New class of codes, correcting errors in the Lee metric.

*A new class of Q-ary codes that correct errors in the Lee metric is described. For the received codes there is no restriction on the number of correctable errors associated with the size of the code alphabet. In addition, the resulting codes have less redundancy compared to known codes.

Viacheslav Davydov.
HSE Tikhonov Moscow Institute of Electronics and Mathematics (MIEM)
National Research University Higher School of Economics (HSE)
Moskow, Russia
v.davydov@hse.ru

I. Introduction

Lee [1] introduced the Lee metric in 1958 as an alternative to the Hamming metric for certain noisy channels. Let a positive integer m, a prime number p, a finite field $GF(p^m)$ and a set of integers $\{0, 1, 2, \ldots, p^m - 2\} \equiv M$ be given. Denote by α the primitive element of $GF(p^m) \equiv \{0, \alpha^0, \alpha^1, \ldots, \alpha^{p^m-2}\}$. Denote by M^n the set of vectors of length $n < p^m$ with elements from the set M. The number of elements of the set M is denoted by $Q = p^m - 1$. Note that for any nonzero element of the field $\gamma \in GF(p^m)$ the identity

$$\gamma^{(p^m-1)} = \gamma^{(0)} = 1 \tag{1}$$

is satisfied.

The distance in the Lee metric between two vectors $u = (u_1, u_2, \ldots, u_n) \in M^n$ and $v = (v_1, v_2, \ldots, v_n) \in M^n$ is calculated by the formula

$$d_L(u; v) = \sum_{i=1}^{n} \min \begin{Bmatrix} (u_i - v_i) & \mod Q \\ (v_i - u_i) & \mod Q \end{Bmatrix} \tag{2}$$

The weight in the Lie metric of the vector u is determined by the formula

$$w_L(u) = \sum_{i=1}^{n} \min\{u_i, Q - u_i\}$$

In [2], Chiang and Wolf derived all discrete, memoryless, symmetric channels matched to the Lee metric and investigated the general properties of Lee metric block codes.

In [3], Berlekamp introduced negacyclic codes for which the generator polynomial contains the roots $\alpha^1, \alpha^3, \ldots, \alpha^{2t-1}$. The lower bound on the minimum Lee distance of this class of codes is $2t - 1$ when $t \leq \frac{p-1}{2}$.

In [4], Roth and Siegel characterized the Lee distance properties of a class of BCH codes whose generator polynomial contains $\alpha^0, \alpha^1, \ldots, \alpha^{t-1}$ as its roots. When $t \leq \frac{p-1}{2}$ or when the code lies in $GF(p)$, the minimum Lee distance is shown to be at least $2t$. The authors also developed a decoding algorithm utilizing Euclids algorithm to correct up to $t - 1$ Lee errors. In contrast to the performance of negacyclic codes, this class of codes has twice the length of the negacyclic construction.

In [5], Byrne showed that, under certain restrictions on t, the $2t$ lower bound on the minimum Lee distance also holds for codes on a Galois ring and devised a decoding algorithm in light of a Grobner basis.

We say that the coordinate u_i of the vector u is obtained from the coordinate v_i of the vector v with increasing errors $e_i^{(+)}$, if the condition

$$(u_i - v_i) \mod Q = e_i^{(+)} \tag{3}$$

is satisfied.

The vector of increasing errors that translate the vector v into the vector u will be denoted by $e^{(+)} = (e_1^{(+)}, e_2^{(+)}, \ldots, e_n^{(+)}) \in M^n$. Determine the distance of the increasing errors in the Lie metric between the vectors $u = (u_1, u_2, \ldots, u_n) \in M^n$ and $v = (v_1, v_2, \ldots, v_n) \in M^n$ by the formula

$$d_L^+(u; v) = \sum_{i=1}^{n} (u_i - v_i) \mod Q = \sum_{i=1}^{n} e_i^{(+)} \tag{4}$$

We define the operation of adding the vectors $v = (v_1, v_2, \ldots, v_n) \in M^n$ and $e^{(+)} = (e_1^{(+)}, e_2^{(+)}, \ldots, e_n^{(+)}) \in M^n$ at which the corresponding components of these vectors are added modulo Q. Thus $v + e^{(+)} = u$, $(v_i + e_i^{(+)}) \mod Q = u_i$, $1 \leq i \leq n$.

