On Channels and Codes for the Lee Metric

J. Chung-Yaw Chiang

GTE Laboratories, 40 Sylvan Road, Waltham, Mass. 02154

AND

Jack K. Wolf

Department of Electrical Engineering, Polytechnic Institute of Brooklyn
Brooklyn, N. Y. 11201

Almost all nonbinary codes were designed for the Hamming metric. The Lee metric was defined by Lee in 1958. Golomb and Welch (1968) and Berlekamp (1968) have designed codes for the Lee metric. In this paper, we derive all the discrete, memoryless, symmetric channels matched to the Lee metric, and investigate general properties of Lee metric block codes. Finally, a class of cyclic Lee metric codes is defined and the number of information symbols is discussed.

1. INTRODUCTION

Almost all nonbinary codes in coding theory were designed for the Hamming metric. Hamming metric codes are ideal codes for the balanced channel (Helstrom, 1961) in which probabilities of error for all symbols are equal. Ulrich (1957) considered codes which can correct a + 1 or −1 error in a codeword. Lee (1958) defined the Lee metric. Later, Prange (1959), Massey (1967), Graham and Wyner (1968), Golomb and Welch (1968), Berlekamp (1968a, b) and Golomb (1969) have considered this metric. Golomb and Welch (1968) and Berlekamp (1968a, b) have designed codes for the Lee metric. Massey (1967) defined the notion of a metric matched to a channel and included as an example a channel matched to the Lee metric. Graham and

* This work was taken from a dissertation submitted by Chung-Yaw Chiang to the Faculty of the Polytechnic Institute of Brooklyn, in partial fulfillment of the requirements for the Ph.D. degree. This research was sponsored by the U.S. Air Force office of Scientific Research under Contracts AF 49(638)-1600 and F-44620-71-C-0001.
Wyner (1968) derived a Plotkin bound for Lee metric codes. Golomb and Welch (1968) found a class of single-Lee-error-correcting perfect codes and a class of double-Lee-error-correcting perfect codes. Golomb (1969) discussed the general error spheres for several possible metrics. Berlekamp (1968a, b) derived a class of negacyclic Lee metric codes.

In Section 2 of this paper, we derive all the discrete, memoryless, symmetric channels matched to the Lee metric. Section 3 treats the information rate of optimum Lee metric block codes. An upper bound on the minimum Lee distance of a linear code is established. In Section 4, we consider some properties of linear Lee metric block codes. In the last section, a class of cyclic Lee metric codes is defined by modifying Berlekamp's negacyclic codes. The number of information symbols for both cyclic and negacyclic codes is then investigated.

2. Lee Metric and Channel Models

The Lee metric was defined by Lee (1958) for the integers mod $q$ and vectors over these integers. We represent the integers mod $q$ by

\[-\frac{q-1}{2}, \ldots, -\frac{q-3}{2}, -1, 0, 1, \ldots, \frac{q-1}{2}, \]

if $q$ is odd,

\[-\frac{q-2}{2}, \ldots, -1, 0, 1, \ldots, \frac{q-2}{2}, \frac{q}{2}, \]

if $q$ is even.

The *Lee weight* of an element $C_i$ of the integers mod $q$ is defined as the absolute value of $C_i$, i.e.,

$$W_L(C_i) = |C_i|.$$ 

The *Lee weight* of a vector is the sum of the Lee weights of its components. The *Lee distance* between any two elements $C_i$ and $C_j$ of the integers mod $q$ is the Lee weight of $C_i - C_j$ mod $q$. If the $q$ elements are drawn on a circle as shown in Fig. 1 and if each arc is of Lee distance one, then the Lee distance between any two elements is the minimum distance one has to trace on the circle from one element to the other.

The Lee distance between two vectors $\mathbf{a}$ and $\mathbf{b}$, $\rho_L(\mathbf{a}, \mathbf{b})$, is the sum of the Lee distance between their corresponding components $a_i$ and $b_i$,

$$\rho_L(\mathbf{a}, \mathbf{b}) = \sum_{i=1}^{n} \rho_L(a_i, b_i).$$
The problem of choosing a metric for a given channel or finding the channels which are matched to a given metric is dependent on the decoding scheme.

