Journal of Information Security, 2014, 5, 178-191
Published Online October 2014 in SciRes. http://www.scirp.org/journal/jis
http://dx.doi.org/10.4236/jis.2014.54017

Scientific Research

On the Matrix and Additive Communication Channels

Vladimir Leontiev[1], Garib Movsisyan[2], Arthur Osipyan[1], Zhirayr Margaryan[3]

[1]Moscow State University, Moscow, Russia
[2]BIT Group, Moscow, Russia
[3]Yerevan State University, Yerevan, Armenia
Email: vkleontiev@yandex.ru, garib@firmbit.ru, osipyan.arthur.a@gmail.com, jiromr@mail.ru

Received 21 July 2014; revised 20 August 2014; accepted 13 September 2014

Copyright © 2014 by authors and Scientific Research Publishing Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY).
http://creativecommons.org/licenses/by/4.0/
Open Access

Abstract

The notion of a communication channel is one of the key notions in information theory but like the notion "information" it has not any general mathematical definition. The existing examples of the communication channels: the Gaussian ones; the binary symmetric ones; the ones with symbol drop-out and drop-in; the ones with error packets etc., characterize the distortions which take place in information conducted through the corresponding channel.

Keywords

Additive Communication Channel, Error, Matrix Channel, Neighborhood, Correcting Code, Alphabet

1. Introduction

We confine our discussion to the following situation.

Let $B=\{0,1\}$ be a binary alphabet and B^* be the set of all words with finite length in the alphabet, B. We take the dictionary function as the following partial mapping:

$$B^* \to B^*.$$

Saying a communication channel, we mean an arbitrary multi-valued mapping, having the following form:

$$\Psi(x)=\{\Psi_0(x),\Psi_1(x),\cdots,\Psi_m(x)\}, \quad (1)$$

where $\Psi_i(x)$, $i=\overline{0,m}$ is some dictionary function.

As to the content, equality (1) means that when the word x is transferred we have one of the words $\Psi_i(x)$

How to cite this paper: Leontiev, V., Movsisyan, G., Osipyan, A. and Margaryan, Z. (2014) On the Matrix and Additive Communication Channels. *Journal of Information Security*, **5**, 178-191. http://dx.doi.org/10.4236/jis.2014.54017

at the exit.

Below we take $\Psi_0(x) = x$ without any loss of generality.

We denote the set of all binary words with the length n by B^n; below the terms, "a word" and "a Boolean vector" are synonyms.

Example.

1) Mapping (1) is called a standard communication channel if it has a limited number of distortions of the form: $0 \to 1$, $1 \to 0$, where

$$\Psi_k(x) = x \oplus v_k.$$

Besides, we say that there are no more than t errors in the channel if $\|v_k\|$ does not exceed t. (Here $\|v_k\|$ is Hamming weight of the word v_k). On the other hand, the following holds:

$$\Psi(x) = \{\Psi_0(x), \Psi_1(x), \cdots, \Psi_m(x)\},$$

where $m = \sum_{i=0}^{t} \binom{n}{i}$ is the cardinality of the sphere with the radius t in B^n.

The notion of the code that corrects the errors of the channel Ψ is completely analogous to the classic definition of the code, correcting the distortions of the form: $0 \to 1$, $1 \to 0$.

Definition 1. The code $V = \{v_0, v_1, \cdots, v_N\}$ corrects the errors of the channel:

$\Psi(x) = \{\Psi_0(x), \Psi_1(x), \cdots, \Psi_m(x)\}$, if the following is valid:

$$\Psi_p(v_i) \neq \Psi_q(v_j) \tag{2}$$

for i, $j = \overline{0, N}$; p, $q = \overline{0, m}$.

Condition (2) means that consequences of errors are different; hence we can restore one to one the initial information at the exit. The decision process at the exit usually is formalized in the form of the "decoding table" [1]:

v_0	$v_1 \cdots$	v_N
$\Psi_0(v_0)$	$\Psi_0(v_1)$	$\Psi_0(v_N)$
$\Psi_1(v_0)$	$\Psi_1(v_1)$	$\Psi_1(v_N)$
$\vdots$	$\vdots$	$\vdots$
$\Psi_m(v_0)$	$\Psi_m(v_1)$	$\Psi_m(v_N)$

Error "correction" through the table takes place as follows. According to definition, every "transferred" word x is transformed by the channel Ψ into $\Psi_i(x) = y$, which is at least in one of the columns of the table.

Then the code vector in the first row of any row is the "prototype" of the transferred word.

It is clear that if the word y belongs to the only one of the columns in the table, then the "decoding" process leads to a right result.

Condition (2) can be formulated in a little different way using the notion of "neighborhood" which gives certain advantage when making estimates of the cardinality of the correcting code.

The neighborhood of the k *th* order of the word $x \in B^n$ built up with respect to the set:

$$\Psi_k(x) = \{\Psi_0(x), \Psi_1(x), \cdots, \Psi_m(x)\},$$

Is formed by the following induction:

$$\Psi^0(x) = x,\ \Psi^1(x) = \{\Psi_i(x) : i = \overline{0, m}\},\ \cdots,\ \Psi^k(x) = \{\Psi_i(y) : y \in \Psi^{k-1}(x),\ i = \overline{0, m}\} \tag{3}$$

Condition (3) shows that the neighborhood of the k *th* order of the word $x \in B^n$ is the union of the neighborhood of the 1st order of all words belonging to the neighborhood of the $(k-1)$ *th* order of the word x.

In the term of the neighborhood condition (2) of error correction takes the following form:

$$\Psi^1(v_i) \cap \Psi^1(v_j) = \varnothing, \quad \text{if} \quad i \neq j \tag{4}$$

We denote by $V(\Psi)$ the code correcting the errors of the channel Ψ.

In the terms of the above introduced notions for the given channel Ψ the problem is to build the code of the maximum cardinality $\overline{V}(\Psi)$.

It is obvious that this cardinality depends on the "structure" of Ψ.

