ISSN 0032-9460, Problems of Information Transmission, 2019, Vol. 55, No. 2, pp. 145–151. © Pleiades Publishing, Inc., 2019.
Russian Text © V.A. Davydov, 2019, published in Problemy Peredachi Informatsii, 2019, Vol. 55, No. 2, pp. 50–57.

CODING THEORY

On Application of the Modulus Metric to Solving the Minimum Euclidean Distance Decoding Problem

V. A. Davydov

Tikhonov Moscow Institute of Electronics and Mathematics,
National Research University—Higher School of Economics, Moscow, Russia
e-mail: novdav2017@yandex.ru

Received May 9, 2018; revised March 23, 2019; accepted April 16, 2019

Abstract—We prove equivalence of using the modulus metric and Euclidean metric in solving the soft decoding problem for a memoryless discrete channel with binary input and Q-ary output. For such a channel, we give an example of a construction of binary codes correcting t binary errors in the Hamming metric. The constructed codes correct errors at the output of a demodulator with Q quantization errors as $(t+1)(Q-1)-1$ errors in the modulus metric. The obtained codes are shown to have polynomial decoding complexity.

Key words: modulus metric, Euclidean metric, soft decoding, binary-input Q-ary output channel, codes in the modulus metric.

DOI: 10.1134/S0032946019020030

1. MODEL OF A SYMMETRIC MEMORYLESS CHANNEL WITH BINARY INPUT AND Q-ARY OUTPUT ALPHABETS

By a symmetric binary-input continuous-output channel we call a discrete-time channel with the following properties:

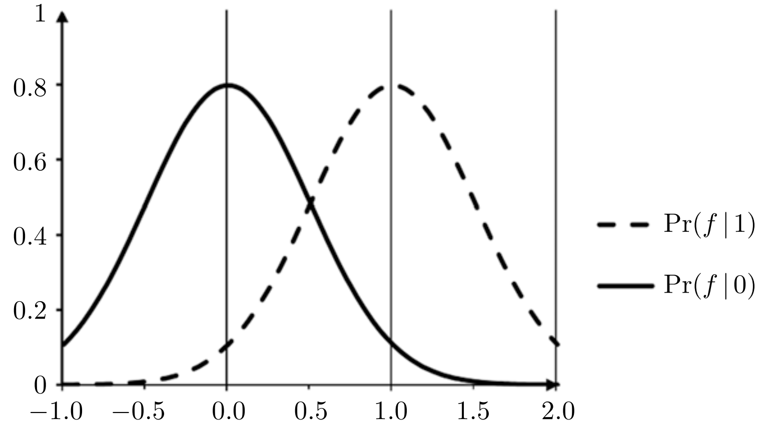
- The input alphabet $U \equiv \{0,1\}$ consists of two symbols, denoted by 0 and 1. We denote by U^n the set of length-n vectors with elements from U;
- The output alphabet F is the set of real numbers;
- An output $f \in F$ at a given time slot depends on a single input symbol;
- All outputs f satisfy the symmetry property: $\Pr(f\,|\,0) = \Pr(1-f\,|\,1)$. By $\Pr(f\,|\,x)$ we mean the distribution density of the conditional probability of receiving symbol f from the channel given that symbol $x \in U$ was transmitted.

An example of functions $\Pr(f\,|\,0)$ and $\Pr(f\,|\,1)$ is shown in the figure.

By an error vector for a codeword $\boldsymbol{u} = (u_1, u_2, \ldots, u_n)$, $u_i \in U$, of length n we mean a vector $\boldsymbol{e} = (e_1, e_2, \ldots, e_n)$, $e_i \in F$, of the same length whose corresponding elements are differences between the vector $\boldsymbol{f} = (f_1, f_2, \ldots, f_n)$ received from the channel and the transmitted word: $e_i = f_i - u_i$, $1 \le i \le n$.