**FIG. 1.** Lee metric for integers mod $q$, for $q = 8$.

**DEFINITION 1.** A metric and a discrete, memoryless channel are said to be matched for maximum likelihood decoding (MLD) if the decoding rule "decode the received vector to the nearest (or farthest) codeword" always gives a most probable codeword (Massey, 1967).

We shall also consider the following weakened form of matching.

**DEFINITION 2.** A metric and a discrete, memoryless channel are said to be matched for bounded discrepancy decoding (BDD) (Wyner, 1965) if the decoding rule "decode the received vector to the codeword which is within a distance of $t$ or less", where $t$ is an integer smaller than half of the minimum distance between all pairs of codewords, gives (whenever a decision has been made) a most probable codeword.

In this paper, we will consider only those channels for which the errors are independent of the codeword being transmitted. For such channels,

$$\Pr(R | C_i) = \Pr(R - C_i | 0) = \Pr(E_i),$$

where $R$ is the received vector, $C_i$ is a codeword, and $E_i$ is the error vector. Then we will show the following two definitions are restatements of Definitions 1 and 2, with the additional requirement that the nearest codeword be strictly more probable than a codeword farther from the received word.
DEFINITION 3. A metric and a discrete, memoryless channel are strictly matched for MLD if the following is true\(^1\). Let \( E \) and \( E' \) be two error vectors, 
\[
W(E) < W(E') \quad \text{iff} \quad \Pr(E) > \Pr(E')
\]
(Note that Definition 3 implies \( W(E) = W(E') \) iff \( \Pr(E) = \Pr(E') \).)

DEFINITION 4. A metric and a discrete, memoryless channel are strictly matched for BDD if the following is true: If 
\[
W(E) \leq t \quad \text{and} \quad W(E') \geq t + 1, \quad \text{then} \quad \Pr(E) > \Pr(E').
\]

It is obvious from the definitions that a metric matched to a channel for MLD is also matched to the channel for BDD.

Definition 1 (matching) and Definition 3 (strictly matching) coincide except for the trivial channels in which all error patterns have the same probability. To show this, note that Definition 1 requires that nearest neighbor decoding be maximum likelihood decoding for all block lengths. Now suppose that for some block length one can find \( E \) and \( E' \) such that \( W(E) < W(E') \) but \( \Pr(E) = \Pr(E') \), and suppose there is at least one pair of error digits \( e_i \) and \( e_j \) such that \( \Pr(e_i) < \Pr(e_j) \). Letting \( E^q \) be the concatenation of \( q \) vectors of \( E \), \( q \) being a number greater than \( W(e_i) \), then
\[
W(E^q) \leq W(E'^q) - q
\]
and
\[
W(e_iE^q) < q + W(E^q) \leq W(E'^q) \leq W(e_iE'^q),
\]
where \( e_i \) is concatenated to \( E^q \) and \( e_j \) to \( E'^q \). But also
\[
\Pr(e_iE^q) < \Pr(e_jE'^q)
\]
so that the nearest neighbor decoder would not be maximum likelihood. Hence \( W(E) < W(E') \) must imply \( \Pr(E) > \Pr(E') \) if the channel is matched, and the converse is trivial. Thus Definitions 1 and 3 are equivalent whenever the error digits (including zero) do not all have the same probability.

THEOREM 1. A discrete, memoryless, symmetric channel as shown in Fig. 2 is strictly matched to the Lee metric for MLD iff \( p_i = p_1^i/p_0^{i-1} \) and \( p_0 > p_1 \).

