Decoding BCH codes and $q$-ary lattices in the Lee metric

Robson Ricardo de Araujo  Antonio Aparecido de Andrade
Instituto de Biociências, Letras e Ciências Exatas - IBILCE/UNESP  São José do Rio Preto, SP
E-mail: robcardo@ig.com.br, andrade@ibilce.unesp.br

SUMMARY

The Theory of Error Control Codes began around the late 1950’s by Claude Shannon. Since then, many works were published in this area and developed contributing to the transmission of information and data retention. Most often, these studies are done on codes in the Hamming metric. Such codes are designed to correct a certain number of errors, where error is defined as a change of an entry in the transmitted codeword through a channel of communication, irrespective of the (nonzero) error value.

Alternatively to Hamming metric was developed the Lee metric for transmission of nonbinary signals over certain noisy channels. The Lee metric is defined over integer residues modulo $q$. For codes in the Lee metric, an error is a change of an entry in a codeword by $\pm 1$. Such codes were described first by C. Y. Lee, in 1958, and by W. Ulrich, in 1957. This type of errors is found in noisy channels that use phase-shift keying (PSK) modulation and in channels that are susceptible to synchronization errors. In [1], the authors do applications to Constrained and Partial-Response Channels. The Lee metric can also be used in information compactification (see [6]). According to [2], the Lee metric has a close relation with the $l_1$ metric (or Taxi Cab metric), concerning the existence of perfect codes and the construction of dense error-correcting codes from dense lattice packings of $n$-dimensional cross-polytopes. In this work, we will present how decode BCH codes and $q$-ary lattices defined over the Lee metric.

Let $a \in \mathbb{Z}_q$, for $q \in \mathbb{Z}_+$. The Lee value of $a$, denoted by $|a|$, is $a$, if $0 \leq a \leq q/2$, or $q - a$, if $q/2 < a < q - 1$. For vectors $c = (c_1, c_2, \ldots, c_n)$ and $d = (d_1, d_2, \ldots, d_n)$ over $\mathbb{Z}_q$, the Lee weight of $c$ is $w_L(c) = \sum_{j=1}^{n} |c_j|$ and the Lee distance between them is defined by $d_L(c, d) = w_L(c - d)$, which is a metric. Let $C \subset \mathbb{Z}_q^n$ be a set. The minimum Lee distance of $C$ is the minimum Lee distance between any pair of distinct vectors in $C$, which is denoted by $d_L(C)$. If $C$ is a linear code, this is, a $\mathbb{Z}_q$-submodule of $\mathbb{Z}_q^n$, then $d_L(C)$ is the minimum Lee weight of any nonzero codeword in $C$. Let $c \in C$ be a codeword transmitted for a communication channel and be $y \in \mathbb{Z}_q^n$ the vector received after the transmission. Then, $e = y - c$ is called error vector of the transmission and the number of Lee errors is given by $w_L(e)$. If $C \subset \mathbb{Z}_q^n$ is a linear code whose minimum distance is $d$, then $C$ can correct any pattern of up to $(d - 1)/2$ Lee errors.

In the first part of the work, we will present BCH codes in the Lee metric and its decoding. A BCH code of length $n$ over $\mathbb{Z}_p = GF(p)$ (finite field, $p$ prime) is a linear code $C(n, r, \alpha; p)$ whose elements are $c$ such that $HC^T = 0$, where

$$H = \begin{bmatrix}
1 & 1 & \ldots & 1 \\
\alpha_1 & \alpha_2 & \ldots & \alpha_n \\
\alpha_1^2 & \alpha_2^2 & \ldots & \alpha_n^2 \\
\ldots & \ldots & \ldots & \ldots \\
\alpha_1^{r-1} & \alpha_2^{r-1} & \ldots & \alpha_n^{r-1}
\end{bmatrix}$$
(this is called parity-check matrix), \( \alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \) is the locator vector, consisting of distinct nonzero elements of the smallest field \( GF(p^m) \) of size greater than \( n \), and \( r \) is a positive integer. In this case, the linear code \( C(n, r; \alpha; p) \) is a vector subspace whose dimension is \( k \), where \( k \) is \( n - s \), being \( s \) the number of lines of \( H \) when \( H \) is described over \( GF(p) \). If \( m = 1 \), \( C(n, r; \alpha; p) \) is called base-field code. If \( n = p^m - 1 \), \( C(n, r; \alpha; p) \) is called primitive code.

The minimum Lee distance, \( d_L \), of the code \( C(n, r; \alpha; p) \) is bounded by

\[
d_L(n, r, \alpha; p) \geq \begin{cases} 
2r & \text{se } r \leq \frac{p-1}{2} \\
p & \text{se } \frac{p+1}{2} \leq r < p.
\end{cases}
\]

If \( C(n, r; \alpha; p) \) is a base-field code, we can ignore the condition \( r \leq \frac{p-1}{2} \), this is, the lower bound of this code takes the form \( d_L(n, r; \alpha; p) \geq 2r \) for \( r \leq n \leq p - 1 \). To prove these two bounds it is used power formal series, polynomials and the Newton’s identities. If \( C = C(p-1, \alpha, r; p) \) is a primitive base-field BCH code with dimension \( k \neq 0 \) \((k = p-1 - r)\), then \( d_L(C) \geq (p^2 - k^2)/(4k) \), that is a better bound for \( C \) than \( 2r \) if \( r \geq 6p/7 \).

If \( r \leq (p-1)/2 \) or \( r \leq n \leq p \), the BCH code \( C(n, r; \alpha; p) \) has minimum Lee distance \( d_L \geq 2r \) and, therefore, it is capable to correct up to \( r - 1 \) Lee errors. In this case, it exist a decoding procedure for \( C(n, r, \alpha; p) \) based upon Euclid’s algorithm for division of polynomials. In this work, we intend to describe the algorithm to decoding a BCH code. In [1], the authors do an adaptation of that algorithm for base-field BCH codes.

