Scientific
Research

Dirichlet Regions and Perfect Codes in Additive Channel

Garib Movsisyan
BIT Group, Moscow, Russia
Email: garib@firmbit.ru

ABSTRACT

In the present work, the class of metrics connected with subsets of the linear space on the field, GF(2), is considered and a number of facts are established, which allow us to express the correcting capacity of codes for the additive channel in terms of this metrics. It is also considered a partition of the metric space, B^n, by means of D-representable codes. The equivalence of D-representable and the perfect codes in the additive channel is proved.

Keywords: Dirichlet Regions; Perfect Codes; Additive Channel

1. Introduction

We consider the additive channel of communication [1-4] as a transformer of information, which is a generalization of the classical binary channel with limited number of distortions, $0 \to 1, 1 \to 0$. Many notions and facts in the present work take their origins in the classic coding theory and are the direct analogues of the well-known results [1-5].

The "noise" generated by the additive channel leads to the fact that there appears a word at the outlet of the channel which is different from that at its inlet. In connection with this there rises a necessity of transforming (coding) information for conducting it through the given channel, as well as a necessity of retransforming (decoding) it at the channel outlet. This circumstance makes one introduce such standard notions in the coding theory as: error correcting code; transfer/decoding speed, etc.

On the other hand, as there are many additive channels, the problem of ordering and classification of such channels rises, taking into account the main difficulty, namely, the possibility of correcting the generated errors.

We consider the class of metrics connected with the subsets of the space on the field, GF(2), and establish a number of facts which allow us to express the correcting capacity of codes for the additive channel in terms of this metrics. Also, we consider the partition of the metric space, B^n, through D-representable codes. The equivalence of D-representable and perfect codes in the additive channel is proved.

2. Codes in the Additive Channel

Let $B = \{0,1\}$ be a Galua field of two elements and $B^n = \{0,1\}^n$ be an n-dimensional vector space on that field.

If $A = \{y_0, y_1, \cdots, y_m\}$ is a subset of B^n, then the notion of the additive channel is connected with A, as follows.

Any of the vectors, $x \in B^n$, in the channel, A, is transformed into one of the following vectors:

$$y = x \oplus y_s, s = \overline{0, m},$$

where $\oplus$ is the operation of addition (with respect to mod 2) in the space, B^n.

Definition [1]. For any vector, $x \in B^n$, we call the neighbourhood of order t with respect to C, the following set:

$$C^t(x) = \{u \oplus y : u \in C^{t-1}(x), y \in C\}.$$

For convenience we take, $C^o(x) = \{x\}$.

Examples:

1) Let $A = \{0^n, 1^n\}$. Then $A^t(x) = \{x, \bar{x}\}$, where $\bar{x}$ is the logic negation of x.

2) If $A = \{y : \|y\| \equiv 0 (\mathrm{mod}\, 2)\}$ is the parity counter, then:

$$A^t(x) = \begin{cases} A, \text{if } \|x\| \equiv 0 (\mathrm{mod}\, 2), \\ \overline{A}, \text{ if } \|x\| \equiv 1 (\mathrm{mod}\, 2), \end{cases}$$

where $\overline{A}$ is complement of the set, A, in B^n.

3) If $A = \{y : \|y\| \leq t\}$, then in the additive channel,

A, can occur no more than t 'errors' of the form, $0 \rightarrow 1, 1 \rightarrow 0$. Consequently, $A^t(x)$ is a sphere of the radius, t, having its centre at the point, x.

Thus, we get the classical case of the binary channel with limited number of errors.

Definition [2]. The code, $V = \{v_0, v_1, \cdots, v_N\}$, corrects the errors of the additive channel, $A = \{y_0, y_1, \cdots, y_m\}$, if: $A^1(v_i) \bigcap A^1(v_j) = \varnothing$, for $i \neq j$.

An equivalent form of this condition is:

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

or the one symmetrical to it:

$$v_i \oplus v_j \neq y_s \oplus y_r.$$

It is obvious that the preceding definitions are symmetric with respect to the pair, (A, V), and therefore, both "generation" and "correction" of errors have the same nature.

Statement 1 [3]. If the code, V, corrects the errors of the additive channel, A, then the code, A, corrects the errors of the additive channel, V.