Among the codes $V(\Psi)$ the so called perfect codes are of special interest.

Definition 2. The code $V(\Psi)$ is called perfect if:

$$\bigcup_{v_i \in V(\Psi)} \Psi^1(v_i) = B^n$$

Definition 3 [2]. The channel $\Psi(x) = \{\Psi_0(x), \Psi_1(x), \cdots, \Psi_m(x)\}$ is called algebraic if:

$\Psi_i^{-1}(x) \in \Psi(x)$, for all $i = \overline{0,m}$.

Assume that for all $i = \overline{0,m}$, that if $x \in B^n$, then $\Psi_i(x) \in B^n$.

We consider the graph (B^n, E_Ψ), adjacency of the vertices are defined as follows. The vertices $x, y \in B^n$ are adjacent iff there exists a Ψ_i satisfying the condition $y = \Psi_i(x)$ or $x = \Psi_i(y)$. The distance on the graph (B^n, E_Ψ) between any vertices $x, y \in B^n$ is the minimum number of the arcs in the chain connecting the vertices x, y and the infinity if there does not exist such a chain.

It is not difficult to prove the following condition. In the graph (B^n, E_Ψ) the distance between any two vertices from $V \subseteq B^n$ no less than three it is necessary and sufficient that V be an error correcting code of the algebraic channel Ψ.

Further we discuss a special but having certain interest type of communication channel which is carried out by linear mappings, $\Psi_k(x)$.

2. Matrix Channels [3]

Let $F_2 = \{0,1\}$ be a finite field of two elements and $M_{p,g}$ be the set of matrices of the order $(p \times g)$ with the elements belonging to the field F_2 with the usual operations of addition and multiplication for $p = g$. If $M = \{M_0, M_1, \cdots, M_m\}$ then the set M, defines a matrix channel in the sense of (1):

$$\Psi(x) = \{xM_0, xM_1, \cdots, xM_m\}.$$

Examples.

2) Let such "errors" take place in a "real" channel, which are connected with wrong reading of adjacent letters of the transferred vector, $x = (x_1 x_2 \cdots x_n)$; and this means the following transformation:

$$x_i x_{i+1} \to x_{i+1} x_i, \quad i = \overline{1, n-1}.$$

This situation can be modelized by the matrix channel $M = \{M_0, \cdots, M_{n-1}\} \subseteq M_{n,n}$ where M_0 is the unit matrix:

$$M_1 = \begin{Vmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{Vmatrix}, \; M_2 = \begin{Vmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{Vmatrix}, \; \cdots, \; M_{n-1} = \left\| \begin{array}{c|cccc} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & 1 \\ 0 & 0 & 0 & \cdots & 1 \end{array} \right\|,$$

Indeed, when transferring $x = (x_1 x_2 \cdots x_n)$ through the channel we have a vector of the following form at the exit:

$$xM_i = (x_1 x_2 \cdots x_{i-1} x_{i+1} x_i x_{i+2} \cdots x_n),$$

where $1 \le i \le n-1$.

3) if a "drop-out" of symbols takes place in the channel, *i.e.* the length of the word is changed, then it can be presented in the matrix form as follows. Let $x = (x_1 x_2 \cdots x_n)$ is the initial word in which just one symbol can be lost. We discuss the following set of matrices belonging to $M_{n-1,n}$:

$$M_1 = \begin{Vmatrix} 0 & 0 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{Vmatrix}, \; M_2 = \begin{Vmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{Vmatrix}, \; \cdots, \; M_{n-1} = \begin{Vmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{Vmatrix},$$

Then:

$$xM_1 = (x_2 x_3 \cdots x_n), \; xM_2 = (x_1 x_3 \cdots x_n), \; \cdots, \; xM_n = (x_1 x_2 \cdots x_{n-1}).$$

The notion of the code that corrects the errors of the matrix channel M is completely analogous to the classic definition of the code, correcting the distortions of the form: $0 \to 1$, $1 \to 0$.

Definition 4. The code $V = \{v_0, v_1, \cdots, v_N\}$ corrects the errors of the channel $\Psi(x) = \{\Psi_0(x), \Psi_1(x), \cdots, \Psi_m(x)\}$ if the following condition is valid:

$$\Psi_p(v_i) \neq \Psi_q(v_j)$$

for all i, $j = \overline{0, N}$; and p, $q = \overline{0, m}$.

The neighborhood of the k *th* order of the word $x \in B^n$ built with respect to the set $M = \{M_0, M_1, \cdots, M_m\}$, is defined as in (3):

$$M^0(x) = x, \; M^1(x) = \{xM_i : M_1 \in M\}, \; \cdots, \; M^k(x) = \{yM_i : y \in M^{k-1}(x), \; M_i \in M\}.$$

In the terms of neighborhood the error correction condition becomes as follows:

$$M^1(v_i) \cap M^1(v_j) = \varnothing, \quad \text{if} \quad i \neq j.$$

3. The Group Matrix Channels

Let $GL_2(n)$ be the group of the non-degenerated matrices of the order n on the field F_2 and G be the subgroup of $GL_2(n)$. We discuss the matrix channel generated by the subgroup:

$$G = \{M_0, M_1, \cdots, M_m\},$$

where m is a divisor of the number:

$$\left|GL_2(n)\right| = \prod_{i=0}^{n-1} \left(2^n - 2^i\right)$$

We can consider that the group $G = \{M_0, \cdots, M_m\}$, operates in the set B^n, as follows:

$y = xM_k$, where $M_k \in G$, $x \in B^n$.

Moreover, the transitive set:

$$G(x) = \{y : y = xM_k, \; k = \overline{0, m}\},$$

coincides with the neighborhood of the first order of the point $x \in B^n$, *i.e.* $G(x) = G^1(x)$.

These neighborhoods do not intersect and thus, form the partition B^n. Consequently, if we take an arbitrary representative from each transitive set, we will have a code, correcting the errors of the group channel, G.

