $C(n, r, \boldsymbol{\alpha}; p)$, let $\mathbf{e}$ be an error vector of Lee weight smaller than r and let S_0 and $\phi(x)$ be as in Theorem 6.*

(a) There is a unique (up to scalar normalization) pair of polynomials $\sigma^+(x)$ and $\sigma^-(x)$ over $GF(p)$ which satisfy the following three conditions:

1. both polynomials factor into linear terms over $GF(p)$;

2. the multiplicity of each linear term in $\sigma^+(x)$ and $\sigma^-(x)$ is at most $(p-1)/2$;

3. the polynomials satisfy properties (i)–(iv) of Theorem 6.

(b) With the proper scaling, the polynomials in (a) are the positive and negative error-locator polynomials, respectively, associated with $\mathbf{e}$.

(c) The polynomials $\sigma^+(x)$ *and* $\sigma^-(x)$ *are obtained as in Theorem 7(c), except that the stopping rule (30) changes to*

$$\deg R_s - \deg T_s \in \left\{ \overline{S_0},\ \overline{S_0} - p \right\} ,$$

and the proper choice of s *is determined by criterions 1 and 2 in (a).*

If we determine the value of s in Theorem 8(c) according to criterion 1 only, we might get the ambiguity which was illustrated in Example 3, where both pairs of polynomials were associated, in principle, to the same true error vector.

Proof of Theorem 8. Let $\sigma^+(x)$ and $\sigma^-(x)$ be polynomials which satisfy the three conditions in (a). Then $\sigma^+(x)$ and $\sigma^-(x)$ serve as the positive and negative error-locator polynomials of some error vector $\hat{\mathbf{e}}$ whose Lee weight is smaller than r. (Indeed, it can be verified that by properties (i) and (iii) of Theorem 6, the term x cannot be one of the linear terms referred to in criterion 1 in (a).) By property (iv) of Theorem 6, both $\mathbf{e}$ and $\hat{\mathbf{e}}$ share the same first syndrome value S_0. Furthermore, the equation $\sigma^-(x)\hat{\phi}(x) \equiv \sigma^+(x) \pmod{x^r}$ defines a unique polynomial $\hat{\phi}(x)$ of degree smaller than r. Hence, $\mathbf{e}$ and $\hat{\mathbf{e}}$ share the same polynomial $\phi(x)$. Since the mapping $[\, S_0\, S_1\, S_2\, \ldots\, S_{r-1}\,] \mapsto (S_0, \phi(x))$ is one-to-one, we thus conclude that $\mathbf{e}$ and $\hat{\mathbf{e}}$ have the same syndrome vector and, as such, these two error vectors must be equal. This proves parts (a) and (b). Part (c) follows from Theorem 6 and Lemma 3. □

The following is an outline of the decoding algorithm for $C(n, r, \boldsymbol{\alpha}; p)$ with $\boldsymbol{\alpha} = [\, \alpha_1\, \alpha_2\, \ldots\, \alpha_n\,]$. The input to the algorithm is the received word $[\, y_1\, y_2\, \ldots\, y_n\,]$, and the algorithm produces the error vector $[\, e_1\, e_2\, \ldots\, e_n\,]$, or returns an 'uncorrectable error' flag.

1. Compute the syndrome values $S_\ell \leftarrow \sum_{j=1}^{n} y_j \alpha_j^\ell,\ 0 \le \ell < r$.
2. Compute the polynomial $\phi(x) = 1 + \sum_{i=1}^{r-1} \rho_i x^i$ using the recurrence

$$\rho_i \ \leftarrow\ -\frac{1}{i}\left(S_i \ +\ \sum_{\ell=1}^{i-1} \rho_\ell\, S_{i-\ell} \right) , \qquad 1 \le i < r\ .$$

3. Apply Euclid's algorithm to the polynomials $A(x) = x^r$ and $B(x) = \phi(x)$ to obtain pairs of polynomials (R_i, T_i), $i = 0, 1, 2, \ldots$, until $\deg R_i - \deg T_i \leq \overline{S_0} - p$.