To describe the "relations" of the additive channel, A, and the code, V, correcting the errors of that channel it is convenient to introduce the following double-case predicate, $X(A, V)$:

$$X(A, V) = \begin{cases} 1, \text{ if the code, } V, \\ \text{corrects the errors of the channel, } A, \\ 0, \text{ otherwise.} \end{cases}$$

Definition. We call any pair, (A, V), additive if it is a solution of the following equation:

$$X(A, V) = 1.$$

Taking this definition into account, the property of perfectness of codes can be written as follows:

The pair, (A, V) is additive if $\bigcup_{v \in V} A^1(v) = B^n$.

Note that there are as many additive channels, as there are Boolean functions, and a few of them do not essentially differ from each other. It is not clear how to classify such channels yet, but the following statements correspond the commonly accepted viewpoint.

Definition [3]. The channels, A and C, are called equivalent if any code correcting the errors of the additive channel, A, corrects the errors of the channel, C, and vice versa.

Introducing the following relation of partial order, one can formally write:

$$A \leq C; X(C, V) = 1 \rightarrow X(A, V) = 1, \text{ for all } V \subseteq B^n.$$

If $A \subseteq C$, then $A \leq C$, which is natural.

This property makes possible to look additive channels with the 'best' and 'worst' correcting capacities for each

$m < 2^n$.

Statement 2 [3]. The additive channels, $(A \oplus u)$ and $(A \oplus v)$, are equivalent for any $u, v \in B^n$.

Statement 3 [3]. If $X(A, V) = 1$, then $|A \bigcap V| \leq 1$.

It follows from the preceding statements that one can consider—without loss of generality:

a) If $\{A\}$ is a class of additive channels equivalent to A, then it is sufficient to solve the coding problem for any representative of that class.

b) The additive channel, A, includes the null vector, which can be interpreted as the possibility of errorless transfer of the signal through that channel.

As it follows from $X(A, V) = 1$ that $X(V, A) = 1$, then an analogical statement is correct for the vector, V, too, i.e. it is sufficient to discuss the codes including the null vector.

Thus, it follows from $X(A, V) = 1$ that the sets, A and V, can overlap only at zero, and the search of the code, V, is to be organized in the set, $\{B^n \setminus A\} \bigcup 0^n$. Below:

$$y_0 = 0^n \in A, v_0 = 0^n \in V.$$

As the power of the neighbourhood of order t does not depend on the vector, v, we make the following denotation, $C^t = |C^t(v)|$.

Note that for the additive pair, (A, V), the following limits take place [2]:

$$\frac{2^n}{A^2} \leq |V| \leq \frac{2^n}{A^1}.$$

It is clear that the upper limit is reached for the perfect pair, (A, V)

3. Metrics and Codes

The standard and most used metrics in coding theory is Hamming's metrics, i.e. the following function:

$$\|x\|_E = \|(x_1 x_2 \cdots x_n)\|_E = \sum_{i=1}^{n} x_i.$$

One can consider that this metrics is connected with the "natural" basis, $E = (e_1, e_2, \cdots, e_n)$, in the following way:

$$x = \sum_{i=1}^{n} \alpha_i e_i \rightarrow \|x\|_E = \sum_{i=1}^{n} \alpha_i.$$

It is obvious that if another basis, $C = \{y_1, y_2, \cdots, y_n\}$, is chosen then another metrics is generated:

$$x = \sum_{i=1}^{n} \beta_i y_i \rightarrow \|x\|_C = \sum_{i=1}^{n} \beta_i.$$

The more general procedure of metrics generation in the above-mentioned way is as follows. For the given subset, $C = \{y_1, y_2, \cdots, y_s\} \subseteq B^n$, and the given vector, $x \in B^n$, we consider all expansions of x with respect to

C , *i.e.* the expansions having the following form:

$$x = \sum_{i=1}^{s} \alpha_i y_i, \qquad (1)$$

and then we put the following number into correspondence with the above expansion:

$$\sum_{i=1}^{s} \alpha_i.$$

Then, choosing the least of these numbers, we define the following norm (the MLM norm) connected with C :

$$\|x\|_C = \begin{cases} \min\{\sum \alpha_i\}, \text{for expansion (1),} \\ \infty, \qquad \text{if there is no such an expansion.} \end{cases}$$

Lemma 1 [4]. The function, $\|x\|_C$, is a metrics (below, MLM metrics) for any subset, $C \subseteq B^n$.