The total number of increasing errors that translate the vector v into the vector u will be called the weight of the increasing errors of the vector $e^{(+)}$ and denoted $W_L^{(+)}(e^{(+)}) = \sum_{i=1}^{n} e_i^{(+)}$

We say that the coordinate u_i of the vector u is obtained from the coordinate v_i of the vector v with decreasing weight errors $e_i^{(-)}$ if the condition

$$(v_i - u_i) \mod Q = \sum_{i=1}^{n} e_i^{(-)} \tag{5}$$

is satisfied.

The vector of decreasing errors transforming the vector v into the vector u will be denoted by $e^{(-)} = (e_1^{(-)}, e_2^{(-)}, \ldots, e_n^{(-)}) \in M^n$ Determine the distance of reducing errors in the Lee metric between the vectors $u = (u_1, u_2, \ldots, u_n) \in M^n$ and $v = (v_1, v_2, \ldots, v_n) \in M^n$ by the formula

$$d_L^-(u;v) = \sum_{i=1}^{n}(v_i - u_i) \mod Q = \sum_{i=1}^{n} e_i^{(-)} \tag{6}$$

Define the operation of subtracting the vectors $v = (v_1, v_2, \ldots, v_n) \in M^n$ and $e^{(-)} = (e_1^{(-)}, e_2^{(-)}, \ldots, e_n^{(-)}) \in M^n$ for which the corresponding components of these vectors are subtracted modulo Q. Thus $v - e^{(-)} = u$, $(v_i - e_i^{(-)}) \mod Q = u_i$, $1 \le i \le n$.

The total number of decreasing errors that convert the vector v to the vector u will be called the weight of the error reducing vector $e^{(-)}$ and denoted by

$$W_L^{(-)}(e^{(-)}) = \sum_{i=1}^{n} e_i^-$$

Note that the equality $e_i^{(-)} + e_i^{(+)} = Q$ holds for any values of u_i,v_i. Respectively,

$$e_i^{(-)} = -e_i^{(+)} \mod Q, 1 \le i \le n$$

Then from (3) and (5) it follows that

$$e^{(-)} = -e^{(+)} \tag{7}$$

For any vectors $u = (u_1, u_2, \ldots, u_n) \in M^n$ and $v = (v_1, v_2, \ldots, v_n) \in M^n$ the equality

$$d_L^+(u;v) + d_L^-(u;v) = Qn$$

.

From (4) and (6) it follows that

$$d_L^+(u;v) = d_L^-(v;u) \tag{8}$$

II. Codes in the Lie metric over the alphabet equal to the length of the code

The set $C_L(n;t) \subset M^n$ is called a code correcting t^+ increasing errors in the Lee metric if for any pair of different vectors $u \in C_L(n;t), v \in C_L(n;t)$ is not there exists a vector $c \in M^n$ such that $d_L^+(c;v) \le t^+$ and $d_L^+(c;u) \le t^+$

We define the mapping $\mathcal{F}$ of the set M^n to the set of polynomials in the formal variable x over the field $GF(p^m)$. To do this, we associate the i-th position ($1 \le i \le n$) of the vectors of the set M^n with a non-zero element α^i of the field $GF(p^m)$. It follows from the inequality $p^m > n$ that such a comparison is possible. Define the mapping F of the vector $u = (u_1, u_2, \ldots, u_n)$ to the polynomial $u(x)$ by the rule

$$\mathcal{F}(u) \triangleq u(x) = \prod_{i=1}^{n}(x - \frac{1}{a^i})^{u_i}$$

We will call a polynomial $u(x)$ a locator polynomial for the vector u. Note that for any vectors $u, v \in M^n$ the condition $\mathcal{F}(u) \equiv \mathcal{F}(v) \equiv 1 \mod x$ holds.

Denote by $GF[x]$ the ring of polynomials in the formal variable x over the field $GF(q^m)$. Let $s(x) \in GF[x]$ be a polynomial of degree less than or equal to t, whose lowest coefficient is one.

Lemma 1. The set of words $C_L(n;t) \triangleq \{u | u \in M^n, \mathcal{F}(u) \equiv s(x) \mod x^{t+1}\}$ is the code correcting t^+ increasing errors in the Lee metric.

Evidence.