4. For integers s for which $\deg R_s - \deg T_s \in \left\{\overline{S_0},\ \overline{S_0} - p\right\}$ and $\deg R_s + \deg T_s < r$ do:

   (a) let $\sigma^+(x) \leftarrow R_s(x)$ and $\sigma^-(x) \leftarrow T_s(x)$;

   (b) using formal derivatives find, for $j = 1, 2, \ldots, n$, the multiplicity e_j^+ of α_j^{-1} in $\sigma^+(x)$ and the multiplicity e_j^- of α_j^{-1} in $\sigma^-(x)$;

   (c) if $\sum_{j=1}^n e_j^+ = \deg \sigma^+$ and $\sum_{j=1}^n e_j^- = \deg \sigma^-$, set $e_j \leftarrow e_j^+ - e_j^-$.

5. If no such integers s exist, or if the values e_j were not set in step 4c, return an 'uncorrectable error' flag.

The decoding method we have just described for codes over $GF(p)$ is easily adapted for the integer codes $C(n, r, \boldsymbol{\alpha})$. In this case all operations will be carried out in the rational field, and we will have the stopping rule $\deg R_i - \deg T_i = S_0$ in Theorem 7(c).

6 Applications

In this section, we describe two applications involving the class of Lee-metric BCH codes. The first application uses the codes to efficiently protect against synchronization and so-called bitshift errors in runlength-limited (RLL) (d, k)-constrained channels.

The second application is to the algebraic decoding of spectral-null codes over the integer alphabet, including matched-spectral-null codes for partial-response channels with exponentially distributed noise.

6.1 Synchronization and bitshift error correction

In this section, we propose a new application of codes for the Lee-metric: detection and/or correction of certain types of errors in (d, k)-constrained channels commonly used in digital data recording [23],[8],[17]. Among known Lee-metric codes, Lee-metric BCH codes are particularly attractive for this application in light of the improved attainable codeword length

and simple algebraic decoding algorithm. The codes of [22] will have similar advantages when the application calls for use of Lee-metric codes over integer rings of size 2^h.

Digital magnetic and optical data recorders often make use of runlength-limited codes. These binary codes are characterized by two parameters (d, k), where d and k represent, respectively, the minimum and maximum number of contiguous 0's between consecutive 1's. For our purposes, it will be convenient to view a (d, k)-constrained sequence as a sequence of "runs," where a run is a symbol 1 along with the following contiguous symbols 0 prior to the next consecutive symbol 1. Associated to a run is a positive integer called the runlength, the number of symbols in the run. For example, the (1,7) sequence 10100000001000100(1) corresponds to the sequence of runs having runlengths 2, 8, 4, 3.

There are four predominant types of errors that may be encountered in a recording system. The first two types, sometimes referred to as drop-ins and drop-outs, involve the incorrect detection of a recorded 0 as a 1, or vice-versa. The third type of error is called a bitshift error, where a pair of recorded symbols 01 is detected as 10 (a left shift) or a pair 10 is detected as 01 (right shift). Finally, a less common error, but one with potentially catastrophic consequences in most recording systems, is a synchronization error, where a symbol 0 is inserted or deleted from a run.

Drop-in, drop-out, and bitshift errors in most digital recorders are propagated by the (d, k) decoder into burst errors (of length bounded from above by a fixed number depending on the particular modulation code and its design). The detection and correction of these bursts are typically addressed by the use of an outer algebraic error-correcting code, such as a Fire code or Reed-Solomon code. Recently, several authors have proposed schemes that combine the (d, k) constraints and limited error-correcting capability into a single code. In particular, Hilden, et al. [7] have proposed a class of shift-error-correcting modulation (SECM) codes that efficiently correct bitshift errors. Kuznetsov and Vinck [12],[13] also have constructed a class of codes suitable for correction of a single error which is either of the bitshift or synchronization type. To the best of our knowledge, all of the combined modulation/error-correction schemes so far have relied upon error-control techniques using the Hamming metric. Also, none have addressed the problem of correcting multiple bitshift and synchronization errors occurring simultaneously. We will now show that codes for the Lee-metric are well-suited for handling such combinations of bitshift and synchronization

errors. Crucial to the application of Lee-metric codes is the examination of the effect of these errors on runlengths in (d, k) sequences.

Let $\mathbf{s}$ be a (d, k)-constrained sequence with N runs and associated runlength sequence $\boldsymbol{\ell} = \ell_1, \ell_2, \ldots, \ell_N$.