Maximum likelihood decoding for a code $\boldsymbol{G} \subset U^n$ means the following [1]: for a given received vector $\boldsymbol{f}$, find a codeword $\boldsymbol{u} \in \boldsymbol{G}$ which maximizes the probability that $\boldsymbol{u}$ was transmitted given that $\boldsymbol{f}$ was received: $P(\boldsymbol{u}\,|\,\boldsymbol{f}) \to \max$. An additive white Gaussian noise memoryless channel is compatible with the Euclidean metric. The maximum likelihood decoding in this case consists in finding a vector $\boldsymbol{u} = (u_1, u_2, \ldots, u_n) \in \boldsymbol{G}$ which is at the smallest Euclidean distance from the received vector $\boldsymbol{f} = (f_1, f_2, \ldots, f_n)$.

In [2], the soft decoding problem for a binary-input Q-ary output channel was considered. In this problem setting, values of components of a vector $\boldsymbol{f} = (f_1, f_2, \ldots, f_n)$ remain to be real but



Example of the functions $\Pr(f\,|\,0)$ and $\Pr(f\,|\,1)$ versus f.

may take a finite number of values, which will be referred to as an output alphabet. The output alphabet size is determined by the number of quantization levels of an output matched filter. A quantization scheme with $Q = 8$ is often used in soft decision decoding systems. As was noted in [2], the behavior of such a system is close to that obtained under infinitely many quantization levels. The maximum likelihood decoding for a quantized channel also consists in finding a vector $\boldsymbol{u} = (u_1, u_2, \ldots, u_n) \in \boldsymbol{G}$ which is at the smallest Euclidean distance from the received vector $\boldsymbol{f} = (f_1, f_2, \ldots, f_n)$.

Real-world communication systems, as is noted in [2], use not the real values of the components f_i but numbers indicating a quantization level $v_i \in \{0, 1, \ldots, Q-1\}$ that corresponds to f_i. As a result, to a vector $\boldsymbol{f} = (f_1, f_2, \ldots, f_n)$ there corresponds a Q-ary vector $\boldsymbol{v} = (v_1, v_2, \ldots, v_n)$. Thus, we have obtained a description of a discrete binary-input channel with a Q-ary output alphabet. This channel is completely described by a set of transition probabilities $\Pr(j\,|\,x)$, where $\Pr(j\,|\,x)$ is the conditional probability that the output symbol is j given that the input symbol is x. We assume that the channel is symmetric and $\Pr(j\,|\,0) = \Pr(Q-1-j\,|\,1)$.

If a binary vector $\boldsymbol{u} = (u_1, u_2, \ldots, u_n) \in U^n$ was transmitted through the channel, the probability that a vector $\boldsymbol{v} = (v_1, v_2, \ldots, v_n)$ was received is computed as

$$\Pr(\boldsymbol{v}\,|\,\boldsymbol{u}) = \prod_{i=1}^{n} \Pr(v_i\,|\,u_i).$$

By taking the logarithm, we obtain

$$\log(\Pr(\boldsymbol{v}\,|\,\boldsymbol{u})) = \sum_{i=1}^{n} \log(\Pr(v_i\,|\,u_i)). \tag{1}$$

A decoder has to maximize the value of $\Pr(\boldsymbol{v}\,|\,\boldsymbol{u})$, which is maximal when the negative sum on the right-hand side of (1) is minimal. In [2] an approximating expression for (1) was introduced, which is more convenient for computing the distance in soft decoding and which is called the symbol metric. The corresponding values in this metric are defined to be $m_j = -A - B\log(\Pr(j\,|\,0))$. The constants A and B are chosen in such a way that the minimum value of m_j is zero and the others are positive.

The scheme with $m_j = j$ is used most often. If the number of levels is Q, the metric assumes only values in the set $\{0, 1, 2, \ldots, Q-1\}$. As is noted in [2], this choice of a metric well describes many decoders used in practice.

In what follows we will only consider channels compatible with the Euclidean metric defined via their transition probabilities. Thus, the maximum likelihood decoding problem is used by finding a nearest (in the Euclidean metric) codeword to the received vector.

2. INTERRELATION BETWEEN THE MODULUS AND EUCLIDEAN METRICS IN A CHANNEL WITH BINARY INPUT AND Q-ARY OUTPUT ALPHABETS

Consider the channel from Section 1 with $Q = 2^z + 1$. Let a set of binary code vectors $\boldsymbol{G} \subset U^n$ used for the transmission through the channel be fixed.