Let there be different code vectors $u \in C_L(n;t), v \in C_L(n;t)$, and different error vectors $e^{(1)} = (e_1^{(1)}, e_2^{(1)}, \ldots, e_n^{(1)}) \in M^n$ and $e^{(2)} = (e_1^{(2)}, e_2^{(2)}, \ldots, e_n^{(2)}) \in M^n$ increasing errors, the weight of each of which in the Lee metric does not exceed t^+.

Suppose the opposite, that there is a word $c \in M^n$, satisfying conditions, which can be obtained by adding the word u with the error vector $e^{(1)}$ and the word v with the error vector $e^{(2)}$. Then the following relations take place:

$$u + e^{(1)} = v + e^{(2)}$$

$$\mathcal{F}(u + e^{(1)}) = \mathcal{F}(u + e^{(1)})$$

$$\prod_{i=1}^{n}(1 - \frac{x}{a^i})^{u_i} \prod_{i=1}^{n}(1 - \frac{x}{a^i})^{e_i^{(1)}} = \prod_{i=1}^{n}(1 - \frac{x}{a^i})^{v_i} \prod_{i=1}^{n}(1 - \frac{x}{a^i})^{e_i^{(2)}} \tag{9}$$

Since $u \in C_L(n;t), v \in C_L(n;t)$ get the identity $\mathcal{F}(u) \equiv \mathcal{F}(v) \equiv s(x) \mod x^{t+1}$

Then from (9) we get

$$\prod_{i=1}^{n}(1 - \frac{x}{a^i})^{e_i^{(1)}} = \prod_{i=1}^{n}(1 - \frac{x}{a^i})^{e_i^{(2)}} \mod x^{t+1} \tag{10}$$

Notice, that

$$\deg(\mathcal{F}(e^{(1)})) \le t^+ \text{and} \deg(\mathcal{F}(e^{(2)})) \le t^+$$

Therefore, (10) is equivalent to the identity

$$\prod_{i=1}^{n}(1 - \frac{x}{a^i})^{e_i^{(1)}} = \prod_{i=1}^{n}(1 - \frac{x}{a^i})^{e_i^{(2)}} \tag{11}$$

Since the vectors $e_i^{(1)}$ and $e_i^{(2)}$ are different, expression (11) cannot be satisfied. Hence, our assumption is not true.

Proof Completed.

From (8) it follows that the code correcting t^+ increasing errors in the Lee metric is also a code that corrects t^-

reducing errors in the Lee metric. In the sequel, we call $C_L(n;t)$ a code of length n, correcting t unidirectional errors in the Lee metric. One directivity of errors in this case means that in different positions of the code word $u \in C_L(n;t)$ both increasing and decreasing errors cannot occur simultaneously.

Lemma 2.

A set of words $B_L(n;t) \stackrel{\Delta}{=} \{u | u \in C_L(n;t), w_L(u) \equiv \sigma \mod (2t+1)\}$

is a code correcting t of arbitrary errors in the Lee metric.

Evidence.

Consider the case when the two words $u \in B_L(n;t), v \in CB_L(n;t)$ have different weight in the Lee metric. Then they are at a distance in the Lie metric of at least $2t+1$. Thus, for this case, Lemma 2 is proved.

Consider the case $w_L(u) = w_L(v)$. Assume the converse that there are two words $u \in B_L(n;t), v \in B_L(n;t)$, as well as a vector of arbitrary errors $e = (e_1, e_2, \ldots, e_n) \in M^n$ for which identities

$$e + v = u, \tag{12}$$

$$w_L(e) \leq 2t \tag{13}$$

hold. With allowance for $w_L(u) = w_L(v)$ to satisfy identity (12), the vector e must contain the same number of increasing and decreasing errors. Taking into account (13), the maximum number of such errors is $t^- = t^+ = t$.

Represent the vector of multidirectional errors as the difference of the vector of increasing errors $e_1^{(+)} = (e_{11}^{(+)}, e_{12}^{(+)}, \ldots, e_{1n}^{(+)}) \in M^n$ and reducing errors $e_2^{(-)} = (e_{21}^{(-)}, e_{22}^{(-)}, \ldots, e_{2n}^{(-)}) \in M^n$. Then we obtain $e = e_1^{(+)} - e_2^{(-)}$ and equality (13) is written as

$$v + e_1^{(+)} - e_2^{(-)} = u$$

We transform the resulting equality with regard to equation (7).

$$v + e_1^{(+)} = u + e_2^{(-)} = c \in M^n \tag{14}$$

According to the conditions $u \in C_L(n;t), v \in C_L(n;t)$. Consequently, there is no vector $c \in M^n$ such that $d_L^+(c;v) \leq t+$, and $d_L^+(c;u) \leq t+$.