We assume that one or more bitshift errors may occur at a boundary of runs: e left bitshift errors at the boundary between runs j and $j+1$ would induce a change in the runlength sequence to $\boldsymbol{\ell}^* = \ell_1, \ldots, \ell_j - e, \ell_{j+1} + e, \ldots, \ell_N$. Similarly, e right bitshift errors lead to the runlength sequence $\boldsymbol{\ell}^* = \ell_1, \ldots, \ell_j + e, \ell_{j+1} - e, \ldots, \ell_N$. By an *e-bitshift error* we refer to a pattern of e bitshift errors occurring at the same boundary of runs (without loss of generality we can also assume that all e errors are in the same direction — left or right).

In an analogous manner, we assume that one or more synchronization errors may occur within one run: insertion of e zeros in the jth run generates the runlength sequence $\boldsymbol{\ell}^* = \ell_1, \ldots, \ell_j + e, \ell_{j+1}, \ldots, \ell_N$, and the deletion of e zeros from run j produces $\boldsymbol{\ell}^* = \ell_1, \ldots, \ell_j - e, \ell_{j+1}, \ldots, \ell_N$. (Of course, e must not exceed ℓ_j.) An *e-synchronization error* refers to a pattern of e synchronization errors occurring at the same run. Clearly, a bitshift error can be interpreted as a pair of synchronization errors: an insertion error and a deletion error in consecutive runs.

The potential advantage of the Lee-metric perspective over the more traditional Hamming-metric perspective is that, roughly speaking, codes for the Hamming metric require two check symbols per (Hamming) error corrected, while Lee-metric codes require only one check symbol per (Lee) error corrected. In the presence of e-bitshift errors and e-synchronization errors with varying values of e, but with smaller values prevailing, the Lee-metric codes would be expected to show some advantages.

Given constraints (d, k), we choose $p \leq k-d+1$, and proceed as follows: We regard every run of length ℓ in the (d, k)-constrained information sequence as an element $(\ell - d - 1) \bmod p$ of $GF(p)$, and use a systematic encoder for $C(n, r, \boldsymbol{\alpha}; p)$ to compute the corresponding check symbols in $GF(p)$. Each check symbol a, in turn, is associated with a run of length $\overline{a} + d + 1$. The code $C(n, r, \boldsymbol{\alpha}; p)$, with $r \leq (p-1)/2$ and $n \leq p^m - 1$ can simultaneously correct b bitshift errors and s non-bitshift synchronization errors whenever $2b + s < r$ (observe that, when counting errors, an e-bitshift error is counted as e bitshift errors; this applies respectively

also to synchronization errors. Also, bitshift or synchronization errors may create runlengths that violate the (d, k)-constraint. In such a case we can mark the illegal runlength as an erasure rather than an error). The redundancy required will be no more than $1 + (r-1)m$ symbols from the alphabet $GF(p)$. Recall that Theorem 2 proves the near-optimality of the Lee-metric primitive BCH codes $C(p^m - 1, r; p)$, for values $r \ll p^m - 1$.

Example 4. Two typical choices for parameters (d, k) are $(1, 7)$ and $(2, 8)$, both satisfying $k - d + 1 = 7$. Setting $p = 7$ and $r = 3$, we obtain a family of codes for these constraints, based upon $C(n, 3, \boldsymbol{\alpha}; 7)$, that can correct any error pattern of Lee weight 2 (and detect error patterns of Lee weight 3). In particular, the codes will correct one single-bitshift (1-bitshift) error or any other combination of two insertions/deletions of symbols 0. For $n \leq p^m - 1$, the required redundancy is no more than $1 + 2m$ symbols. •

The class of SECM codes in [7] are directed toward the situation when only bitshift-type errors occur. We can modify the Lee-metric BCH codes to improve their efficiency in this type of error environment by means of a precoding operation, as follows.

Let $\mathbf{c} = [\, c_1\, c_2\, \ldots\, c_n\,]$ be a codeword, and construct the differentially precoded word $\mathbf{d} = [\, d_1\, d_2\, \ldots\, d_n\,]$ where $d_1 = c_1$, and $d_j = c_j - c_{j-1}$ for $2 \leq j \leq n$, with all operations taken modulo p. If $\mathbf{d}$ is recorded, and no bitshift errors occur, the original word $\mathbf{c}$ is reconstructed by an "integration" operation:

$$c_j \;=\; \sum_{l=1}^{j} d_l \;.$$

If, however, an e-bitshift error occurs at the boundary between runs j and $j+1$ of $\mathbf{d}$, the integration operation converts the error into an e-synchronization error in run j of $\mathbf{c}$. In other words, the original bitshift error pattern of Lee weight $2e$ is converted into a synchronization error pattern of Lee weight e.