Example:

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

$$\|x\|_C = \sum_{i=1}^{n-1}(x_i \oplus x_{i+1}) + x_n, \text{where } x = (x_1 x_2 \cdots x_n).$$

In particular, for $n = 3$, the MLM norms of vectors in B^3 take the following values:

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

In terms of graph theory, the above situation is as follows. We give the following binary relation on the set of vortices, B^n :

$$x \sim y \leftrightarrow x + y = y_i \text{ for some } y_i \in C.$$

This relation defines adjacency and, geometrically, the set of vortices of the N-dimensional unit cube corresponds to the metrical space, (B^n, ρ_C) , and the distance between two points in B^n is equal to the minimum number of sides in the circuit connecting the corresponding vortices, or it is infinity, if there is no such circuit.

Let $M = \{y_1, y_2, \cdots, y_r\}$ be a basis for the additive channel, *A*. We consider any basis, $\{z_1, z_2, \cdots, z_n\}$, in the space, B^n , where $z_i = y_i, i = \overline{1,r}$, and f is a linear reversible transformation, $f: B^n \to B^n$, defined in the following way:

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

We denote the image of the set, $C \subseteq B^n$, by $f(C)$:

$$f(C) = \{f(y); y \in C\}.$$

It is obvious that if $(\alpha_1 \alpha_2 \cdots \alpha_n) \in f(A)$, then $\alpha_i = 0$ for all $i = \overline{r+1, n}$.

We denote the linear shell of the set, C , by $L(C)$, and we denote by $\overline{L}(C)$ the subset in B^n satisfying the following condition:

$$L(C) = \overline{L}(C) = B^n,$$

where + means the direct sum the subspaces. It is obvious that $\overline{L}(C) = 0^n$, if $L(C) = B^n$.

The following holds true.

Lemma 2 [4]. For any vectors, $u, v \in L(M)$, the following relations hold true:

$$\rho_M(u,v) = \rho_E(f^{-1}(u), f^{-1}(v)); \rho_E(u,v)$$
$$= \rho_M(f(u), f(v)).$$

Lemma 3 [6]. The code, V , corrects the errors of the additive channel, *A*, iff the following holds true:

$$\rho_A(v_i, v_j) \geq 3, i \neq j, v_i, v_j \in V.$$

Example:

5) We consider the channel, $A = \{0^n, 10^{n-1}, 1^2 0^{n-2}, \cdots, 1^n\}$, as an illustration. "Physically", the channel *A* means that the "errors" of the form, $0 \to 1, 1 \to 0$, which take place either in the 1st place, or in the 1st and 2nd places simultaneously, and so on. Thus, $A^1 = n+1$ and to build a maximum volume code correcting the errors of the given channel we use Lemma 3. It is sufficient to consider all the subsets, $V \subseteq B^n$, for which:

$$|V| = \frac{2^n}{n+1}, \rho_A(v_i, v_j) \geq 3, v_i, v_j \in V.$$

Let $C_1, C_2 \subseteq B^n, C = C_1 \bigcup C_2, L(C_1) \bigcap L(C_2) = \{0^n\}$.

Lemma 4. For any $x, y \in L(C)$ holds true the equation:

$$\rho_C(x,y) = \rho_{C_1}(x_1, y_1) + \rho_{C_2}(x_2, y_2),$$

where $x_1, y_1 \in L(C_1); x_2, y_2 \in L(C_2)..$

Proof. It follows from the conditions of lemma that the vectors, $x, y \in L(C)$, are one to one represented in the form [7]:

$$x_1 = x_1 \oplus x_2, y = y_1 \oplus y_2,$$
$$\text{where } x_1, y_1 \in L(C_1), x_2, y_2 \in L(C_2).$$

Consequently:

$$\rho_C(x,y) = \rho_C(x_1 \oplus x_2, y_1 \oplus y_2) \qquad (2)$$
$$= \rho_C(x_1, y_1) + \rho_C(x_2, y_2)$$

We assume—without loss of generality—that:

$$C_1 = \{z_1, z_2, \cdots, z_{m_1}\},$$
$$C_2 = \{z_{m_1+1}, z_{m_1+2}, \cdots, z_m\},$$
$$\rho(x,y) = \sum_{i=1}^{m} \alpha_i; x \oplus y = \sum_{i=1}^{m} \alpha_i z_i.$$