\(^1\) Note that the Hamming metric is matched to the binary symmetric channel with \( p = \frac{1}{2} \) in the sense of Definition 1, but not strictly matched in the sense of Definition 3, since the probability of error is the same for all error vectors.
ON CHANNELS AND CODES FOR THE LEE METRIC

163

\[ M = \left[ \frac{q}{2} \right] \]

\[ [x] = \text{integer part of } x \]

\[ \Pr(b \mid 0) = p_i \quad i = 0, 1, 2, \ldots, M \]

\[ \Pr(b \mid 0) = p_i \quad i = 1, 2, \ldots, M \]

\[ \Pr(b \mid 0) = \Pr(k \mid 0) \text{ where } k \equiv l - j \mod q \]

\[ \begin{array}{c}
\begin{array}{c}
0 \\
1 \\
-1 \\
-2 \\
\vdots \\
\left[ \frac{q-1}{2} \right]
\end{array}
\end{array} \]

\[ p_0 \]

\[ p_1 \]

\[ p_2 \]

\[ p_3 \]

\[ p_4 \]

\[ \vdots \]

\[ p_{M} \]

\[ \begin{array}{c}
\begin{array}{c}
2 \\
1 \\
0 \\
-1 \\
-2 \\
\vdots \\
\left[ \frac{q-1}{2} \right]
\end{array}
\end{array} \]

**FIG. 2.** Conditional probabilities for a discrete, memoryless, symmetric channel.

**Proof.** Let

\[ L = \sum_{i=1}^{M} ih_i = \text{Lee weight of vector } E, \]

\[ L' = \sum_{i=1}^{M} ih_i' = \text{Lee weight of vector } E' \]

where \( h_i (h_i') = \) number of components of \( E (E') \) which have Lee weight \( i \).

Then

\[ \Pr(E) = p_0^{n-\sum_{i=1}^{M} h_i} \prod_{i=1}^{M} p_i^{h_i} = p_0^{n-L} \prod_{i=1}^{M} (p_i p_0^{i-1})^{h_i}, \]

(1)

\[ \Pr(E') = p_0^{n-\sum_{i=1}^{M} h_i'} \prod_{i=1}^{M} p_i^{h_i'} = p_0^{n-L'} \prod_{i=1}^{M} (p_i p_0^{i-1})^{h_i'}. \]

(2)

Dividing (1) by (2),

\[ \frac{\Pr(E)}{\Pr(E')} = p_0^{L-L} \prod_{i=1}^{M} (p_i^{i-1} p_i^{i-h_i})^{h_i-h_i'} = p_0^{L-L} \prod_{i=1}^{M} p_i^{(i-h_i-h_i')} = \left( \frac{p_0}{p_1} \right)^{L-L}. \]

Since \( p_0 > p_1 \),

\[ \frac{\Pr(E)}{\Pr(E')} = \left( \frac{p_0}{p_1} \right)^{L-L} > 1 \quad \text{iff} \quad L < L'. \]
To prove the necessity, let

\[ E_i = (1, 1, \ldots, 1, 0, \ldots, 0), \quad W_L(E_i) = i, \]
\[ E_i' = (i, 0, \ldots, 0), \quad i = 1, 2, \ldots, M. \]

Since \( W_L(E_i) = W_L(E_i') \), then \( p_1 i p_0^{n-i} = p_i p_0^{n-1} \) and \( p_i = p_1 i p_i p_0^{-1} \). Also, \( W_L(E_0) < W_L(E_2) \) implies \( p_0 > p_1 \) Q.E.D.

**THEOREM 2.** A discrete, memoryless, symmetric channel as shown in Fig. 2 is strictly matched to the Lee metric for BDD with \( t = 1 \), iff

\[ p_0 > p_1 > p_j \quad \text{for} \quad j = 2, 3, \ldots, M. \]

**Proof.** Let \( E \) be an error vector of Lee weight one, and let \( E' \) be an error vector of Lee weight greater than one. Then

\[
\frac{Pr(E)}{Pr(E')} = \frac{\frac{p_0^{n-1} p_1}{p_0^{n} - \sum_{i=1}^{M} h_i ^{i} \prod_{i=1}^{M} p_i^{h_i ^{i}}}}{p_0^{n-1} p_1^{h_i ^{i}} \prod_{i=2}^{M} p_i^{h_i ^{i}}} = \frac{p_0^{n-1} p_1^{h_i ^{i}} \prod_{i=2}^{M} p_i^{h_i ^{i}}}{p_0^{h_i ^{i}} \prod_{i=2}^{M} p_i^{h_i ^{i}}} = \frac{p_0}{p_1} \prod_{i=2}^{M} \left( \frac{p_0}{p_i} \right)^{h_i ^{i}}.
\]