A binary vector $\boldsymbol{u} = (u_1, u_2, \ldots, u_n) \in \boldsymbol{G}$ with elements from $\{0, 1\}$ in the situation with $Q = 2^z + 1$ quantization levels and no errors in the channel is considered by a demodulator as a binary vector $\boldsymbol{v}^* = (v_1, v_2, \ldots, v_n) \in \boldsymbol{G}^*$ with elements $v_i \in \{0, 2^z\} \triangleq \boldsymbol{H}$. Thus, the set $\boldsymbol{G}$ of words in the binary alphabet $\{0, 1\}$ will be considered by the demodulator as a set $\boldsymbol{G}^*$ of binary words in the binary alphabet $\{0, 2^z\}$.

When channel errors affect a vector $\boldsymbol{u}^* = (u_1^*, u_2^*, \ldots, u_n^*)$, the output of the demodulator is a Q-ary vector $\boldsymbol{y}^* = (y_1, y_2, \ldots, y_n)$ with elements in $\{0, 1, 2, \ldots, 2^z\} \triangleq \boldsymbol{Z}$. Denote by $\boldsymbol{Z}^n$ the set of length-n vectors with elements from $\boldsymbol{Z}$.

The maximum likelihood decoding problem for a code $\boldsymbol{G}^*$ with $2^z + 1$ sublevels in a memoryless channel under Gaussian noise is solved by finding a codeword $\boldsymbol{v}^* = (v_1, v_2, \ldots, v_n) \in \boldsymbol{G}^*$ nearest to the received vector $\boldsymbol{y}^* = (y_1, y_2, \ldots, y_n) \in \boldsymbol{Z}^n$ with respect to the Euclidean distance

$$d_E(\boldsymbol{y}^*; \boldsymbol{v}^*) = \sqrt{\sum_{i=1}^{n} (y_i - v_i)^2}. \tag{2}$$

The distance $d_M(\boldsymbol{u}; \boldsymbol{v})$ in the modulus metric between vectors $\boldsymbol{u} = (u_1, u_2, \ldots, u_n) \in \boldsymbol{Z}^n$ and $\boldsymbol{v} = (v_1, v_2, \ldots, v_n) \in \boldsymbol{Z}^n$ is

$$d_M(\boldsymbol{u}; \boldsymbol{v}) = \sum_{i=1}^{n} |u_i - v_i|. \tag{3}$$

The weight $w_M(\boldsymbol{u})$ of a vector $\boldsymbol{u} = (u_1, u_2, \ldots, u_n)$ in the modulus metric is defined as the distance $d_M(\boldsymbol{u}; \boldsymbol{0})$, where $\boldsymbol{0}$ is the all-zero vector of length n. If $d_M(\boldsymbol{u}; \boldsymbol{v}) = t$, we will say that $\boldsymbol{u} = (u_1, u_2, \ldots, u_n)$ is obtained from $\boldsymbol{v} = (v_1, v_2, \ldots, v_n)$ by an error of multiplicity t.

Let us introduce a partial order relation on the set $\boldsymbol{Z}^n$ of vectors of length n. We define $\boldsymbol{u} \gg \boldsymbol{v}$ if for all $1 \le i \le n$ we have $v_i \le u_i$. If the last inequality does not hold for all $1 \le i \le n$, we say that $\boldsymbol{u}$ and $\boldsymbol{v}$ are incomparable. Let $d_M(\boldsymbol{u}; \boldsymbol{v}) = t$ and $\boldsymbol{u} \gg \boldsymbol{v}$. Then we say that $\boldsymbol{u}$ is obtained from $\boldsymbol{v}$ by t one-way increasing errors. One-way decreasing errors are defined similarly.

Denote by $\boldsymbol{J}$ the set of vectors of length n with components from the set $\{0, 1, 2, \ldots, 2^z\}$. For the cardinality of $\boldsymbol{J}$, we have $|\boldsymbol{J}| = (2^z + 1)^n$.