Then:

$$\rho_C(x_1, y_1) = \sum_{i=1}^{m_1} \alpha_i = \rho_{C_1}(x_1, y_1);$$

$$\rho_C(x_2, y_2) = \sum_{i=m_1+1}^{m_1} \alpha_i = \rho_{C_2}(x_2, y_2),$$

where:

$$x_1 \oplus y_1 = \sum_{i=1}^{m_1} \alpha_i z_i, x_2 \oplus y_2 = \sum_{i=m_1+1}^{m_1} \alpha_i z_i.$$

Consequently, taking (2) into account, we get:

$$\rho_C(x, y) = \rho_{C_1}(x_1, y_1) + \rho_2(x_2, y_2).$$

Q.E.D.

Lemma 5. For any additive pairs, (A_1, V_1) and (A_2, V_2), where $A_1, V_1 \subseteq L(C_1), A_2, V_2 \subseteq L(C_2)$, the pair, $(A_1 + A_2, V_1 + V_2)$, is additive, too.

Proof. Let for $x, \bar{x} \in A_1 + A_2, y, \bar{y} \in V_1 + V_2$, hold the following equation:

$$x \oplus \bar{x} = y \oplus \bar{y}. \tag{3}$$

From the definition of the direct sum of sets it follows that:

$$x = x_1 \oplus x_2, \bar{x} = \bar{x}_1 \oplus \bar{x}_2, y = y_1 \oplus y_2, \bar{y} = \bar{y}_1 \oplus \bar{y}_2,$$

where $x_1, \bar{x}_1 \in A_1, x_2, \bar{x}_2 \in A_2, y_1, \bar{y}_1 \in V_1, y_2, \bar{y}_2 \in V_2$.

Consequently, taking (3) into account, we get:

$$x_1 \oplus x_2 = y_1 \oplus y_2, \bar{x}_1 \oplus \bar{x}_2 = \bar{y}_1 \oplus \bar{y}_2,$$

That is, the pairs, (A_1, V_1) and (A_2, V_2) are not additive.

Q.E.D.

4. Partition of the Metric Space into Dirichlet's Regions

Let (B^n, ρ_C) be the metric space with an MLM norm, ρ_C, where C is a subset in B^n.

We define for any $V \subseteq B^n$ the Dirichlet region, D_x, of the point, $x \in V$, in the following way:

$$D_x = \{y \in B^n; \rho_C(x, y) \le \rho_C(z, y), \forall z \in V\}.$$

It is obvious that:

$$\bigcup_{x \in V} D_x \subseteq B^n \tag{4}$$

In fact, Dirichlet's region of the point, x, includes all points of the metric space, (B^n, ρ_C), which are not farther from x than from the other points in V.

It is easy to notice that it is sufficient given the coincidence of the sets, $L(C)$ and B^n, for (4). Nevertheless, this condition is not always necessary, which can be seen from the following example.

Examples:

6) Let

$$C = \{(1000), (0100), (0010), (1010)\},$$

and $V = \{x = (0000), y = (1111)\}$.

Then we have:

$$D_x = \{(0000), (1000), (0100), (0010), (1100),$$
$$(1010), (0110), (1110)\}$$

$$D_y = \{(1111), (1001), (0101), (0011), (1101),$$
$$(1011), (0111), (0001)\}$$

that is, $B^4 = D_x \bigcup D_y$.

7) Let

$$C = \{(1000), (0100), (0010)\};$$

$$V = \{x = (0000), y = (0001), z = (1111)\},$$

then:

$$D_x = \{(0000), (1000), (0100), (0010), (1100),$$
$$(1010), (0110), (1110)\}$$

$$D_y = \{(0001), (1001), (0101), (0011)\},$$

$$D_z = \{(1101), (1011), (0111), (1111)\}$$

It is obvious that: $B^4 = D_x \bigcup D_y \bigcup D_z$ and D_x, D_y, D_z do not overlap in pairs. It follows from this example that the condition, $|V| = 2^k$, or $|D_x| = |D_y|$, is not necessary for the equality (4).

The following theorem 'connects' C and V, giving the answer to the question: which are the conditions providing Equation (4).