If \( h_i ^{i} \neq 0 \), then \( \frac{Pr(E)}{Pr(E')} > 1 \). If \( h_i ^{i} = 0 \), but \( h_i ^{i} \neq 0 \) for some \( j > 1 \), then

\[
\frac{Pr(E)}{Pr(E')} = \left( \frac{p_1}{p_0} \right) \left( \frac{p_0}{p_j} \right) ^{h_i ^{i}} \prod_{i=2}^{M} \left( \frac{p_0}{p_i} \right)^{h_i ^{i}} \]

\[
= \left( \frac{p_1}{p_j} \right) ^{h_i ^{i} - 1} \prod_{i=2}^{M} \left( \frac{p_0}{p_i} \right)^{h_i ^{i}} > 1.
\]

To prove the necessity, let

\[ E_1 = (1, 0, \ldots, 0), \]
\[ E_j = (j, 0, \ldots, 0), \quad j = 2, 3, \ldots, M, \]
\[ E_2' = (1, 1, 0, \ldots, 0), \]
then
\[ Pr(E_1) > Pr(E_2') \] implies \( p_0 > p_1 \),
\[ Pr(E_3') > Pr(E_3) \] implies \( p_1 > p_3 \). Q.E.D.

**Theorem 3.** A memoryless channel as shown in Fig. 2 is strictly matched
to the Lee metric for BDD with \( t = 2 \), iff the following are true:

(i) \( p_0 > p_1 > p_2 > p_3 \),
(ii) \( p_1^2 > p_3 p_0 \), for \( j = 3, 4, \ldots, M \), and
(iii) \( p_2 > p_3^{3/2} p_0^{1/2} \).

The proof is parallel to that for Theorem 2 and is omitted.

3. The Information Rate of Optimum Lee Metric Codes

There are four known bounds on the minimum Lee distance of block
codes. These four bounds are true for both linear and nonlinear block codes.
We will derive a fifth bound for linear block codes.

*The Hamming and Gilbert Bounds*

Let the volume of a sphere of radius (in Lee metric) \( r \) in an \( n \)-dimensional
vector space be \( V_r^{(n)} \). Let \( d_L \) be the minimum Lee distance of a code of length \( n \)
and rate \( R \), and let \( t \) be the greatest integer such that \( t \leq (d_L - 1)/2 \). Then

\[ q^n q_v^{(n)} \leq q^n \quad \text{or} \quad V_r^{(n)} \leq q^n (1 - R) \quad \text{(Hamming Bound).} \]

Given \( n \) and \( R \), there is at least one code such that its minimum Lee
distance \( d_L \) satisfies

\[ V_r^{(n)} \geq q^n (1 - R) \quad \text{(Gilbert Bound).} \]

Codes are said to be *closed-packed* or *perfect* if they satisfy the Hamming
bound with equality.

The volume \( V_r^{(n)} \) can be calculated as follows: Let \( A_i^{(n)} \) be the *surface area*
of a sphere of radius \( i \) and let \( A_r^{(n)}(z) = \sum_i A_i^{(n)} z^i \) be a generating function. Then

\[ V_r^{(n)}(z) = \sum_{i=0}^r A_i^{(n)} = \left( \sum_{i=0}^r \frac{1}{i!} \frac{d^i}{dz^i} A_r^{(n)}(z) \right)_{z=0} \]  \quad (3)
Since the Lee distance is additive over the $n$ coordinates, the generating function $A^{(n)}(z)$ is multiplicative over these coordinates (see Berlekamp, 1968b, p. 298), and $A^{(n)}(z) = (A^{(1)}(z))^n$. Thus,

$$A^{(n)}(z) = \begin{cases} 
\left(1 + 2z + 2z^2 + \cdots + 2z^{(q-1)/2}\right)^n & \text{if } q \text{ is odd} \\
\left(1 + 2z + 2z^2 + \cdots + z^{q/2}\right)^n & \text{if } q \text{ is even}
\end{cases}$$

(4)

From Eqs. (3) and (4), one can find the value for $V_r^{(n)}$. For example, $V_1^{(n)} = 1 + 2n$ for any $q \geq 3$, $V_3^{(n)} = 1 + 2n^2$ for $q = 3$, and $V_4^{(n)} = 1 + n + 2n^2$ for $q = 4$ and $V_5^{(n)} = 1 + 2n + 2n^2$ for any $q \geq 5$, etc.