Let $\boldsymbol{u}^*$ and $\boldsymbol{v}^*$ be vectors of length n with components belonging to $\{0, 2^z\} = \boldsymbol{H}$. Denote by $\boldsymbol{W}$ the set of all such vectors. Note that for the cardinality of this set we have $|\boldsymbol{W}| = 2^n$. In fact, vectors from $\boldsymbol{W}$ are vertices of an n-cube, and $\boldsymbol{y}^*$ is an arbitrary point of this cube. For a code $\boldsymbol{B}^*$ and the sets $\boldsymbol{W}$ and $\boldsymbol{J}$, we have $\boldsymbol{B}^* \subset \boldsymbol{W} \subset \boldsymbol{J}$.

Theorem. *For any vector $\boldsymbol{y}^* = (y_1, y_2, \ldots, y_n) \in \boldsymbol{J}$ and any pair of vectors $\boldsymbol{u}^* \in \boldsymbol{W}$ and $\boldsymbol{v}^* \in \boldsymbol{W}$ we have*

$$d_E^2(\boldsymbol{y}^*; \boldsymbol{v}^*) - d_E^2(\boldsymbol{y}^*; \boldsymbol{u}^*) = 2^z(d_M(\boldsymbol{y}^*; \boldsymbol{v}^*) - d_M(\boldsymbol{y}^*; \boldsymbol{u}^*)). \tag{4}$$

Proof. Consider the vectors $\boldsymbol{u}^* \in \boldsymbol{W}$ and $\boldsymbol{v}^* \in \boldsymbol{W}$. Note that the set of positions where these vectors coincide has no effect on the identity (4). Thus, we will only consider positions where these vectors differ. Without loss of generality, let us assume that the first ℓ positions of $\boldsymbol{u}^*$ contain symbol 2^z, and the next m positions contain 0. Accordingly, the first ℓ positions of $\boldsymbol{v}^*$ contain 0, and the next m positions contain 2^z. The remaining $n-\ell-m$ positions of these vectors coincide, so we ignore them in what follows. Then, according to (2), for the left-hand side of (4) we have

$$\begin{aligned} &d_E^2(\boldsymbol{y}^*;\boldsymbol{v}^*) - d_E^2(\boldsymbol{y}^*;\boldsymbol{u}^*) \\ &\quad = \left(\sum_{i=1}^{\ell} y_i^2 + m2^{2z} - 2^{z+1}\sum_{i=\ell+1}^{\ell+m} y_i + \sum_{i=\ell+1}^{\ell+m} y_i^2\right) - \left(\sum_{i=1}^{\ell} y_i^2 + \ell 2^{2z} - 2^{z+1}\sum_{i=1}^{\ell} y_i + \sum_{i=\ell+1}^{\ell+m} y_i^2\right) \\ &\quad = 2^z\left(\left(m2^z - 2\sum_{i=\ell+1}^{\ell+m} y_i\right) - \left(\ell 2^z - 2\sum_{i=1}^{\ell} y_i\right)\right). \end{aligned} \tag{5}$$

Now consider the right-hand side of (4) in the modulus metric. By virtue of (3), we obtain

$$\begin{aligned} d_M(\boldsymbol{y}^*;\boldsymbol{v}^*) - d_M(\boldsymbol{y}^*;\boldsymbol{u}^*) &= \sum_{i=1}^{\ell} y_i + m2^{2z} - \sum_{i=\ell+1}^{\ell+m} y_i - \left(-\sum_{i=1}^{\ell} y_i + \ell 2^z + \sum_{i=\ell+1}^{\ell+m} y_i\right) \\ &= \left(m2^z - 2\sum_{i=\ell+1}^{\ell+m} y_i\right) - \left(\ell 2^z - 2\sum_{i=1}^{\ell} y_i\right). \end{aligned} \tag{6}$$

Comparing (5) and (6) proves the validity of identity (4). △

Corollary. *For any vector* $\boldsymbol{y}^* = (y_1, y_2, \ldots, y_n) \in \boldsymbol{J}$ *and any pair of vectors* $\boldsymbol{u}^* \in \boldsymbol{W}$ *and* $\boldsymbol{v}^* \in \boldsymbol{W}$ *we have the following equivalence of inequalities*:

$$d_E(\boldsymbol{y}^*;\boldsymbol{v}^*) > d_E(\boldsymbol{y}^*;\boldsymbol{u}^*) \iff d_M(\boldsymbol{y}^*;\boldsymbol{v}^*) > d_M(\boldsymbol{y}^*;\boldsymbol{u}^*). \tag{7}$$