This result is predicated upon the correctness of the first run d_1. In order to handle the event in which an uncorrectable bitshift error pattern has occurred at the boundary between the last run of the preceding word and the first run of the current word, it suffices to require that the code contain the all-one word $[\, 1\, 1\, \ldots\, 1\,]$ and all of its multiples. To see this, observe that any error in d_1 propagates into a constant offset in the components of $\mathbf{c}$ upon integration. This bias corresponds to a translation by a valid codeword, so the syndrome computation and subsequently the decoding of the integrated word is not affected.

We can guarantee that the all-one word and its multiples belong to the code $C(n, r, \boldsymbol{\alpha}; p)$ by imposing an additional constraint upon $\boldsymbol{\alpha}$: for example, the all-one word will be a codeword in $C(n, r, \boldsymbol{\alpha}; p)$ if the locator vector $\boldsymbol{\alpha}$ contains elements $\beta \in GF(p^m)$ along with all of their translates $\beta + t$ by elements $t \in GF(p)$.

This construction provides the capability to correct up to $r-1$ bitshift errors and detect up to r bitshift errors, when $2r < p \leq k - d + 1$. The construction extends to the base-field case as well, where an extra column $[\,1\,0\,\ldots\,0\,]^T$ needs to be added to the parity-check matrix, and r must be restricted to the range $r \leq (p-1)/2$ in order for the $2r$ lower bound to apply. (See Remark 1: according to our convention of having only nonzero values in the locator vector $\boldsymbol{\alpha}$, the resulting code will not, in effect, be a base-field code, but rather a code $C(p, r, \boldsymbol{\alpha}; p)$ whose parity-check matrix is over $GF(p^2)$.)

Example 5. Let $p = 7$ and $r = 3$ as in the previous example. The construction above will generate codes with length n a multiple of 7. For $n = 7$, the redundancy is $1+(r-1) = 3$ runs; for $n = 14, 21, \ldots, 49$ the redundancy is $1 + 2(r-1) = 5$ runs; for $n = 56, 63, \ldots, 343$ the redundancy is $1 + 3(r-1) = 7$ runs. All of these codes will correct up to two single-bitshift errors or one double-bitshift (2-bitshift) error. By way of comparison, in [7] Hilden et al. describe SECM codes of lengths 26, 80, and 242 for correcting two single-bitshift errors, requiring redundancy of 7, 9, and 11 runs, respectively. These SECM codes do not handle double-bitshift errors. •

Example 6. As p increases, so does the discrepancy in the number of check symbols (runs) compared to the SECM codes in [7]. For $p = 11$, suitable for representing $(d, k) = (1, 11)$ for example, and $r = 5$, the Lee-metric BCH code with $n = 11$ requires 5 check symbols; for $n = 22, 33, \ldots, 121$, the redundancy is 9 symbols; for $n = 132, 143, \ldots, 1331$ the redundancy will be 13 symbols. These codes will correct up to four single-bitshift errors; two single-bitshift and one double-bitshift errors; or two double-bitshift errors. The codes presented in [7] for correcting up to four single-bitshift errors have lengths 26, 80, and 242 and require redundancy of 16, 21, and 26, respectively. •

So far we have exhibited the improvement on [7] in the number of check symbols per codeword for several examples of (d, k)-constrained channels and minimum-distance requirements. However, assuming a uniform distribution on each check symbol over $GF(p)$, the

improvement on [7] is reflected also in the *average redundancy length* (i.e., the sum of run-lengths of check symbols in a codeword, averaged over all codewords) for a wide range of parameters d, k, and r. Note that the uniformity assumption on the check symbols should hold for sufficiently long codes, even if the information symbols have some other, nonuniform stationary distribution (which will typically be the case in a well-designed (d, k)-encoder). Under the uniformity assumption, the average length of a run representing a check symbol will be $d + ((p+1)/2)$. Therefore, the average length, $\Lambda(n, r; p; d, k)$, of all check symbols in a codeword of $C(n, r, \boldsymbol{\alpha}; p)$ over a (d, k)-constrained channel is given by

$$\Lambda(n, r; p; d, k) \;=\; \left(d \;+\; \frac{p+1}{2}\right)\left(1 \;+\; (r-1)\left\lceil \frac{\log_2 n}{\log_2 p} \right\rceil\right) \;. \tag{31}$$

