Open Journal of Discrete Mathematics, 2014, 4, 67-76
Published Online July 2014 in SciRes. http://www.scirp.org/journal/ojdm
http://dx.doi.org/10.4236/ojdm.2014.43010

Scientific Research

Classification of the Subsets B^n, and the Additive Channels

Vladimir Leontiev[1], Garib Movsisyan[2], Arthur Osipyan[1]

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

Received 24 April 2014; revised 23 May 2014; accepted 22 June 2014

Abstract

The problem of classification of the subset of the vertices of the *n*-dimensional unit cube in respect to all "shifts" by a vector from B^n is studied. Some applications for the investigation of the additive channels of communication are represented.

Keywords

Additive Channel, Code, Group, Stabilizer, Cardinality, Transitive Set

Let $F=\{0,1\}$ be a two element Galois field and F_2^n be an *n*-dimensional space on that field. In other words, F_2^n is the set of vertices of the n-dimensional unit cube, $B^n=\{0,1\}^n$. The subsets B^n have many different interpretations in the terms of Boolean function theory, or of correcting code theory, or of partially ordered set theory, or that of additive channels etc. And each of these theories is connected with a certain class of restrictions imposed on the properties of the subsets, B^n We consider the "shift" of the subsets B^n, and we define equvalence as equality that is accurate within the shift. To define the subsets stabilizers and the transitive subfamilies we use the classic ways connected with Burnside's Lemma.

Let $\binom{B^n}{m}$ be the family of all *m*-element subsets of the cube B^n. The transformation group B^n operates on this set as follows. For any $A\in\binom{B^n}{m}$ and $y\in B^n$ let the following is valid:

$$A+y=\{y+x \mid x\in A\}.$$

Thus $A+y$ is the shift of the set A on the vector y. The transitive set generated by A has the standard

How to cite this paper: Leontiev, V., Movsisyan, G. and Osipyan, A. (2014) Classification of the Subsets B^n, and the Additive Channals. *Open Journal of Discrete Mathematics*, **4**, 67-76. http://dx.doi.org/10.4236/ojdm.2014.43010

form:

$$G(A)=\{A+y \mid y\in B^n\}.$$

The family L_m^n of all transitive sets $G(A)$ generates the partition $\binom{B^n}{m}$:

$$\binom{B^n}{m}=\bigcup_{G(A)\in L_m^n} G(A).$$

The cardinality $|G(A)|$ of a transitive set is found in terms of the stabilizer G_A of the set A:

$$G_A=\{y\in B^n; A+y=A\}.$$

It is well known [1] [2] that G_A is a subsets in B^n and the cardinality of the transitive set $G(A)$ is equal to the index of the subsets G_A; that is:

$$|G(A)|=ind(B^n/G_A), \tag{1}$$

where $ind(B^n/G_A)=\dfrac{|B^n|}{|G_A|}$ is the index of the group B^n in regard to the subsets G_A.

Example.

1) Let A be a subgroup in B^n, and $\{H_1,H_2,\cdots,H_l\}$ be the family of cosets of the subgroup A, and $l=\dfrac{2^n}{|A|}$.

If we form the set:

$$M=\bigcup_{j=1}^{k} H_{i_j},$$

out of an arbitrary collection of the cosets $H_{i_1},H_{i_2},\cdots,H_{i_k}$, then $M\in\binom{B^n}{k|A|}$.

Let $x\in A$ and $y+A=H_i$ be an arbitrary cosets to the subgroup A; then $x+H_i=x+y+A=y+A=H_i$. Consequently, any element of the group, A, belongs to the stabilizer of the set M, and thus: $|G_M|\geq|A|$ and $|M|=k\cdot|A|$.

This example will be used in the sequel.

As (1) shows, to define the cardinality of the transitive set $G(A)$ it is sufficient to know the cardinality of the stabilizer G_A.

Let us note that the group G_A acts on the given set A, that is, G_A is a stabilizer and we can use the same way of argumentation as we did above.

If $x\in A$, then the transitive set $G(x)=\{x+y,\ y\in G_A\}$ is defined in the standard way and:

$$|G(x)|=ind(G_A/G_x), \tag{2}$$

where G_x is the stabilizer of the element, $x\in A$. Taking into account that:

$$G_x=\{y\in G_A : y+x=x\},$$

we have $G_x=\{0\}$, for all x. Then we have from (2):

$$|G(x)|=ind(G_A/E),$$

that is, $|G(x)|$ is equal to the index of the unit subgroup E, or:

$$|G(x)|=|G_A|.$$

Lemma 1. *The following comparison holds*:

$$|A|\equiv 0(\mathrm{mod}|G_A|).$$

This immediately follows from the formula of the partition A:

$$A = \bigcup_{x \in A} G(x).$$

If $\tau_p(n)$ is the power index of the prime number p, which is included in the canonic presentation n, then the following statements hold true:

Corollary 1. *The following inequality holds true*:

$$|G_A| \le 2^{\tau_2(|A|)}.$$

Corollary 2. *The stabilizer* $G_A = \{0\}$ *for any* $A \in \begin{pmatrix} B^n \\ 2m+1 \end{pmatrix}$.