**Plotkin's Low-rate Average Distance Bound**

This bound was obtained by Graham and Wyner (1968), based upon the fact that the minimum distance between any pair of codewords in a code cannot exceed the average distance between all pairs of distinct codewords. The result is $d_L \leq n\bar{D}/(1 - K^{-1})$, where $K$ is the number of codewords in the code and $\bar{D}$ is the average Lee weight of the integers mod $q$, and is given by

$$\bar{D} = \begin{cases} 
\frac{q^2 - 1}{4q} & \text{if } q \text{ is odd} \\
\frac{q}{4} & \text{if } q \text{ is even}
\end{cases}$$

(5)

**The Elias Bound**

This bound was obtained by combining the Hamming bound and the average distance bound. According to Lemmas 13-61 and 13-62 of Berlekamp (1968b), given any integer $t$ and a code of length $n$ and rate $R$, there exists a critical sphere of radius $t$ which includes $K$ codewords, where $K = V_t^{(n)}/q^n(1-R)$. By suitable translation of the code, this critical sphere may be centered at $0$. Then each codeword of the critical sphere has weight smaller than or equal to $t$. The Elias bound says that for $0 < t < \mathcal{D}n$, the minimum distance

$$d_L \leq \left(\frac{t}{1 - K^{-1}}\right)\left(2 - \frac{t}{n\bar{D}}\right),$$

(6)

where $K$ is the least integer not less than $V_t^{(n)}/q^n(1-R)$, and $t$ should be chosen in such a way as to minimize the right side of inequality (6).
An Upper Bound on $d_L$ for Linear Codes

**Theorem 4.** For any $(n, k)$ linear Lee metric code, the minimum distance $d_L$ is bound from above as follows:

$$d_L \leq \begin{cases} 
\frac{q+1}{4} (n-k+1) & \text{if } q \text{ is odd} \\
\frac{q^2}{4(q-1)} (n-k+1) & \text{if } q \text{ is even.}
\end{cases} \quad (7)
$$

**Proof.** Let the parity-check matrix of an $(n, k)$ code be $H$, which has $n$ columns and $n-k$ linear independent rows. We annex to this matrix $k-1$ additional rows, each of which is an $n$-dimensional unit vector, such that the new matrix has rank $n-1$. This new matrix is the parity-check matrix of a subcode of the original code. This subcode consists of $q$ codewords which have zeros in a specified set of $k-1$ positions. Applying Plotkin's average distance bound to this subcode, and from the property that the minimum distance $d_L$ of a code is smaller or equal to the minimum distance of its subcode, we have

$$d_L \leq \frac{\bar{D}(n-k+1)}{1-1/q}.$$ 

The theorem is proved by substituting $\bar{D}$ with values given by (5). Q.E.D.

For any prime $p$, the code generated by

$$G = \left(1, 2, 3, \ldots, \frac{p-1}{2}, -\frac{p-1}{2}, \ldots, -2, -1\right)$$

is an equidistant code in the Lee metric. These codes satisfy (7) with equality. Another example is the $(4,2)$ code over $GF(5)$, generated by

$$G = \begin{pmatrix} -2 & -1 & 1 & 0 \\ 0 & -2 & -1 & 1 \end{pmatrix}.$$ 

The minimum Lee distance of this code is equal to 4, which is the greatest integer satisfying the bound given by (7).

4. **Some Properties of Linear Lee Metric Codes**

The *minimum Lee distance* of a code is defined as the minimum Lee distance between all pairs of codewords. For linear codes, the difference of any two
codewords is also a codeword. Thus, the minimum Lee distance of a linear code is equal to the minimum Lee weight of its nonzero codewords.