Thus, we obtained a contradiction with (14). Hence, our assumption is not true.

Proof Completed.

III. Codes in the Lee metric over the alphabet, less than the length of the code

Let natural numbers l and z be given, such that $lz = m$. Given a finite field $GF(p^l) \subset GF(p^m)$ and the set of integers $0, 1, 2, \ldots, p^l - 1 \equiv L$. Denote by L^n the set of vectors of length n with elements from the set L. The number of elements of the set L is denoted by $q = p^l$ Write down the condition for the code explicitly.

$$C_L(n;t) \stackrel{\Delta}{=} \{u | u \in L^n, \mathcal{F}(u) \equiv s(x) \mod x^{t+1}\}$$

$$\mathcal{F}(u) \stackrel{\Delta}{=} u(x) = \prod_{i=1}^{n}(1 - \frac{x}{a^i})^{u_i} = s(x) + f(x)x^{t+1} \tag{15}$$

Note that $C_L(n;t) \subset L^n \subset M^n$, according to Lemma 1, a code correcting $t^+ = t$ increasing errors in the Lie metric. Moreover, operations with elements of vectors are carried out modulo $Q = p^m - 1$.

We assume that for $1 \leq i \leq n, a^i \in GF(p^m)endn < p^m$. Raise the left and right sides of equation (15) to the power p^z. Since the actions are performed in the characteristic field p, we get

$$u^*(x) = (\prod_{i=1}^{n}(1 - \frac{x}{a^i})^{u_i})^{p^z} = s(x)^{p^z} + f(x)^{p^z} x^{(t+1)p^z}$$

This means that the vector $u = (u_1, u_2, \ldots, u_n)$ with elements from the set $\{0, 1, 2, \ldots, p^l - 1\} \equiv L$ transformed into the vector $u^* = (u_1^*, u_2^*, \ldots, u_n^*)$ with elements from the set $\{0, p^z, 2p^z, \ldots, (p^l - 1)p^z\} \equiv H$.

The degree of the polynomial $s(x)^{p^z}$ satisfies the inequality $deg(s(x)^{p^z}) \leq p^z t$. Thus, $s(x)^{p^z}$ polynomial of degree less than or equal to $p^z t$, whose lowest coefficient is 1. Note that $p^z(t+1) = 1 + (p^z t + p^z - 1)$. Consequently, from the statement of Lemma 1 we obtain that $C_L^*(n;t) \stackrel{\Delta}{=} \{u^* | u^* \in H, \mathcal{F}(u^*) \equiv s(x)^{p^z} \mod x^{p^z(t+1)}\}$ is a code correcting $p^z t + p^z - 1$ unidirectional errors in the Lee metric. Note that operations with elements of vectors are carried out modulo $Q = p^m - 1$.

Since for the vector $u = (u_1, u_2, \ldots, u_n) \in C_L(n;t)$ the condition

$$\sum_{i=1}^{n} u_i = \sigma \mod (2t+1)$$

is satisfied, then for the vector $u^* = (u_1^*, u_2^*, \ldots, u_n^*) \in C_L^*(n;t)$ with elements from the set $\{0, p^z, 2p^z, \ldots, (p^l - 2)p^z\} \equiv H$ condition

$$\sum_{i=1}^{n} p^z u_i = \sigma p^z \mod p^z(2t+1)$$

is satisfied.

Then, from the equality $p^z(t+1) = 1 + (p^z t + p^z - 1)$ and, according to the statement of Lemma 2, we obtain that the code

$$B_L^*(n;t) \stackrel{\Delta}{=} \{u^* | u^* \in C_L(n;t), \sum_{i=0}^{n} u_i^* = \sigma p^z \mod p^z(2t+1)\} \tag{16}$$

is a code correcting $p^z t + p^z - 1$ of arbitrary errors in the Lee metric. Note that the input alphabet of the code $B_L^*(n;t)$ is the set of numbers $\{0, p^z, 2p^z, \ldots, (p^l - 1)p^z\} \equiv H$ of power $q = p^l$, and the output alphabet is the set of numbers $\{0, 1, 2, \ldots, p^m - 2\} \equiv M$ power $Q = p^m - 1$.