Corollary 3. *Let* $A \in \begin{pmatrix} B^n \\ 4m+2 \end{pmatrix}$ *and* $y = \sum_{x \in A} x$ *Then either* $G_A = \{0, y\}$, *or* $G_A = \{0\}$.

Lemma 2. *The stabilizer* $G_A = \{0\}$ *for an arbitrary set* $A \in \begin{pmatrix} B^n \\ 4m \end{pmatrix}$ *if* $\sum_{x \in A} x \ne 0$.

Proof. We assume, $\exists y \ne 0,\ y \in G_A$. Then the elements of the set $A = \{x_1, x_2, \cdots, x_{4m}\}$ satisfy the following system:

$$\begin{cases} x_1 + y = x_{2m+1} \\ x_2 + y = x_{2m+2} \\ \quad \vdots \\ x_{2m} + y = x_{4m}. \end{cases}$$

Adding up all the equations of the system, we get the following equality: $\sum_{i=1}^{2m} x_i + \sum_{i=1}^{2m} y = \sum_{i=2m+1}^{4m} x_i$. From this it follows that: $\sum_{i=1}^{4m} x_i = 0$, which is a contradiction and it proves the Lemma.

In the general case, if the element y belongs to the stabilizer G_A of the subsets $A = \{x_1, x_2, \cdots, x_m\}$, the following holds true (according to the definition):

$$A + y = \{x_1 + y, x_2 + y, \cdots, x_m + y\} = A. \tag{3}$$

Let S_m be a symmetrical group of the degree m. We denote the elements of the group S_m corresponding to transformation (3) by g_y. Consequently, the element g_y should by written as follows:

$$g_y = \begin{pmatrix} x_1 & x_2 & \cdots & x_m \\ x_{i_1} & x_{i_2} & \cdots & x_{i_m} \end{pmatrix}.$$

We consider the expansion g_y into a product of independent cycles:

$$g_y = v_1 v \cdots v_k. \tag{4}$$

Lemma 3. *If* $g_y \ne \mathrm{e}$, *then* $|v_i| = 2$, $i = \overline{1,k}$.

Proof. If $v_r = (x_{i_1}, x_{i_2}, \cdots, x_{i_p})$, we have from (4):

$$\begin{cases} x_{i_1} + y = x_{i_2} \\ x_{i_2} + y = x_{i_3} \\ \quad \vdots \\ x_{i_p} + y = x_{i_1}. \end{cases} \tag{5}$$

It follows from (5) that:

$$x_{i_1} + y = (x_{i_p} + y) + y = x_{i_2} = x_{i_p},$$

that is, $p = 2$ Q. E. D.

To calculate the stabilizer one has to consider the multiset:

$$A+A=\left\{x_i+x_j; x_i, x_j \in A, \text{ where } i<j\right\},$$

which has a key role for the further considerations.

Let $A=\left\{x_1, x_2, \cdots, x_{2m}\right\}$, and:

$$A+A=\left\{\alpha_{ij}\left(x_i+x_j\right)\right\},$$

where α_{ij} is the multiplicity of the inclusion of the element, $\left(x_i+x_j\right)$, into $A+A$.

Lemma 4. *The stabilizer* G_A, *of the set* A, *is the sets of elements* $\left(x_i+x_j\right)$, *where each occurs m times plus the zero element.*

Proof. Let $\alpha_{ij}=m$ then the following holds true:

$$x_{i_p}+x_{j_p}=y; \quad p=\overline{1,m}.$$

Two different p,q pairs: $\left(x_{i_p}, x_{j_p}\right)$ and $\left(x_{i_q}, x_{j_q}\right)$, have no common elements; otherwise they coinside. Thus, the set of pairs $\left(x_{i_p}, x_{j_p}\right)$ form the partition A, and the point *y* belongs to G_A, according to Lemma 3.

From Lemma 4 a simple algorithm for building the stabilizer G_A follows and, as a matter of fact, it is reduced to building of the multiset, $A+A$. Complexity of such an algorithm is $O\left(m^2 n\right)$, where $|A|=2m$. The volume of the input information is the length of the recording of the set A, that is, $O(mn)$.