Lemma 1. *For the group matrix channel G, any code containing one representative of all transitive sets, is a code with the maximum cardinality, correcting the errors of the channel G.*

Proof. As it was mentioned, the code V, built as it was said above, corrects the errors of the matrix channel, G. On the other hand, if some code V correcting the errors of the group channel G contains more points that the number of the transitive sets then at least one of these transitive sets contains two points of V which contradicts condition (4). Q. E. D.

The above Lemma completely describes all the codes of the maximum cardinality, correcting the errors of the group channel G.

The cardinality of the neighborhood $G^1(x)$ of an arbitrary point $x \in B^n$ can be calculated by the stabilizer

of the same point or of the subgroup G_x:

$$G_x = \{M_k : xM_k = x\}.$$

In other words, the following formula is valid:

$$|G^1(x)| = \text{ind } G_x = \frac{|G|}{|G_x|}.$$

The cardinality of the code $\bar{V}(G)$ can be expressed by Burnside's Lemma [4] [5].

Let $N(M_i)$ be the set of the motionless points of the transformation M_i or in another way (which is the same) let it be the set of the eigen vectors of the matrix M_i corresponding the eigen value $\lambda = 1$, that is, let it be the set of the solutions of the following equation:

$$xM_i = x, \quad M_i \in G.$$

Lemma (Burnside's) 2. *The following formula holds true*:

$$|\bar{V}(G)| = \frac{1}{|G|}\sum_{M_i \in G}|N(M_i)| \tag{5}$$

Examples.

4) Let T be the transformation of the cyclic shift in B^n:

$$T(x_1x_2\cdots x_n) = (x_nx_1\cdots x_{n-1}),$$

and M_T be the matrix, corresponding to this transformation:

$$M_T = \begin{Vmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{Vmatrix}.$$

We discuss the group matrix channel $G = \{M_T, M_T^2, \cdots\}$. According to the definition, this channel operates as follows. If the word $x \in B^n$ is put in then we get one of the cyclic shifts of this word at the exit. We call the positive integer d the period of the word x if d is the smallest integer for which $xM_T^d = x$. Then the neighborhood of the first order of the word x has the following form:

$$G^1(x) = \{x, xM_T^1, \cdots, xM_T^{(d-1)}\}.$$

It is clear that the first order neighborhoods carry out a partitioning of B^n into classes of equivalence. If N_d is the number of the equivalence classes the elements of which have the period d then the following obviously holds:

$$\sum_{d/n} dN_d = 2^n \tag{6}$$

Let us note that the maximum cardinality code $\bar{V}(G)$ is any set of the representatives of the transitive sets and its cardinality is given by Formula (5) which has the following form for this case:

$$|\bar{V}(G)| = \sum_{d/n} N_d \tag{7}$$

Through the standard calculation technique, we get from (6) and (7) the well-known expression:

$$|\bar{V}(G)| = \frac{1}{n}\sum_{d/n} 2d\varphi(n/d) = \frac{1}{n}\sum_{d/n} 2^{n/d}\varphi(d)$$

where $\varphi(q)$ is Euler's function which gives the amount of the numbers less than q and which are coprime with respect to it.

In particular, if $n = p$ is a prime number, then:

$$\left|\overline{V}(G)\right| = 2 + \frac{\left(2^p - 2\right)}{p}.$$

5) Let there be a communication channel through which the transmitted word:

$$x = \left(x_1 \cdots x_{2n}\right) \in B^{2n},$$

is transformed into the binary word:

$$\overline{x} = \left(\overline{x}_1 \cdots \overline{x}_{2n}\right),$$

where either $\overline{x_{2i+1}} = x_{2i+1}$, and $\overline{x_{2i+2}} = x_{2i+2}$, or $\overline{x_{2i+2}} = x_{2i+1} \oplus x_{2i+2}$, for $i = \overline{0, n-1}$.

Let us describe the physical meaning of this channel. Saying "transmittance of the word *x* through the communication channel" we understand successive transmittance of symbols or, as they say, transmittance of the pulses (signals) $x_1, x_2, \cdots, x_{2n}$, taking into account that the symbols with the odd indices $x_1, x_3, \cdots, x_{2n-1}$ are transmitted without any distortion, and the rest of them: $x_2, x_4, \cdots, x_{2n}$, can have distortions defined by the directly preceding symbols.

Thus, having the symbol x_{2i} at the exit, we can get either x_{2i} or $x_{2i-1} \oplus x_{2i}$.

Now we give this description of the channel by the matrix "language". Let we have the set of the matrices $M = \{M_0, M_1, \cdots, M_n\} \subset M_{2n,2n}$ where M_0 is the unit matrix:

$$M_1 = \begin{Vmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 \end{Vmatrix}, \; M_1 = \begin{Vmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 1 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 \end{Vmatrix}, \; \cdots, \; M_n = \begin{Vmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 1 \\ 0 & 0 & \cdots & 0 & 0 & 1 \end{Vmatrix}$$

We discuss the group matrix channel G the constituent of which is the set M. As any matrix of M coincides with its inverse matrix in the group G, *i.e.* $M_i = M_i^{(-1)}$, then $M_i M_j = M_i^{-1} M_j^{-1} = \left(M_i, M_j\right)^{-1}$, $i, j = \overline{1, n}$, and G is consisted of all possible products of the matrices $M_{i_1} M_{i_2} \cdots M_{i_k}$ of M; therefore, the order of the group G is 2^n. It follows from the description of the channel $G = \{G_0, G_1, \cdots, G_{2n-1}\}$ that the code, correcting its errors, also corrects the errors of the channel with overlay. The converse proposition also is true.

Let us partition the group G into the non-intersecting sets Q_i, $i = \overline{0, n}$ where $Q_0 = \{M_0\}$ and Q_i be the set of the matrices generated the products of any i different elements, belonging to M\{M$_0$}, *i.e.* the matrix $Q \in Q_i$ if $Q = M_{j_1} M_{j_2} \cdots M_{j_i}$, where $M_{j_k} \in M \setminus \{M_0\}$, $k = \overline{1, i}$.