The minimum Lee distance of a code is greater than or equal to the minimum Hamming distance of the same code, and smaller than or equal to the Lee distance between the two codewords which define the minimum Hamming distance. Thus,

\[ d_H \leq d_L \leq \left\lceil \frac{q}{2} \right\rceil d_H, \]

where \([x]\) is the greatest integer smaller than or equal to \(x\).

A coset leader for a linear code is defined as a vector of minimum Lee weight in a coset. For a linear code with block length \(n\) and minimum Lee distance \(d_L\), any \(n\)-tuple of Lee weight smaller than or equal to \(\left\lfloor (d_L - 1)/2 \right\rfloor\) is the unique coset leader in its coset.

A vector \(v\) is called an immediate descendant of \(u\), if \(v\) can be obtained from \(u\) by changing one nonzero element, say \(u_i\), to \(u_i - 1\) if \(u_i > 0\) and to \(u_i + 1\) if \(u_i < 0\). \(v\) is called a descendant of \(u\), if \(v\) can be obtained from \(u\) by forming successive immediate descendants. It can be shown that if \(u\) is a coset leader, then all its descendants are coset leaders.

An interleaved code has the same minimum Lee distance as the basic code. The minimum Lee distance of a direct product code (for definition, see Berlekamp, 1968b, p. 338) can be bounded as follows. Let \(d_L\) and \(d_H\) be the minimum Lee distance and the minimum Hamming distance of the direct product code, respectively. The product code is formed from two codes, one has minimum distances \(d_{L1}\) and \(d_{H1}\) and the other has \(d_{L2}\) and \(d_{H2}\). Then it is easily seen that

\[ \max(d_{H2}d_{L1}; d_{H1}d_{L2}) \leq d_L \leq d_{L1}d_{L2}. \]

Since \(d_H = d_{H1}d_{H2}\) and from inequality (8),

\[ \max(d_{H2}d_{L1}; d_{H1}d_{L2}) \leq d_L \leq \min\left(\frac{q}{2} d_{H1}d_{H2}; d_{L1}d_{L2}\right). \]

5. CODES FOR MEMORYLESS LEE METRIC CHANNELS

Golomb and Welch (1968) showed that for every positive integer \(t\), there is a closed-packed \(t\)-Lee-error-correcting code of block length 2, over the alphabet of integers mod \(q\), \(q = 2t^2 + 2t + 1\). Berlekamp (1968b) has found a class of such codes. Golomb and Welch (1968) conjectured that no perfect Lee-error-correcting codes exist with \(t > 1\), \(n > 2\), and \(q > 3\).
Berlekamp (1968a, b) has found a class of negacyclic $t$-Lee-error-correcting codes over $GF(p)$, for any $t$ smaller than or equal to $(p - 1)/2$. The negacyclic code exists for any block length $n$ of the form $n = (p^m - 1)/2\lambda$, where $m$ and $\lambda$ are integers. Let $\alpha$ be a primitive element of $GF(p^m)$ and let $\beta = \alpha^\lambda$. Then the negacyclic $t$-Lee-error-correcting code is generated by the generator polynomial which has $\beta, \beta^3, \ldots, \beta^{2t-1}$ as the roots.

A class of cyclic Berlekamp Lee metric codes exist for odd $n$ of the form $n = (p^m - 1)/2$.

**Theorem 5.** For odd $n$, the $p$-ary code, with $p > 2$, generated by the polynomial which has $\gamma, \gamma^3, \ldots, \gamma^{2t-1}$ as roots, $\gamma = \alpha^{2\lambda}$ and $t \leq (p - 1)/2$, is a cyclic $t$-Lee-Error-correcting code.

**Proof.** The proof is similar to that for the negacyclic codes given by Berlekamp (1968b, Theorem 9.34). We have to show only that $\pm\gamma, \pm\gamma^2, \pm\gamma^3, \ldots, \pm\gamma^n = \pm1$ are distinct error locators. $\gamma, \gamma^2, \ldots, \gamma^n$ are distinct elements of $GF(p^m)$. Since $n$ is odd, $-1$ cannot be expressed as a power of $\gamma$. Thus, $-\gamma^i \neq \gamma^j$ for all $i, j$. The code is cyclic, because $(\gamma^i)^n = 1$ for $i = 1, 2, 3, \ldots, 2t - 1$. Q.E.D.