Theorem 2. The equation:

$$\bigcup_{x \in V} D_x = B^n$$

holds true for all $y \in \bar{L}(C)$ iff:

$$V \bigcap (L(C) \oplus y) \ne \varnothing.$$

Proof. Taking (4) into account, it is sufficient to prove that $B^n \subseteq \bigcup_{x \in V} D_x$, *i.e.* for every vector, $z \in L(C) \oplus y, y \in \bar{L}(C)$, there is such x that $z \in D_x$. As for any vectors, $z_1 \in L(C) \oplus y_1$, $z_2 \in L(C) \oplus y_2$, $y_1 \ne y_2, y_1, y_2 \in \bar{L}(C)$, holds the following:

$$\rho_C(z_1, z_2) = \infty,$$

then $z \in D_x$ iff $x, z \in L(C) \oplus y$.

Q.E.D.

Definition. The code, V, is called D-representable in the metrical space, (B^n, ρ_C), if all Dirichlet regions of the points in V do not overlap in pairs.

We note that D-representability of a code is connected with a certain metrics and, in general, this property does

not preserve if the metrics is changed.

Example:

8) Let:

$$C_1 = \{(1000),(0100),(0010),(0001),$$
$$(1100),(1010),(0110)\}$$
$$C_2 = \{(1000),(0100),(0010),(0001)\},$$
$$V = \{x = (0000), y = (1111)\}.$$

We have in the metric space, $\left(B^4, \rho_{c_1}\right)$ that $D_x \bigcap D_y = \varnothing$. But $D_x \bigcap D_y \neq \varnothing$ in the metric space, $\left(B^4, \rho_{c_2}\right)$.

Theorem 3. The code, V, is D-representable in the metrical space, $\left(B^n, \rho_C\right)$, iff the code, $V \bigcap \left(L(C) \oplus y\right)$, is D-representable in the metrical space, $\left(L(C) \oplus y, \rho_C\right)$, for all $y \in \bar{L}(C)$.

Proof. For $L(C) = B^n$ we have:

$$V \cap L(C) = V, \left(L(C) \oplus y, \rho_C\right) = \left(B^n, \rho_C\right);$$

then it is logical to consider the case, $L(C) \neq B^n$.

Necessity. Let the code, V, be D-representable in $\left(B^n, \rho_C\right)$. Then the following holds true: for every vector, $y \in \bar{L}(C)$, the vector, $z \in L(C) \oplus y$ belongs only to one Dirichlet region, D_x, where $x \in V$. Then, according to Theorem 2, we have that $x \in V \bigcap \left(L(C) \oplus y\right)$. Consequently, the code, $V \bigcap \left(L(C) \oplus y\right)$, is D-representable in $\left(L(C) \oplus y, \rho_C\right)$.

Sufficiency. Let V be not D-representable in $\left(B^n, \rho_C\right)$. Then there is such vector, $z \in B^n$, that $z \in D_{x_1} \bigcap D_{x_2}$, where $x_1 \in V \bigcap L(C) \oplus y_1, x_2 \in V \bigcap L(C) \oplus y_2$, and $y_1, y_2 \in \bar{L}(C)$. The following cases are possible:

a) $y_1 = y_2, z \in L(C) \oplus y_1$;

b) $y_1 = y_2, z \notin L(C) \oplus y_1$;

c) $y_1 \neq y_2, z \notin L(C) \oplus y_1 \bigcup \left(L(C) \oplus y_2\right)$;

d) $y_1 \neq y_2, z \in L(C) \oplus y_1$.

It is not difficult to prove with these that in the space, $\left(L(C) \oplus y, \rho_C\right)$, including the vector, z, the code, $V \bigcap \left(L(C) \oplus y\right)$, is not D-representable, which is a contradiction. Q.E.D.

This theorem can be formulated in another way.

Corollary. The metric space, $\left(B^n, \rho_C\right)$, is partitioned into Dirichlet's regions of the points of the code, V, iff the metric space, $\left(L(C) \oplus y, \rho_C\right)$, is partitioned into Dirichlet's regions of the points, $x \in V \bigcap \left(L(C) \oplus y\right)$, for all $y \in \bar{L}(C)$.

We describe the algorithm of building the code, V, partitioning the metric space, $\left(B^n, \rho_C\right)$, into Dirichlet's regions.

Step 1. We choose an arbitrary code, $V(y)$, from the space, $L(C) \oplus y$, partitioning the metric space, $\left(L(C) \oplus y, \rho_C\right)$, into Dirichlet's regions for which $y \in \bar{L}(C)$.