Talking figuratively if we enumerate the matrix rows of the group G from the top to the bottom, then the set Q_i, $i = \overline{0, n}$ is consisted of all matrices having the dimension $2n \times 2n$ and which have two units in their i-th rows with odd numbers on their diagonal positions and immediately on the right, but in the rows numbered by $2n - i$ the unit is only in a diagonal position. The other elements of the matrices are zero.

It immediately follows from the definition of the set Q_i that $\left|Q_i\right| = \binom{n}{i}$, $i = \overline{0, n}$ and for any matrix $Q \in Q_i$ the number of the motionless points of the transformation is:

$$\left|N(Q)\right| = 2^{2(n-i)} 2^i$$

As we have:

$$Q_i \cap Q_j = \varnothing, \text{ for } i \neq j, \text{ and } \bigcup_{i=0}^{2^n - 1} N(G_i) = \bigcup_{i=0}^{n} \bigcup_{Q \in Q_i} N(Q),$$

then it follows from Lemma 2 that for the maximum cardinality code $\bar{V}(G) \subseteq B^{2n}$ the following holds true:

$$\left|\bar{V}(G)\right| = \frac{1}{|G|}\sum_{i=0}^{2^n-1}\left|N(G_i)\right| = \frac{1}{2^n}\sum_{i=0}^{n}|Q_i|\left|N(G_i)\right|\frac{1}{2^n}\sum_{i=0}^{n}|Q_i|2^{2(n-i)}2^i = \frac{1}{2^n}\sum_{i=0}^{n}\binom{n}{i}2^n 2^{n-i} = \sum_{i=0}^{n}\binom{n}{i}2^{n-i} = 3^n.$$

Let us discuss Example 5 for $n=2$, *i.e.* that there is a word $x=(x_1x_2x_3x_4)\in B^4$ which can be transformed into one of the words:

$$(x_1x_2x_3x_4),\ \ (x_1(x_1\oplus x_2)x_3x_4),\ \ (x_2x_2x_3(x_3\oplus x_4)),\ \ (x_1(x_1\oplus x_2)x_3(x_3\oplus x_4)),$$

when transmitted through the channel. For the given case the set of the matrices $M=\{M_0,M_1,M_2\}$ is the following:

$$M_0=\begin{Vmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{Vmatrix},\ \ M_1=\begin{Vmatrix}1&1&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{Vmatrix},\ \ M_2=\begin{Vmatrix}1&0&0&0\\0&1&0&0\\0&0&1&1\\0&0&0&1\end{Vmatrix}.$$

The group channel $G=\{G_0,G_1,G_2,G_3\}$ having the set M as its constituent is consisted of the following matrices:

$$G_0=M_0=\begin{Vmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{Vmatrix},\ \ G_1=M_1=\begin{Vmatrix}1&1&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{Vmatrix},\ \ G_2=M_2=\begin{Vmatrix}1&0&0&0\\0&1&0&0\\0&0&1&1\\0&0&0&1\end{Vmatrix},$$

$$G_3=M_1\cdot M_2=\begin{Vmatrix}1&1&0&0\\0&1&0&0\\0&0&1&1\\0&0&0&1\end{Vmatrix}.$$

Let us find the set of the motionless points of the transformation for each element of the group G. As it was said above the set of the solutions of the equation:

$$xG_i = x \tag{8}$$

corresponds to the set $N(G_i)$, $i=\overline{0,3}$. For the matrix G_0 Equation (8) is as follows:

$$(x_1x_2x_3x_4)\begin{Vmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{Vmatrix}=(x_1x_2x_3x_4),$$

and the set of solutions of it is the set B^4. Consequently, $N(G_0)=B^4$.

Then, from (8) for the cases: $x=G_1x$, $xG_2=x$, $xG_3=x$, we find for G_1, G_2, G_3 the respective sets of the solutions:

$$N(G_1)=\{(0\ 0\ 0\ 0),(0\ 0\ 0\ 1),(0\ 0\ 1\ 0),(0\ 0\ 1\ 1),(0\ 1\ 0\ 0),(0\ 1\ 0\ 1),(0\ 1\ 1\ 0),(0\ 1\ 1\ 1)\},$$
$$N(G_2)=\{(0\ 0\ 0\ 0),(0\ 0\ 0\ 1),(0\ 0\ 1\ 0),(0\ 0\ 1\ 1),(1\ 0\ 0\ 0),(1\ 0\ 0\ 1),(1\ 0\ 1\ 0),(1\ 0\ 1\ 1)\},$$
$$N(G_3)=\{(0\ 0\ 0\ 0),(0\ 0\ 0\ 1),(0\ 1\ 0\ 0),(0\ 1\ 0\ 1)\}.$$

And, applying Lemma 2 we get the cardinality of the code $\bar{V}(G)$:

$$\left|\bar{V}(G)\right| = \frac{1}{|G|}\sum_{i=0}^{2^n-1}\left|N(G_i)\right| = \frac{1}{4}\left(\left|N(G_0)\right|+\left|N(G_1)\right|+\left|N(G_2)\right|+\left|N(G_3)\right|\right) = \frac{1}{4}(16+8+8+4) = 9$$

6) Let us discuss a little modified channel of Example 2. Namely, we take that when transmitting the vector $x=(x_1x_2\cdots x_{2n})$ some "transposition" errors of the following form take place:

$$x_{2i-1}x_{2i}\to x_{2i}x_{2i-1}\quad i=\overline{1,n},$$

taking into account that such inversions can take place in a few places.