Table I shows some of the codes promised by Theorem 5.

The above cyclic and negacyclic codes will be said to be **primitive** if $\lambda = 1$.

**Example.** A $(15, 10)$ cyclic triple-Lee-error-correcting code over $GF(11)$ has the following parity-check matrix and generator polynomial.

$$H = \begin{pmatrix}
1 & \alpha & \alpha^8 & \alpha^{16} & \alpha^{24} & \alpha^{32} & \alpha^{40} & \alpha^{48} & \alpha^{56} & \alpha^{64} & \alpha^{72} & \alpha^{80} & \alpha^{88} & \alpha^{96} & \alpha^{104} & \alpha^{112} \\
1 & \alpha^{24} & \alpha^{48} & \alpha^{72} & \alpha^{96} & 1 & \alpha^{24} & \alpha^{48} & \alpha^{72} & \alpha^{96} & 1 & \alpha^{24} & \alpha^{48} & \alpha^{72} & \alpha^{96} \\
1 & \alpha^{40} & \alpha^{80} & 1 & \alpha^{40} & \alpha^{80} & 1 & \alpha^{40} & \alpha^{80} & 1 & \alpha^{40} & \alpha^{80} & 1 & \alpha^{40} & \alpha^{80}
\end{pmatrix}$$

$$= \begin{pmatrix}
0 & -2 & -3 & 0 & 4 & -5 & 0 & 3 & -1 & 0 & 5 & 2 & 0 & 1 & -4 \\
1 & 1 & 2 & -2 & -2 & 4 & 4 & 4 & 3 & 3 & 3 & -5 & 5 & 5 & -1 \\
1 & -2 & 4 & 3 & 5 & 1 & -2 & 4 & 3 & 5 & 1 & -2 & 4 & 3 & 5 \\
0 & -5 & 5 & 0 & -5 & 5 & 0 & -5 & 5 & 0 & -5 & 5 & 0 & -5 & 5 \\
1 & -4 & 3 & 1 & -4 & 3 & 1 & -4 & 3 & 1 & -4 & 3
\end{pmatrix},$$

where $\alpha^3 - 3\alpha - 3 = 0$,

$$g(x) = (x^2 + 4x + 5)(x + 2)(x^2 + x + 1) = x^5 - 4x^4 - 2x^3 - 4x^2 + x - 1.$$
### Table I

Some of the Cyclic Codes Promised by Theorem 5

<table>
<thead>
<tr>
<th>$p$</th>
<th>$m$</th>
<th>$(n = p^n - 1)/2$</th>
<th>Error correction</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>2</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>31</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>8</td>
<td>39</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>781</td>
<td>5</td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>171</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>57</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>16</td>
<td>4</td>
</tr>
<tr>
<td>11</td>
<td>1</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>21</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>665</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>133</td>
<td>3</td>
</tr>
<tr>
<td>13</td>
<td>2</td>
<td>8</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>549</td>
<td>3</td>
</tr>
<tr>
<td>19</td>
<td>1</td>
<td>9</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>3429</td>
<td>3</td>
</tr>
</tbody>
</table>

*Good nonprimitive codes.*

#### Number of Information Symbols in Berlekamp Lee Metric Codes

For a cyclic or negacyclic Berlekamp code, with block length $n = (p^n - 1)/2$ and designed minimum Lee distance $2t + 1$, the number of information symbols is greater than or equal to $n - mt$. We will show that for primitive codes the number of information symbols is exactly $n - mt$.

**Theorem 6.** If $\alpha$ is a primitive element of $\text{GF}(p^m)$, then the minimal polynomials of $\alpha, \alpha^2, \ldots, \alpha^{p-1}$ are distinct and each has degree $m$.