Returning to Example 5 we have, for the $(2, 8)$-constrained channel,

$$\Lambda(n, 3; 7; 2, 8) \;=\; O(1) \;+\; \tfrac{12}{\log_2 7}\, \log_2 n \;\approx\; O(1) \;+\; 4.27\, \log_2 n \;,$$

whereas a similar analysis for the construction in [7] yields average redundancy length $O(1) + \frac{8}{\log_2 3}\, \log_2 n \approx O(1) + 5.05\, \log_2 n$. The gain in length is not just asymptotic: extending the construction of [7] to shortened BCH codes over $GF(3)$ (to allow a denser range of lengths) shows that $\Lambda(n, 3; 7; 2, 8)$ turns out to be smaller for $28 \leq n \leq 343$. For the $(1, 7)$-constrained channel we have

$$\Lambda(n, 3; 7; 1, 7) \;=\; O(1) \;+\; \tfrac{10}{\log_2 7}\, \log_2 n \;\approx\; O(1) \;+\; 3.56\, \log_2 n \;,$$

whereas the construction in [7] has average redundancy length $O(1) + \frac{6}{\log_2 3}\, \log_2 n \approx O(1) + 3.79\, \log_2 n$. A similar redundancy gain exists also for the code described in Example 6.

We remark that, in general, the redundancy given in (31) can be shown to be 3/4 times the redundancy of the construction in [7] for sufficiently large d, k, and n, whenever $k < 2d$ or $r \ll d$. This is in addition to being able to deal with e-bitshift errors for $e > 1$ as well.

The preceding discussion illustrates some of the differences between Lee-metric codes and Hamming-metric codes aimed at correcting bitshift and synchronization errors. It should also be pointed out that SECM codes can be adapted to channels with 1-synchronization errors by means of a precoding operation, and the comparison with Lee-metric-based codes for synchronization error correction will follow similar lines to those in the examples above.

Finally, we note that drop-ins and drop-outs can be detected by an external means and, if desired, flagged for erasure decoding by an outer, burst-correcting code, as described in the context of SECM codes in [7].

6.2 Algebraic decoding of integer spectral-null codes

As was mentioned in Section 4, the $2r$ lower bound on the minimum Lee distance for the base-field codes $C(n, r, \boldsymbol{\alpha}; p)$ implies such a bound for the codes $C(n, r, \boldsymbol{\alpha})$ over the integer ring. In particular, the bound applies to codes with an rth-order spectral null at zero frequency [9],[11],[4] (see Equation (5)).

One application of integer spectral-null codes is to improving the reliability of information transmission over noisy partial-response channels. As shown in [11], the application of a code with Kth-order spectral null at zero frequency to a partial-response channel with Lth-order spectral null at zero frequency (i.e., transfer polynomial $h(D)$ divisible by $(1-D)^L$) ensures a minimum Lee distance no smaller than $2(K+L)$. When used in this context, the code is referred to in [11] as a matched-spectral-null code. We will consider the integer codes $C(n, K)$ for transmission over the channel $h(D) = (1-D)^L$. During the transmission process, a codeword of $C(n, K)$ is sent through the channel, followed by L consecutive zeros. Assuming that the initial channel memory is all-zero, the corresponding noiseless output words in the channel will be codewords of $C(n+L, K+L)$ i.e., they will have a $(K+L)$th-order spectral null at zero frequency.

When the channel noise samples are independent, and identically distributed according to a bilateral exponential density,

$$f(x) = \frac{\gamma}{2} e^{-\gamma|x|} \, ,$$

having zero mean and variance equal to $2\gamma^{-2}$, maximum-likelihood decoding is equivalent to finding a channel noiseless output word which is at the smallest Lee distance from the received word. Since the noiseless output words are codewords of $C(n+L, K+L)$, the algorithm of Section 5, when applied to $C(n+L, K+L)$, performs an efficient decoding with respect to the Lee metric for all error patterns in such a channel with Lee weight up to $K+L-1$.

Acknowledgment

The authors thank Noga Alon for helpful discussions. We also wish to thank Jack Wolf, Dave Forney, Dennis Howe, and Solomon Golomb for useful comments.

References

[1] J.T. Astola, *Concatenated codes for the Lee metric, IEEE Trans. Inform. Theory,* Vol. IT-28, No. 5 (September 1982), pp. 778–779.

[2] E.R. Berlekamp, *Algebraic Coding Theory,* Revised Edition, Aegean Park Press, Laguna Hills, California, 1984.