BCH codes in the Lee metric can be studied over the ring \( \mathbb{Z} \) too (change \( \mathbb{Z}_q \) by \( \mathbb{Z} \)), which is denoted by \( C(n, r, \alpha) \). Using the results about base-field BCH codes, it is possible prove that, if \( r \leq n \) and \( C = C(n, r, \alpha) \) is a integer code then \( d_L(C) \geq 2r \). The decoding method for codes over \( GF(p) \) can be adapted for integer codes. Integer BCH codes can be applied to efficiently protect against synchronization and so-called bitshift errors in runlength-limited (RLL) \((d,k)\)-constrained channels (see [1]).

In the second part of the work, we will present \( q \)-ary lattices in the Lee metric. A lattice \( L \) is a discrete additive subgroup of \( \mathbb{R}^n \) or, equivalently, \( L \subset \mathbb{R}^n \) is a lattice iff there are linearly independent vectors \( v_1, v_2, \ldots, v_m \in \mathbb{R}^n \) such that \( L = \{a_1v_1 + a_2v_2 + \ldots + a_nv_n : a_i \in \mathbb{Z} \} \). The set \( \{v_1, v_2, \ldots, v_m\} \) is called a basis for \( L \). If \( m = n \), \( L \) is said a full rank lattice. If \( L \subset \mathbb{Z}^n \), we can say that \( L \) is an integer lattice. A subset \( X \subset \mathbb{R}^n \) is called discrete if, for all \( x \in X \), exist \( r \) such that \( B(x, r) \cap X = \{x\} \), where \( B(x, r) \) means the ball of center \( x \) and radius \( r \). Then, a additive subgroup of \( \mathbb{R}^n \) is a lattice if and only if it is discrete.

A matrix \( M \) whose columns are \( v_1, v_2, \ldots, v_m \) is a generator matrix for \( L \). If \( L \) is a full rank lattice, we can define the determinant of \( L \) by \( \det(L) = |\det(M)| \), which is invariant under basis change. Given \( d \) a matrix in \( \mathbb{R}^n \), the Voronoi region of \( x \in L \) is the set \( V(x) = \{y \in \mathbb{R}^n : d(y, x) \leq d(z, x), \forall z \in L \} \). Geometrically, the Voronoi region of \( x \in L \) is the set of the points in \( \mathbb{R}^n \) closer of \( x \) than of other \( z \in L \). We can use a lattice as a code. In this case, to decode \( y \in \mathbb{R}^n \) means finding the closest point \( x \in L \) to \( y \) (lattice decoding). The lattice decoding has applications in information transmission over a channel with additive white Gaussian noise and in cryptography. This problem is computationally difficult for general integer lattices, proved to be NP-Hard.

Let \( C \subset \mathbb{Z}_q^n \) be a linear code. Then, by the so-called Construction A, it is possible associates to \( C \) an integer lattice \( L_q(C) \) via the surjective map \( \phi : \mathbb{Z}^n \rightarrow \mathbb{Z}_q^n \) given by \( \phi(x_1, x_2, \ldots, x_n) = (\overline{x_1}, \overline{x_2}, \ldots, \overline{x_n}) \), where \( \overline{v} \) will denote the the value of \( v \in \mathbb{Z} \) in \( \mathbb{Z}_q \) henceforward. Due to this map, \( L_q(C) = \phi^{-1}(C) \) is a lattice, which is called \( q \)-ary lattice associated to \( C \). Any \( q \)-ary lattice has \( q\mathbb{Z}^n \) as a sublattice. On the other hand, if \( q\mathbb{Z}^n \subset L \) then \( L \) is a \( q \)-ary
lattice. Moreover, $L_q(C)/q\mathbb{Z}^n \sim C$ (where $\sim$ denotes isomorphism).

If $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ are two vectors in $\mathbb{R}^n$, the sum distance (or $l_1$ distance) of $\mathbb{R}^n$ is defined by $d_1(x, y) = \sum_{i=1}^{n} |x_i - y_i|$. Through the map $\phi$, the distance induced by $d_1$ is the Lee metric $d_L(x, y)$. The minimum norm $\mu$ of a lattice $L$ is $\mu = \min_{x \neq 0} d_L(x, 0)$ and for a $q$-ary lattice $L_q(C)$, $\mu = \min\{q, d_L(C)\}$, where $d_L(C)$ denotes the minimum Lee distance of $C$.

It is known a decoding process for lattices constructed from binary codes via Construction A. In this work, we intend to present the relationship between decode $C \subset \mathbb{Z}_q^n$ and decode $L_q(C)$ with the Lee metric. Given $r \in \mathbb{R}^n$, let $z$ be its closest point in $L_q(C)$ by the Lee metric. We will see via Construction A a representative of $z$ which is given by a codeword in $C$. So, we will have a decoding process for $q$-ary lattices with the Lee metric via its generator code, what is mainly interesting if the associated codes with an efficient Lee decoding algorithm. For example, we can use the BCH codes with parameter $r \leq (p - 1)/2$ or $r \leq n \leq p$ because it is known a good method of decoding to them.

Finally, we can conclude that the Lee metric can be used as an alternative to codes in the Hamming metric. Furthermore, due to the fact that the Lee metric in $\mathbb{Z}_q^n$ is induced by the sum distance in $\mathbb{R}^n$, it is possible decode $q$-ary lattices mainly when its associated code can be corrected efficiently in the Lee metric.

Classification: Information and communication, circuits - Theory of error-correcting codes and error-detecting codes.

Keywords: Lee metric, BCH codes, lattices, $q$-ary codes.

References