**Proof.** We will first show that the minimal polynomials are distinct. Let $M_i(x)$ be the minimal polynomial of $\alpha^i$. Assume $j \neq i$ and $\alpha^i$ is a root of $M_j(x)$. Since any root of $M_i(x)$ can be put in the form of $\alpha^{ir^j}$, $0 \leq r < m$,
we have \( \alpha^j = \alpha^{ip^r} \) and \( i p^r \equiv j \mod (p^m - 1) \). But \( ip^r \) and \( j \) are nonzero and smaller than \( p^m \), so that we have \( ip^r = j \) which can be true iff \( r = 0 \) and \( i = j \). Thus, we have a contradiction.

To show that each minimal polynomial is of degree \( m \), let \( \deg[M_i(x)] = s_i \). Then \( s_i \) divides \( m \) and we let \( m = as_i \). Since \( \alpha^{k(p^s_t - 1)} = 1 \) and is of order \( p^m - 1 \), then \( p^m - 1 \) divides \( i(p^s_t - 1) \). Thus,

\[
\frac{i(p^s_t - 1)}{p^m - 1} = \text{integer} = \frac{i(p^s_t - 1)}{p^{as_i} - 1} < p \left( \frac{p^s_t - 1}{p^{as_i} - 1} \right).
\]

It can be true only for \( a = 1 \), since the right side is less than 1 for \( a > 2 \).

Q.E.D.

The above theorem shows that \( M_1(x), M_2(x), \ldots, M_{2t-1}(x) \) are distinct polynomials and are of degree \( m \), for \( t \leq (p - 1)/2 \). Thus, the number of information symbols in a primitive negacyclic Berlekamp code is exactly \( n - mt \).

Similarly, we can show that the following theorem is true. The proof is omitted.

**Theorem 7.** If \( \alpha \) is a primitive element of \( GF(p^m) \), and if \( p^m - 1 \) is not divisible by 4, then the minimal polynomials of \( \alpha^1, \alpha^2, \ldots, \alpha^{2(p-1)} \) are distinct and have degree \( m \).

From Theorem 7, we know that the number of information symbols in a primitive cyclic Berlekamp code is also exactly \( n - mt \).

The exact number of information symbols in a nonprimitive code is not known. However, the following theorem and corollary are of help in estimating the number of information symbols.

**Theorem 8.** Let \( M_i(x) \) be the minimal polynomial of \( \alpha^i \), where \( \alpha \) is a primitive element of \( GF(p^m) \). If \( s \) is an integer which divides \( m \), then \( M_{(p^m-1/p^s-1)}(x) \) has degree smaller than or equal to \( s \) for any integer \( k \).

**Proof.** Let \( c = (p^m - 1)(p^s - 1) \). The polynomial \( M_{ck}(x) \) has \( \alpha^c, \alpha^{ck}, \alpha^{ck^2}, \ldots, \alpha^{ck^{k+1}}, \ldots \) as roots. But

\[
\alpha^{ck^s} = \alpha^{ck(p^s - 1)} \alpha^c
= \alpha^{k(p^m - 1/p^s - 1)(p^{s-1})} \alpha^c
= \alpha^c
\]

implies that the polynomial \( M_{ck}(x) \) has at most \( s \) roots. Q.E.D.
**Corollary.** The polynomial \( M_{(p+1)k}(x) \) has degree one for any positive integer \( k \).

**Proof.** In Theorem 8, let \( m = 2 \) and \( s = 1 \); then the corollary follows from the theorem.

From the above corollary, we know that for \( m = 2 \) there may exist some nonprimitive Berlekamp codes which have more than \( n - 2t \) information symbols. In Table I, such codes are marked by the superscript \( a \).

6. Conclusions

A necessary and sufficient condition has been established for a symmetric, memoryless channel to be matched to the Lee metric. This channel model can be used in evaluating the performance of a Lee metric code, and in practice it can be used in determining the modulation schemes for which Lee metric codes are better suited than the codes designed in other metrics such as the Hamming metric.

The bounds and properties of codes included in this paper are applicable to general linear Lee metric codes (group codes). The cyclic and negacyclic codes described in this paper were all defined over \( GF(p) \), and the removal of this restriction could lead to other useful results.

**Acknowledgment**

The authors wish to thank the referee for his review and the proof given for distinguishing strictly matching from matching.

Received: July 20, 1970; Revised: March 22, 1971

**References**