In the terms of matrix channels the model is as follows. We have the set of the matrices $M=\{M_0,M_1,\cdots,M_n\}\subseteq M_{2n,2n}$, where M_0 is the unit matrix:

$$M_1=\begin{Vmatrix}0&1&0&0&\cdots&0\\1&0&0&0&\cdots&0\\0&0&1&0&\cdots&0\\0&0&0&1&\cdots&0\\\vdots&\vdots&\vdots&\vdots&\ddots&\vdots\\0&0&0&0&\cdots&1\end{Vmatrix},\ M_2=\begin{Vmatrix}1&0&0&0&\cdots&0\\0&1&0&0&\cdots&0\\0&0&0&1&\cdots&0\\0&0&1&0&\cdots&0\\\vdots&\vdots&\vdots&\vdots&\ddots&\vdots\\0&0&0&0&\cdots&1\end{Vmatrix},\ \cdots,\ M_n=\begin{Vmatrix}1&0&0&0&\cdots&0\\0&1&0&0&\cdots&0\\\vdots&\vdots&\vdots&\vdots&\cdots&\vdots\\0&0&\cdots&1&0&0\\0&0&\cdots&0&0&1\\0&0&\cdots&0&1&0\end{Vmatrix}.$$

Considerations analogous in the preceding example let us establish the following facts. The matrix channel G consisting of all possible products of the elements $M_{i1}\cdot M_{i2}\cdot\cdots\cdot M_{ik}$ of the set M is a group one. Besides the order of the group G is 2^n and the code, correcting the errors of the channel G also corrects the errors of the channel with the transpositions. Then, following the same logic and, using Formula (5) for the maximum cardinality code $\bar{V}(G)\subseteq B^{2n}$ we get:

$$\left|\bar{V}(G)\right|=\frac{1}{|G|}\sum_{i=0}^{2^n-1}\left|N(G_i)\right|=\frac{1}{2^n}\sum_{i=0}^{n}\binom{n}{i}2^n2^{n-i}=3^n.$$

4. The Metrics and Codes in the Additive Channel

Definition 5 (See [6]). *The arbitrary subset* $A=\{y_0,y_1,\cdots,y_m\}\subseteq B^n$ *that carries out the function* $\psi_i(x)=x\oplus y_i$, where $i=\overline{0,m}$ is called additive channel. Here $y_0=0^n$.

Definition 6 (See [7]). *The code* $V=\{v_0,\cdots,v_N\}$ *corrects the errors of the additive channel* $A=\{y_0,y_1,\cdots,y_m\}$ *if* $v_i\oplus v_i\neq y_r\oplus y_s$ where i, $j=\overline{1,N}$, r, $s=\overline{0,m}$, $i\neq j$.

As in the preceding section we define the neighborhood of k-th order of the word $x\in B^n$ as follows:

$$A^0(x)=x,\ A^1(x)=\{x\oplus y_i:y_i\in A\},\ \cdots,\ A^k(x)=\{y\oplus y_i:y\in A^{k-1}(x),y_i\in A\}.$$

NB 1. *For the additive channel* $A\subseteq B^n$ *the following equality holts true:*

$$A^k(x)\oplus x\oplus y=A^k(y),$$

For any x, $y\in B^n$.

Definition 7. (See [8] [9]) *The code* $V(A)$ *correcting the errors of the additive channel* $A\subseteq B^n$ *is called perfect if:*

$$\left|V(A)\right|=\frac{2^n}{|A|}$$

Note that the perfect code $V(A)$ has maximum cardinality though the convers statement is not always valid.

NB 2. Any word from B^n belongs to the neighborhood of the first order of only one word of the perfect code $V(A)$.

The standard and most used metric in code theory is Hamming's metric [9], *i.e.* the following function:

$$\|x\|_E=\|(x_1x_2\cdots x_n)\|_E=\sum_{i=1}^{n}x_i.$$

It can be taken that this metric is connected with the "natural" basis $E=(e_1,e_2,\cdots,e_n)$ in the following way:

$$x=\sum_{i=1}^{n}\alpha_ie_i\to\|x\|_E=\sum_{i=1}^{n}\alpha_i.$$

It is clear that if another basis is chosen, for instance, if $C=\{z_1,z_2,\cdots,z_n\}$ is taken, then another metric will be generated:

$$x=\sum_{i=1}^{n}\beta_i z_i \to \|x\|_C=\sum_{i=1}^{n}\beta_i .$$

A more general procedure of metric generation shown above is as follows. For the given subset $C=\{z_1,z_2,\cdots,z_m\}\subseteq B^n$ and the vector $x\in B^n$ we consider all "expansions" of x into C, *i.e.* the expression of the following form:

$$x=\sum_{i=1}^{m}\alpha_i z_i \tag{9}$$

and we put the following number:

$$\sum_{i=1}^{m}\alpha_i ,$$

into correspondence to (9).

Now choosing the least number of these we define the following norm ([1]; the MLM norm) connected with C:

$$\|x\|_C=\begin{cases}\min\{\sum\alpha_i\} \text{ into the representation with respect to } (9),\\ \infty, \text{ if there are no such representations.}\end{cases} \tag{10}$$

Lemma 3. *The function* $\|\ \|_C$ *is a metric* (*below*, "*MLM metric*") *for any subset* $C\subseteq B^n$.

In terms of graph theory the described situation is as follows. Let us give the following binary relation on the set of vertices B^n:

$x\sim z \leftrightarrow x\oplus z=z_i$ for some $z_i\in C$.

This relation defines adjacency of vertices and we get a graph, *i.e.* the set of arcs E_c, which is given by the equality: $x\oplus z=z_i$.

The distance among the vertices of this graph is given in the standard way: the minimum number of the arcs in the chain connecting these vertices; and the infinity if there is not such a chain.

Example.

7) If $C=\{(10\cdots0),(11\cdots0),\cdots,(11\cdots1)\}$ then the MLM norm has the following form:

$$\|x\|_C=\sum_{i=1}^{n-1}(x_i\oplus x_{i+1})+x_n, \text{ где } x=(x_1x_2\cdots x_n).$$

In particular, for $n=3$ the MLM norms of the vectors in B^3 are as follow:

$$\|000\|_C=0,\ \|001\|_C=2,\ \|010\|_C=2,\ \|100\|_C=1,\ \|011\|_C=2,\ \|101\|_C=3,\ \|110\|_C=1,\ \|111\|_C=1.$$

If $A=\{y_0,y_1,\cdots,y_m\}$ is an arbitrary additive channel then the set A generates an MLM norm in B^n given by Formula (10). The statement presented below shows that the ability of the code $V=\{v_0,v_1,\cdots,v_N\}$ to correct the errors of the additive channel A can be formulated in terms of the MLM norm generated by the set.