Proof. Assume that for a vector $\boldsymbol{y}^* = (y_1, y_2, \ldots, y_n) \in \boldsymbol{J}$ and any pair of vectors $\boldsymbol{u}^* \in \boldsymbol{W}$ and $\boldsymbol{v}^* \in \boldsymbol{W}$ we have

$$d_E(\boldsymbol{y}^*;\boldsymbol{v}^*) > d_E(\boldsymbol{y}^*;\boldsymbol{u}^*).$$

Then squaring both sides of the inequality does not change the inequality sign; i.e., we have

$$d_E^2(\boldsymbol{y}^*;\boldsymbol{v}^*) > d_E^2(\boldsymbol{y}^*;\boldsymbol{u}^*).$$

This follows from the fact that the set $\{0, 1, 2, \ldots, 2^z\}$ containing all components of $\boldsymbol{u}^*$, $\boldsymbol{v}^*$, and $\boldsymbol{y}^*$ consists of nonnegative integers.

Now we divide both sides of the obtained inequality by 2^z. We obtain an inequality with the same inequality sign

$$\frac{d_E^2(\boldsymbol{y}^*;\boldsymbol{v}^*)}{2^z} > \frac{d_E^2(\boldsymbol{y}^*;\boldsymbol{u}^*)}{2^z},$$

which implies

$$\frac{d_E^2(\boldsymbol{y}^*;\boldsymbol{v}^*)}{2^z} - \frac{d_E^2(\boldsymbol{y}^*;\boldsymbol{u}^*)}{2^z} > 0. \tag{8}$$

Identity (4) proved above implies that (8) is equivalent to the inequality

$$d_M(\boldsymbol{y}^*;\boldsymbol{v}^*) - d_M(\boldsymbol{y}^*;\boldsymbol{u}^*) > 0.$$

Thus, the desired equivalence (7) is proved. △

If a vector $\boldsymbol{y}^* = (y_1, y_2, \ldots, y_n) \in \boldsymbol{J}$ is received, maximum likelihood soft decoding of a code $\boldsymbol{B}^*$ using 2^z+1 sublevels for a memoryless white Gaussian noise channel is performed by finding a word $\boldsymbol{v}^* = (v_1, v_2, \ldots, v_n) \in \boldsymbol{W} \subset \boldsymbol{J}$ nearest to the received word $\boldsymbol{y}^*$ in the Euclidean metric which at the same time is a codeword of $\boldsymbol{B}^* \in \boldsymbol{W}$.

Taking into account the above-proved equivalence (7), we conclude that it is possible to use the modulus metric in soft decoding instead of the Euclidean metric. The result of such decoding will not change.

3. CODES IN THE MODULUS METRIC

A set $\boldsymbol{G}(n,t) \subset \boldsymbol{Z}^n$ is said to be a code correcting t one-way increasing errors if for any pair of distinct vectors $\boldsymbol{u} \in \boldsymbol{G}(n,t)$ and $\boldsymbol{v} \in \boldsymbol{G}(n,t)$ there is no vector $\boldsymbol{c}$ such that $\boldsymbol{c} \gg \boldsymbol{u}$, $\boldsymbol{c} \gg \boldsymbol{v}$, $d_M(\boldsymbol{c};\boldsymbol{v}) \le t$, and $d_M(\boldsymbol{c};\boldsymbol{u}) \le t$.

Choose a finite field $GF(q^m)$, where q is a prime, m is a positive integer, and the inequality $q^m > n$ holds. Let α be a primitive element of the field. Define a mapping $\mathcal{F}$ from $\boldsymbol{Z}^n$ to the set of polynomials in a formal variable x over $GF(q^m)$. To this end, to the ith position $(1 \le i \le n)$ of vectors of $\boldsymbol{Z}^n$ we put into correspondence the nonzero element α^i of $GF(q^m)$. The inequality $q^m > n$ implies that this correspondence is well defined. Now define a mapping $\mathcal{F}$ taking a vector $\boldsymbol{u} = (u_1, u_2, \ldots, u_n)$ to a polynomial $u(x)$ according to the rule

$$\mathcal{F}(\boldsymbol{u}) \triangleq u(x) = \prod_{i=1}^{n} \Bigl(1 - \frac{x}{\alpha^i}\Bigr)^{u_i}.$$

Note that for any vectors $\boldsymbol{u}, \boldsymbol{v} \in \boldsymbol{Z}^n$ we have $\mathcal{F}(\boldsymbol{u}) \equiv \mathcal{F}(\boldsymbol{v}) \equiv 1 \bmod x$.