Step 2. The code obtained through the formula:

$$V = \bigcup_{y \in \bar{L}(C)} V(y),$$

partitions the metric space, $\left(B^n, \rho_C\right)$, into Dirichlet's regions.

Let M any basis of the channel, A.

Theorem 4. If the code, V, is D-representable in the metric space, $\left(B^n, \rho_C\right)$, then the additive pair, $D_y, V \bigcap L(M) \oplus y$, is perfect for $y \in \bar{L}(M)$.

Proof. It follows from Theorem 3 that the code, $V \bigcap L(M) \oplus y$, is D-representable in $\left(L(M) \oplus y, \rho_M\right)$. As M is a basis for $L(M)$, then it follows from Theorem 4 [8] (taking Lemma 2 and Lemma 3 into account) that the code, $V \bigcap \left(L(M) \oplus y\right)$, is perfect in $\left(L(M) \oplus y, \rho_M\right)$. Applying Lemma 3 and Lemma 4, we get that the additive pair, $\left(D_y, V \bigcap \left(L(M) \oplus y\right)\right)$, is perfect for every vector, $y \in \bar{L}(M)$.

Q.E.D.

Nevertheless, we note that the perfectness of the additive pairs:

$$\left(A(y), V \bigcap \left(L(M) \oplus y\right)\right), y \in \bar{L}(M),$$

is not a sufficient condition for D-representability of the code, V, in $\left(B^n, \rho_M\right)$, though M is a basis for all $A(y)$.

Example:

9)
$$M = \{(1000),(0100),(0010),(0001)\},$$
$$V = \{(0000),(1111)\},$$
$$A = \{(0000),(1000),(0100),(0010),(0001),$$
$$(1100),(1010),(0110)\}$$

The code, V, is D-representable in $\left(B^4, \rho_A\right)$, but it is not D-representable in $\left(B^4, \rho_M\right)$, though the additive pair, (A, V), is perfect in B^4.

Theorem 5. If the additive pair, (A, V) is perfect, then V is D-representable in the metric space, $\left(B^n, \rho_A\right)$.

Proof. As $A^1(x) \subseteq D_x$ for every vector, $x \in V$, and $\bigcup_{x \in V} A^1(x) = B^n$, then $D_x = A^1(x)$. On the other hand, from perfectness of the code, V, it follows that the set, D_x, for all $x \in V$, disjoints. That is, V is D-representable.

Corollary. The additive pair, $((A, V)$ is perfect if the metric space, (B^n, ρ_A), is partitioned by the Dirichlet's regions, $D_x = A^1(x)$, of the points, x, from V.

Thus, we reduced the problem of building the perfect Pair, (A, V) to the problem of D-representability of the code, V, in the metric space, (B^n, ρ_A).

REFERENCES

[1] V. K. Leontyev and G. L. Movsisyan, "On the Additive Channel of Communication," *Reports of Academy of Sciences of Armenia*, Vol. 104, No. 1, 2004, pp. 23-27.

[2] V. K. Leontyev, G. L. Movsisyan and J. G. Margaryan, "Perfect Codes in Additive Channels," *Reports of RAS*, Vol. 411, No. 3, 2006, pp. 306-309.

[3] V. K. Leontyev, G. L. Movsisyan and J. G. Margaryan, "On Perfect Codes in Additive Channels," *Problems of Information Communication*, Vol. 44, No. 4, 2008, pp. 12-19.

[4] V. K. Leontyev, G. L. Movsisyan and J. G. Margaryan, "Codes in Additive Channels," *Report of the Academy of Sciences of Armenia*, Vol. 110, No. 4, 2010, pp. 334-339.

[5] F. J. M. Williams and N. J. A. Sloane, "The Theory of Error-Correcting Codes," Bell Laboratories, Marray Hill, 1977.

[6] V. K. Leontyev, G. L. Movsisyan and J. G. Margaryan, "Correction of Errors in the Additive Channel," *Vestnik RAU*, Vol. 2, No. 1, 2010, pp. 12-25.

[7] Yu. M. Movsisyan, "Higher Algebra and Number Theory," Yerevan State University, Yerevan, 2008, p. 455.

[8] V. K. Leontyev, G. L. Movsisyan and J. G. Margaryan, "Partition of N-Dimensional Space on GF(2) into Dirichlet's Regions," *Vestnik RAU*, Vol. 2, No. 1, 2011, pp. 26-41.