Lemma 4. *The code* V *corrects the errors of the additive channel* A *iff the following conditions hold*:

$$\rho_A(v_i,v_J)\geq 3, \text{ for } i,\ j=\overline{0,N};\ i\neq j .$$

Proof: If $\rho_A(v_i,v_J)\geq 2$, then according to definition:

$$v_i\oplus v_j=y_r\oplus y_s ,$$

or in another way:

$$v_i\oplus y_r=v_j\oplus y_s \tag{11}$$

But it follows from (11) that the code V does not correct the errors of the additive channel A.

And if $\rho_A(v_i,v_J)\geq 3$, then:

$$v_i \oplus v_j = \sum_{K=1}^{m} \lambda_k y_k ,$$

where $\sum_{K=1}^{m} \lambda_k \geq 3$. But the equality:

$$v_i \oplus v_j = y_r \oplus y_s ,$$

is impossible; hence, the code V corrects the errors of the additive channel A.

Let us discuss an arbitrary basis $\{z_1, z_2, \cdots, z_n\}$ of the space B^n and the linear reversible transformation $f : B^n \to B^n$ defined in the following way:

$$f(z_i) = e_i = \left(0^{i-1}10^{n-i}\right), \quad i = \overline{1,n} .$$

The image of any set $Q \subseteq B^n$ is denoted by $f(Q)$:
$f(Q) = \{f(z); z \in Q\}$, and $|f(Q)| = |Q|$,
and the spectra $\{\rho_C(u,v) : u, v \in Q\}$ and $\{\rho_C(f(u), f(v)), f(u), f(v) \in f(Q)\}$, have no any simple connection. The situation will be changed to an extent if we consider different MLM norms and introduce limitations on the subject transformations.

Definition 8. *The MLM metric ρ_C is called a basis one if $C \subseteq B^n$ is a basis.*

Lemma 5. *For the basis MLM metrics ρ_C and ρ_E the following relations hold true*:

$$\rho_E(u,v) = \rho_C\left(f^{-1}(u), f^{-1}(v)\right), \quad \rho_C(u,v) = \rho_E\left(f(u), f(v)\right) \tag{12}$$

where u, $v \in B^n$.

For the given MLM metric all the standard definitions of the correcting code theory can be modified replacing Hamming's metric by any basis MLM metric. In particular, the perfect code V with the distance $d = 2t+1$ is a partition of the set B^n in the union of the spheres of the radius t in the MLM metric. According to (12) the perfect codes in one metric are transformed into perfect codes in another metric. Besides Formulas (12) allow various interpretations of geometrical character. We present two facts which we use further.

Lemma 6.

a) *The subset, $A \subseteq B^n$ with the metric ρ_C and the subset $f(A)$ with the basis metric ρ_E simultaneously are spheres with the radius t.*

b) *The code $V \subseteq B^n$ with the basis metric ρ_C and the code $f(V)$ with the basis metric ρ_E simultaneously are perfect with the distance $2t+1$.*

Example.

9) We discuss in B^3 the perfect code in Hamming's metric $V = \{(000),(111)\}$, with the distance $d = 3$. When choosing the basis $C = \{(100),(110),(111)\}$ the image of this perfect code in the transformation $f(x) = xM$ is the following code $f(V) = \{(000),(101)\}$ where M is the matrix with the following vectors of the set C as its rows:

$$M = \begin{Vmatrix} 100 \\ 110 \\ 111 \end{Vmatrix}.$$

Then the spheres with the unit radius having their centres at the points of the code $f(V)$ have the following forms:

$$S_1(000) = \{(100),(110),(111),(000)\},$$

$$S_2(101) = \{(101),(010),(001),(011)\}.$$

(See example 7). Thus $f(V)$ is a perfect code with the distance 3 in the MLM metric:

$$\|x\|_C = (x_1 \oplus x_2) + (x_2 \oplus x_3) + x_3 .$$

Though the metrics with different bases can strongly differ the spectrum of distances of the space B^n is always the same.

Lemma 7. *Let* $t_k(C)$ *be the number of the points from* B^n *with* $\|x\|_C = k$. *Then* $t_k(C) = \binom{n}{k}$, $k = \overline{0,n}$ *for an arbitrary basis* C.

Proof. According to the definition, $\|x\|_C$ is the number of the vectors of the basis $C = \{z_1, z_2, \cdots, z_n\}$ included into the expansion of the vector *x*:

$$x = \sum_{i=1}^{n} \lambda_i z_i .$$

Therefore, the number of the vectors x with $\|x\|_C = k$ is equal to the number of the solutions of the following equation:

$$\sum_{i=1}^{n} \lambda_i = k ,$$

where $\lambda_i = \{0,1\}$, *i.e.* it is equal to $\binom{n}{k}$.

NB 3. If the basis C is chosen as in Example 7 then the preceding statement is equivalent to the following formula:

$$\sum_{\{x_1 \cdots x_n\}} z^{\sum_{i=1}^{n-1}(x_i \oplus x_{i+1}) + x_n} = (1+z)^n .$$

The preceding statements make possible to build the perfect codes in B^n for arbitrary basis metrics if one such code is already built for one basis metric at least. In particular, if $A \setminus y_0 = \{y_1, y_2, \cdots, y_m\}$ is the basis for the subspace $H \subseteq B^n$ then the following statement holds true:

Theorem 1. *The perfect codes in* B^n, *correcting the errors of the additive channel* $A^t(y_0)$ *for* $1 \le t < \frac{m-1}{2}$, *exist only for the following values of m and* t:

a) $m = 2^r - 1, \quad t = 1$,
b) $m = 23, \quad t = 3$.