Denote by $GF[x]$ the ring of polynomials in a formal variable x over $GF(q^m)$. Let $s(x) \in GF[x]$ be a polynomial of degree no greater than t with lowest-degree coefficient 1. In [3] it is proved that the set

$$\boldsymbol{C} \triangleq \{\boldsymbol{u} \mid \boldsymbol{u} \in \boldsymbol{Z}^n,\ \mathcal{F}(\boldsymbol{u}) \equiv s(x) \bmod x^{t+1}\} \tag{9}$$

is a code correcting t one-way increasing errors in the modulus metric. It is proved in [3] that a code $\boldsymbol{C}$ correcting t one-way increasing errors in the modulus metric also corrects t one-way decreasing errors. It is also proved in [3] that for any $0 \le \sigma \le 2t$ the subset

$$\boldsymbol{B} \triangleq \Bigl\{\boldsymbol{u} \Bigm| \boldsymbol{u} \in \boldsymbol{C},\ \sum_{i=1}^{n} u_i \equiv \sigma \bmod (2t+1)\Bigr\} \subset \boldsymbol{C} \tag{10}$$

is a code correcting t arbitrary errors in the modulus metric. Along with code constructions, in [4] there was also proposed a polynomial-complexity decoding algorithm for such codes based on solving the key equation by the Euclidean method.

4. USING CODES IN THE MODULUS METRIC FOR SOFT DECODING IN A CHANNEL WITH BINARY INPUT AND Q-ARY OUTPUT ALPHABETS

Let binary vectors $\boldsymbol{u} \in 2^n$ and $\boldsymbol{v} \in 2^n$ be given. Denote by $d_H(\boldsymbol{u};\boldsymbol{v})$ the distance between these vectors in the Hamming metric. Then for any vectors $\boldsymbol{u}$ and $\boldsymbol{v}$ we have the identity

$$d_M(\boldsymbol{u};\boldsymbol{v}) = d_H(\boldsymbol{u};\boldsymbol{v}).$$

Consider the set of words

$$\boldsymbol{C} \triangleq \{\boldsymbol{u} \mid \boldsymbol{u} \in 2^n,\ \mathcal{F}(\boldsymbol{u}) \equiv s(x) \bmod x^{t+1}\}.$$

Then the subset

$$\boldsymbol{B} \triangleq \left\{\boldsymbol{u} \;\middle|\; \boldsymbol{u} \in \boldsymbol{C},\ \sum_{i=1}^{n} u_i \equiv \sigma \bmod 2(t+1)\right\} \subset \boldsymbol{C}$$

is a binary code correcting t errors in both the Hamming metric and modulus metric.

We will construct a soft decoding scheme for $\boldsymbol{B}$. Let us explicitly write the condition for $\boldsymbol{C}$:

$$\mathcal{F}(\boldsymbol{u}) \triangleq u(x) = \prod_{i=1}^{n}\left(1-\frac{x}{\alpha^i}\right)^{u_i} = s(x) + f(x)x^{t+1}. \tag{11}$$

We will assume that $n < 2^m$ and $\alpha^i \in GF(2^m)$ for $1 \le i \le n$. Let the decoder have $Q = 2^z + 1$ sublevels. In other words, at the output of the demodulator, for each symbol of the code a decision belonging to $\{0, 1, 2, \dots, 2^z\}$ is made.

Now we rise both side of equation (11) to the power 2^z. Since operations are made in a filed of characteristic 2, we obtain

$$u^*(x) = \left(\prod_{i=1}^{n}\left(1-\frac{x}{\alpha_i}\right)^{u_i}\right)^{2^z} = s(x)^{2^z} + f(x)^{2^z}x^{(t+1)2^z}.$$

This means that the binary vector $\boldsymbol{u} = (u_1, u_2, \dots, u_n) \in \boldsymbol{C}$ with elements from $\{0, 1\}$ was transformed to a binary vector $\boldsymbol{u}^* = (u_1^*, u_2^*, \dots, u_n^*)$ with elements from the set $\{0, 2^z\} = \boldsymbol{H}$.