[3] J.C.-Y. Chiang, J.K. Wolf, *On channels and codes for the Lee metric, Inform. Control,* Vol. 19, No. 2 (September 1971), pp. 159–173.

[4] E. Eleftheriou, R. Cideciyan, *On codes satisfying Mth order running digital sum constraints, IEEE Trans. Inform. Theory,* Vol. IT-37, No. 5 (September 1991), pp. 1294–1313.

[5] S.W. Golomb, L.R. Welch, *Algebraic coding and the Lee metric,* in: *Error Correcting Codes* (H.B. Mann, Editor), John Wiley, 1968, pp. 175–194.

[6] S.W. Golomb, L.R. Welch, *Perfect codes in the Lee metric and the packing of polyominoes, SIAM J. Appl. Math.,* Vol. 18, No. 2 (January 1970), pp. 302–317.

[7] H.M. Hilden, D.G. Howe, E.J. Weldon, Jr., *Shift error correcting modulation codes, IEEE Trans. Magn.,* Vol. MAG-27, No. 6 (November 1991), pp. 4600–4605.

[8] K.A.S. Immink, *Coding Techniques for Digital Recorders,* Prentice-Hall, London, 1991.

[9] K.A.S. Immink, G. Beenker, *Binary transmission codes with higher order spectral zeros at zero frequency, IEEE Trans. Inform. Theory,* Vol. IT-33, No. 3 (May 1987), pp. 452–454.

[10] H. Jinushi, K. Sakaniwa, *A construction method for multilevel error-correcting codes based on absolute summation weight, Abstracts of 1990 IEEE Int. Symp. Info. Th.,* San Diego, CA (January 1990), p. 87.

[11] R. Karabed, P.H. Siegel, *Matched spectral-null codes for partial-response channels, IEEE Trans. Inform. Theory,* Vol. 37, No. 3, Part II (May 1991), pp. 818–855.

[12] A.V. Kuznetsov, A.J. Han Vinck, *Single peak-shift correction in (d, k)-sequences, Abstracts of 1991 IEEE Int. Symp. Info. Th.,* Budapest, Hungary (June 1991), p. 256.

[13] A.V. Kuznetsov, A.J. Han Vinck, *The application of q-ary codes for the correction of single peak-shifts, deletions and insertions of zeros,* preprint.

[14] C.Y. Lee, *Some properties of nonbinary error-correcting codes, IRE Trans. Inform. Theory,* Vol. IT-4, No. 4 (June 1958), pp. 77–82.

[15] R. Lidl, H. Niederreiter, *Finite Fields,* Addison-Wesley, Reading, Massachusetts, 1983.

[16] F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error-Correcting Codes,* North-Holland, Amsterdam, 1977.

[17] B.H. Marcus, P.H. Siegel, J.K. Wolf, *Finite-state modulation codes for data storage, IEEE J. Select. Areas Commun.,* Vol. 10, No. 1 (January 1992), pp. 5–37.

[18] J.L. Massey, *Shift register synthesis and BCH decoding, IEEE Trans. Inform. Theory,* Vol. IT-15, No. 1 (January 1969), pp. 122–127.

[19] L.E. Mazur, *Codes correcting errors of large weight in Lee metric, Problems Inform. Trans.,* Vol. 9, No. 4 (1973), pp. 277–281 (translated from Russian).

[20] R.J. McEliece, *The Theory of Information and Coding,* Addison-Wesley, Reading, Massachusetts, 1977.

[21] K. Nakamura, *A class of error-correcting codes for DPSK channels, Proc. IEEE International Conference on Communications* (1979), 45.4.1–45.4.5.

[22] A. Orlitsky, *Interactive communication: balanced distributions, correlated files, and average-case complexity, Proc. 32nd IEEE Symposium on the Foundations of Computer Science* (1991), 228–238. To appear in *SIAM J. Disc. Math.*

[23] P.H. Siegel, *Recording codes for digital magnetic recording, IEEE Trans. Magn.*, Vol. MAG-21, No. 5 (September 1985), pp. 1344–1349.

[24] C. Satyanarayana, *Lee metric codes over integer residue rings, IEEE Trans. Inform. Theory,* Vol. IT-25, No. 2 (March 1979), pp. 250–254.

[25] W. Ulrich, *Non-binary error correction codes, Bell Sys. Tech. J.,* Vol. 36, No. 6 (November 1957), pp. 1341–1387.