Proof. We discuss the basis $C = \{z_1, z_2, \cdots, z_n\}$ of the space B^n where $z_i = y_i$, $i = \overline{1,m}$ and the linear reversible transformation $f : B^n \to B^n$, is defined above.

Necessity. Let $V(A^t(y_0))$ be a perfect code in B^n with the basis metric ρ_C.

It follows from Lemma 6 that the code $f(V(A^t(y_0)))$ also is perfect in B^n with the basis metric ρ_E, correcting the errors of the channel $f(A^t(y_0))$. Then as $A^t(y_0) \subseteq H$ and for $(\alpha_1 \alpha_2 \cdots \alpha_n) \in f(H)$ holds the following: $\alpha_i = 0$, $i = \overline{m+1,n}$ and we have:

$$f(A^t(y_0)) \subseteq f(H) = B^n \times (0^{n-m})$$

Taking this and NB 1 and 2 into account we see that the code:

$$V_1 = \{v \in B^m : vu \in f(V(A^t(y_0))), u \in B^{n-m}\},$$

is perfect in B^n and it corrects the errors of the channel:

$$\{y \in B^m : y0^{n-m} \in f(A^t(y_0))\},$$

with the basis metric ρ_E. It is possible only for $m = 2^r - 1$, $t = 3$ or $m = 23$, $t = 3$ [9].

Sufficiency. We discuss the perfect code $V\left(A^t\left(e_0\right)\right)\subseteq B^m$ where $A=\left\{e_0,e_1,\cdots,e_m\right\}$ for $m=2^r-1$, $t=1$ (Hamming's code) or $m=23$, $t=1$ (Gallay's code) [10].

Now, as for any $u_1,\ u_2\in V\left(A^t\left(e_0\right)\right)\times B^{n-m}$ the following inequality holds true:

$$\rho_E\left(u_1,u_2\right)\geq 3,$$

then it follows from Lemma 4 that the code $V\left(A^t\left(y_0\right)\right)\times B^{n-m}$ corrects the errors of the channel:

$$A^t\left(y_0\right)\times 0^{n-m}$$

On the other hand, we have:

$$\left|V\left(A^t\left(y_0\right)\right)\times B^{n-m}\right|=\frac{2^n}{\left|A^t\left(y_0\right)\times 0^{n-m}\right|},$$

i.e. $V\left(A^t\left(y_0\right)\right)\times B^{n-m}$ is perfect in B^n with the basis metric ρ_{E} and consequently (according to Lemma 6 the code $f\left(\left(V\left(A^t\left(y_0\right)\right)\right)\times B^{n-m}\right)$ is perfect in B^n with the basis metric ρ_C. Q. E. D.

5. The Upper and Lower Limits of the Cardinality of the Matrix Channel

The case of an arbitrary cannel does not make possible to obtain simple solutions for the code cardinality and even to obtain some universal Hamming and Varshamov-Gilbert type boundaries and requires some special restrictions on the structure for the matrix channel M.

Let the channel $M=\left\{M_0,\cdots,M_m\right\}\subseteq M_{n,n}$ is algebraic, *i.e.* all the matrices in M are reversible and belong to M with their reverse ones. We introduce two parameters connected with M. Let:

$$\overline{d^1}\left(M\right)=\max_{x\in B^n}\left|M^1\left(x\right)\right|,$$

$$\overline{d^2}\left(M\right)=\max_{x\in B^n}\left|M^2\left(x\right)\right|.$$

Lemma 8. *The following inequalities hold true*:

$$\frac{2^n}{\overline{d^2}\left(M\right)}\leq\left|\overline{V}\left(M\right)\right|\leq\frac{2^n}{d^1\left(M\right)} \tag{13}$$

here M *is a matrix algebraic channel.*

We consider the matrix channel $M\subseteq M_{n,n}$ from Example 2. This channel exchanges the places of two neighboring letters in the word $x=\left(x_1x_2\cdots x_n\right)\in B^n$.

Let $x=\left(\left(\gamma^{t_1}\overline{\gamma}^{t_2}\gamma^{t_3}\cdots\overline{\gamma}^{t_k}\right)\right.$ where $\gamma\in\left\{0,1\right\}$, $t_i\geq 1$, $\overline{\gamma}=\gamma\oplus 1$ for $i=\overline{1,k}$. We denote the number of the sequences of the word x, by $\mu\left(x\right)$. Then $\left|M^1\left(x\right)\right|=\mu\left(x\right)$ and $\underline{d^1}\left(M\right)=1$.

If $T\left(x\right)=\min_k\mu\left(xM_k\right)$ then $\mu\left(x\right)-2\leq T\left(x\right)\leq\mu\left(x\right)$. Consequently:

$$\left|M^2\left(x\right)\right|\leq\sum_{y\in M^1\left(x\right)}\mu\left(y\right).$$

As $M^1\left(x\right)$ is the neighborhood of the first order of the word x then all the words obtained from x by transposition of the neighboring letter are included into $M^1\left(x\right)$. Every one of these words has no more than $\mu\left(x\right)=k$ sequences and the number of such words exactly equals to k. It follows from this that:

$$\left|M^2\left(x\right)\right|\leq k^2,$$

and, according to Lemma 8 universal limitations (13) have the form:

$$\frac{2^n}{n^2}\leq\left|\overline{V}\left(M\right)\right|\leq 2^n.$$

Roughness of these limits is connected with the great generality of the above considerations.

Below we present more accurate limits, taking the specification of the matrix channel M into account.