Note that the degree of the polynomial $s(x)^{2^z}$ satisfies the inequality $\deg(s(x)^{2^z}) \le 2^z t$. Thus, $s(x)^{2^z}$ is a polynomial of degree no greater than $2^z t$ with lowest-degree coefficient 1.

Note that $2^z(t+1) = 1 + (2^z t + 2^z - 1)$. Therefore, from (9) we obtain that

$$\boldsymbol{C}^* \triangleq \{\boldsymbol{u}^* \mid \boldsymbol{u}^* \in \boldsymbol{H}^n,\ \mathcal{F}(\boldsymbol{u}^*) \equiv s(x)^{2^z} \bmod x^{2^z(t+1)}\}$$

is a code correcting $2^z t + 2^z - 1$ one-way increasing errors in the modulus metric if a single error is understood as a change by one level in the level set $\{0, 1, 2, \dots, 2^z\}$ in one of the n symbols of a vector $\boldsymbol{u}^* = (u_1^*, u_2^*, \dots, u_n^*)$.

If for a vector $\boldsymbol{u} = (u_1, u_2, \dots, u_n) \in \boldsymbol{C}$ we have

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

then for the vector $\boldsymbol{u}^* = (u_1^*, u_2^*, \dots, u_n^*) \in \boldsymbol{C}^*$ with elements in the set $\{0, 2^z\} = \boldsymbol{H}$ we have

$$\sum_{i=1}^{n} 2^z u_i \equiv \sigma 2^z \bmod (2^z(2t+1)).$$

Then from the equality $2^z(t+1) = 1 + (2^z t + 2^z - 1)$, taking into account (10), we conclude that

$$\boldsymbol{B}^* \triangleq \left\{\boldsymbol{u}^* \;\middle|\; \boldsymbol{u}^* \in \boldsymbol{C}^*,\ \sum_{i=0}^{n} u_i^* \equiv \sigma 2^z \bmod (2^z(2t+1))\right\} \subset \boldsymbol{C}^*$$

is a code correcting $2^z t + 2^z - 1$ arbitrary errors in the modulus metric if a single error is understood as a change by one level in the level set $\{0, 1, 2, \dots, 2^z\}$ in one of the n symbols of $\boldsymbol{u}^* = (u_1^*, u_2^*, \dots, u_n^*)$.

The algebraic structure of the obtained code$\boldsymbol{B}^*$ can be used together with the algorithm from [4] for finding (with polynomial complexity) a part of errors corrected by the code $\boldsymbol{B}^*$ in the modulus metric up to its designed distance $1 + (2^z t + 2^z - 1)$. Finding all other errors corrected by $\boldsymbol{B}^*$ in the modulus metric yields maximum likelihood soft decoding for the binary-input code $\boldsymbol{B}^*$ with an output alphabet of $Q = 2^z + 1$ symbols.

REFERENCES

1. Kolesnik, V.D. and Mironchikov, E.T., *Dekodirovanie tsiklicheskikh kodov* (Decoding of Cyclic Codes), Moscow: Svyaz', 1968.

2. Clark, G.C., Jr., and Cain, J.B., *Error-Correction Coding for Digital Communications*, New York: Plenum, 1981. Translated under the title *Kodirovanie s ispravleniem oshibok v sistemakh tsifrovoi svyazi*, Moscow: Radio i svyaz', 1987.

3. Davydov, V.A., Codes Correcting Errors in the Modulus Metric, Lee Metric, and Operator Errors, *Probl. Peredachi Inf.*, 1993, vol. 29, no. 3, pp. 10–20 [*Probl. Inf. Transm.* (Engl. Transl.), 1993, vol. 29, no. 3, pp. 208–216].

4. Davydov, V.A., Methods for Error Correction in the Modulus Metric and Derived Metrics, *Cand. Sci. (Engrg.) Dissertation*, St. Petersburg, 1993.