Consider H as the output alphabet of the code $B_L^*(n;t)$. Let us number all elements of the alphabet $\{0, p^z, 2p^z, \ldots, (p^l - 1)p^z\}$ from 0 to $q-1$ and denote them by the symbols

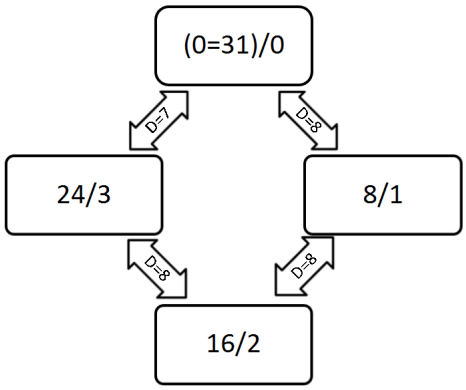

Fig. 1.

$\{h_0, h_1, \ldots, h_{q-1}\}$. For the distance $d_L(h_i; h_{i+1})$ the condition

$$\begin{cases} d_L(h_i; h_{i+1}) = p^z, & 0 \le i \le q-2, \\ d_L(h_{q-1}; h_0) = p^z - 1, & i = q-1 \end{cases}$$

is satisfied.

Thus, the distance in the Lee metric between the characters h_i and h_j, $0 \le i \le q-1$, $0 \le j \le q-1$ of the alphabet H is

$$\begin{cases} d_L(h_i; h_j) = p^z d_L(i; j), & i - j < q - i + j \\ d_L(h_{q-1}; h_0) = p^z d_L(i; j) - 1, & i - j > q - i + j \end{cases} \quad (17)$$

Consider an example of distances for $p = 2, l = 2, z = 3$. Then $q = 2^2 = 4$,$\{0, 1, 2, 3\} = L, p^z = 2^3 = 8, Q = 2^{(2+3)} - 1 = 31, \{0, 8, 16, 24\} = H$. The distances between the four elements of the alphabet H are shown in $Fig.1$.

From (17) it follows that t errors in the alphabet $\{0, 1, 2, \ldots, p^l - 1\} = L$ lead to no more than tp^z errors in the alphabet $\{0, p^z, 2p^z, \ldots, (p^l - 1)p^z\} \equiv H$ From (16) we obtain that the code $B_L^*(n; t)$ with the input and output alphabet H corrects t errors of multiplicity p^z. Thus, the code $B_L^*(n; t)$ can be considered as a code correcting t errors in the alphabet $\{0, 1, 2, \ldots, p^l - 1\} \equiv L$.

IV. Conclusion

The number of different polynomials $s(x) \in GF[x]$ with coefficients over a field $GF(p^m)$ of degree less than or equal to t, the lowest coefficient of which is one equals p^{mt}. The number of different residues modulo $(2t + 1)$ is $2t + 1$. Let code length $n = p^m - 1$. Then, for the cardinality of the code $B_L^*(n; t)$ with the incoming and outgoing alphabet $\{0, 1, 2, \ldots, p^l - 1\} = L$ of power $q = p^l$ the inequality

$$|B_L^*(n; t)| \ge \frac{q^n}{(2t + 1)(n + 1)^t} \quad (18)$$

holds.

For the power code $G(n; t)$ constructed in [3], the following estimate is valid.

$$|G(n; t)| \ge \frac{q^n}{2^t (n)^t} \quad (19)$$

For codes of [3] and [4], the restriction $t \le \frac{p-1}{2}$ should be satisfied. For the codes constructed in this paragraph, there is no such restriction.

References

[1] C. Y. Lee, Some properties of non-binary error-correcting codes, IRE Trans. Inform. Theory, vol. 4, pp. 77-82, June 1958.
[2] J. C. Chiang and J. K. Wolf, On channels and codes for the Lee metric, Inform. and Control, vol. 19, pp. 159173, Sept. 1971.
[3] E. R. Berlekamp, Algebraic Coding Theory, McGraw-Hill, New York. 1968.
[4] R. M. Roth and P. H. Siegel, Lee-metric BCH codes and their application to constrained and partialresponse channels, IEEE Trans. Inform. Theory, vol. 40, pp. 10831095, July 1994.
[5] E. Byrne, Decoding a class of Lee metric codes over a Galois ring, IEEE Trans. Inform. Theory, vol. 48, pp. 966975, Apr. 2002.