6. The Upper Limit for $\left|\bar{V}(M)\right|$

We partition $\bar{V}(M)$ into the two subsets V_1 and V_2 such that the first one includes the words with their sequence number not exceeding λ and the second one includes those exceeding λ. Then we have:

$$\left|\bar{V}(M)\right| = \left|V_1\right| + \left|V_2\right|$$

and

$$\left|V_1\right| < 2\sum_{k=1}^{\lambda}\binom{n-1}{k-1}, \quad \left|V_2\right| < \frac{2^n}{\lambda} \tag{14}$$

The first inequality follows from the fact that the number of the words in B^n having exactly k sequences equals to $2\binom{n-1}{k-1}$ see [2]), and the second one results in the fact that the cardinality of the neighborhood of the first order of the word $x \in B^n$ equals to the number of the sequences of x. We choose the parameter λ such that to minimize the upper limit $\left|\bar{V}(M)\right|$. Then we have from (14) for

$$\lambda < \frac{n}{2} : \left|\bar{V}(M)\right| < 2\lambda\binom{n-1}{\lambda-1} + \frac{2^n}{\lambda}.$$

Choosing $\lambda = \frac{n}{2} - \sqrt{n\ln n}$ and applying Sterling's formula for $n \to \infty$ [2]:

$$\binom{n}{\lambda} \sim \frac{2^{n+1}}{\sqrt{2\pi n}} \mathrm{e}^{-\frac{(2\lambda-n)^2}{2n}}$$

we get:

$$\left|\bar{V}(M)\right| < \frac{2^n}{n\sqrt{2\pi r}} + \frac{2^{n+1}}{n - 2\sqrt{n\ln n}} \sim \frac{2^{n+1}}{n}.$$

7. The Lower Limit for $\left|\bar{V}(M)\right|$

We discuss the following additive channel $A = \left\{\left(0^n, 1^2 0^{(n-2)}, \cdots, 0^{(n-2)}11\right)\right\}$ This channel corresponds to that essential situation when the errors rise in pairs and in neighboring places. The connection of this channel with the matrix channel M is explained by the following statement.

Lemma 9. *Every code that corrects the errors of the additive channel A also corrects the errors of the matrix channel M.*

Proof: We assume that the code $V = \{v_0, v_1, \cdots, v_N\}$ corrects the errors of the channel:

$$A = \left\{y_0, y_i = 0^{i-1}1^2 0^{n-i-1}, \ i = \overline{1, n-1}\right\},$$

and that there exist the matrices:

$$M_i,\ M_j \in M = \{M_0, M_1, \cdots, M_{n-1}\}$$

such that for some v_s, $v_r \in V$ takes place the equality:

$$v_s M_i = v_r M_j.$$

Hence we have:

$$\left(\alpha_1^s \cdots \alpha_{i+1}^s \alpha_i^s \cdots \alpha_n^s\right) = \left(\alpha_1^r \cdots \alpha_{j+1}^r \alpha_j^r \cdots \alpha_n^r\right),$$

where $v_s = \left(\alpha_1^s \cdots \alpha_n^s\right)$, $v_r = \left(\alpha_1^r \cdots \alpha_n^r\right)$. Then taking into account that $v_r \neq v_s$ we get:

$$\alpha_i^s \neq \alpha_{i+1}^s \ \text{ or } \ \alpha_j^r \neq \alpha_{j+1}^r$$

Consequently, the following variants are possible:

a) $\alpha_i^s \neq \alpha_{i+1}^s$ and $\alpha_j^r \neq \alpha_{j+1}^r$.

Then the following equality takes place:

$$v_s \oplus y_i = v_r \oplus y_j ,$$

which is a contradiction.

If:

b) $\alpha_i^s \neq \alpha_{i+1}^s$ and $\alpha_j^r = \alpha_{j+1}^r$,

c) $\alpha_i^s = \alpha_{i+1}^s$ and $\alpha_j^r \neq \alpha_{j+1}^r$,

then the following equalities take place, respectively:

$$v_s \oplus y_i = v_r \oplus y_0, \quad v_s \oplus y_0 = v_r \oplus y_j$$

which also contradict the conditions of the Lemma. Q. E. D..

It follows from Lemma 9 that the maximum cardinality of the code, correcting the errors of the channel A is the lower estimation for the cardinality $\bar{V}(M)$, *i.e.* $\left|\bar{V}(M)\right| \geq \left|\bar{V}(A)\right|$. Taking into account Theorem 1 we get the lower estimation of $\left|\bar{V}(M)\right|$ for $n = 2^r$:

$$\left|\bar{V}(M)\right| \geq \frac{2^n}{n}.$$

References

[1] Leontiev, V.K., Movsisyan, G.L. and Margaryan, J.G. (2012) Geometry of the Additive Channel. *Reports at NAS*, **112**, 7-18.

[2] Leontiev, V.K. and Movsisyan, G.L. (2007) Algebraic Communication Channels. *The First International Algebra and Geometry Conference*, Yerevan, 16-20 May 2007, 16-20.

[3] Leontiev, V.K., Movsisyan, G.L. and Osipyan, A.A. (2012) Matrix Communication Channels. *Materials of the XI International Seminar Discrete Mathematics and Its Application*, Moscow State University, 415-416.

[4] Sachkow, W.N. (1977) Combinatoric Methods of Descret Mathematics. Nauka, Moscow.

[5] Lang, S. (1968) Algebra. Mir, Moscow.

[6] Deza, M.E. (1964) On Correction of Arbitrary Noise and on Worst Noise. Theory of Information Communication, Moscow, 26-31.

[7] Leontiev, V.K., Movsisyan, G.L. and Margaryan, J.G. (2004) On the Additive Communication Channel. *Reports at NAS*, **104**, 23-27.

[8] Leontiev, V.K., Movsisyan, G.L. and Margaryan, J.G. (2008) On Perfect Codes in Additive Channels. *Information Transfer Problems*, **44**, 12-19.

[9] Leontiev, V.K., Movsisyan, G.L. and Margaryan, J.G. (2006) Perfect Codes in Additive Channels. *Reports at RAS*, **411**, 306-309.

[10] Mac Williams, F.J. and Sloane, N.J.A. (1979) The Theory of Error-Correcting Codes. Svjaz, Moscow.