Lemma 5. *If the cardinality of the subsets* A *and that of the stabilizer* G_A *satisfy the following conditions*:

$$|A|=2^k, |G_A|>2^{k-2},$$

then:

$$|G_A|=2^k.$$

Proof. Let $|G_A|=2^{k-1}$ For any $x_1 \in A$ we build the set $A_1=\left\{x_1+y; y \in G_A\right\}$. We choose any element x_2 from $A \setminus A_1$ and define the set $A_2=\left\{x_2+y; y \in G_A\right\}$. We assume that there exists $x \in A_1 \cap A_2$. Then the vector x can be represented in two ways, namely:

$$x=x_1+y_1 \quad \text{and} \quad x=x_2+y_2$$

where $y_1, y_2 \in G_A$. Consequently, we get: $x_2=x_1+y_1+y_2 \in A_1$, which contradicts the choice of the element x_2. Hence, the following holds true:

$$A_1 \bigcap A_2=\varnothing. \tag{6}$$

Taking into account that $|A_1|=|A_2|=|G_A|=\frac{1}{2}|A|$ we have:

$$A_1 \bigcup A_2=A. \tag{7}$$

We denote $z=x_1+x_2$. Taking into account that $x_2 \notin A_1$, we have: $z \notin G_A$. It follows from (6) and (7) that $\forall x \in A$ is represented either in the form:

$$x=x_1+y_1, \text{ or } \quad x=x_2+y_2$$

where $y_1, y_2 \in G_A$. If $x=x_1+y_1$, then $x+z=x_1+y_1+z=x_2+y_1 \in A$. It can be proved in the same way that $x+z \in A$, for the case, $x=x_2+y_2$, Consequently, $z \in G_A$ We got a contradiction and it concludes the proof of Lemma 5 if we take into account Lemma 1.

Lemma 5 is a useful tool for calculation of the stabilizer G_A for $A \in \binom{B^n}{2^k}$. Its content can be interpreted as follows. If it is possible to define $2^{k-2}+1$ elements belonging to G_A, then, taking into account that the cardinality of a stabilizer is an exponent with the base 2, we directly get: $|G_A|=2^k$.

Examples.

2) *If* $m=1$, *then* $A=\left\{x_1, x_2\right\}$. *Consequently,* $A+A=\left\{x_1+x_2\right\}$. *Taking Lemma* 4 *into account, we get*:

$$G_A=\left\{x_1+x_2, 0\right\}$$

3) *If* $m=2$ *then* $A=\{x_1,x_2,x_3,x_4\}$ *Consequently*:

$$A+A=\{x_1+x_2,\ x_1+x_3,\ x_1+x_4,\ x_2+x_3,\ x_2+x_4,\ x_3+x_4\}$$

All the partitions into pairs of the set A are generated by one of them, for instance:

$$A=\{x_1,x_2\}\bigcup\{x_3,x_4\}.$$

It follows from this that if:

$$x_1+x_2=x_3+x_4,$$

then the following equalities hold true:

$$x_1+x_3=x_2+x_4,$$

$$x_1+x_4=x_2+x_3.$$

Consequently, the following statement holds true:

Statement 1. *If* $x_1+x_2+x_3+x_4=0,$ *then* $G_A=\{0,x_1+x_2,\ x_1+x_3,\ x_1+x_4\}$, *But if* $x_1+x_2+x_3+x_4\neq 0$ *then* $G_A=\{0\}$.

Examples.

4) *Let* $A=\{x_1=(0011),\ x_2=(1010),\ x_3=(1110),\ x_4=(0111)\}$ *Then*:

$A+A=\{2(x_1+x_2),2(x_1+x_3),2(x_1+x_3),2(x_1+x_4)\}=\{2(1001),2(1001),2(1101),2(1101),2(0100)\}$ *and* $G_A=\{(0000),(1001),(0100),(1101)\}$.

5) *Let* $A=\{x_1=(100),x_2=(010),x_3=(001),x_4=(110),x_5=(101),x_6=(011)\}$ *Then*:

$A+A=\{2(110),2(101),2(010),2(001),2(100),3(111),2(011)\}$ *And as* $m=3$ *then*: $G_A=\{(000),(111)\}$

Now let us calculate the number of the sets that are transitive in regard to the group B^n The tool for such calculation is Burnside's Lemma: [1] [2].

Lemma (Burnside's) 6. *The number* $\left|L_m^n\right|$ *of the equivalence classes or transitive sets is as follows*:

$$\left|L_m^n\right|=\frac{1}{2^n}\sum_{y\in B^n}\left|N(y)\right|,$$

where $N(y)$ *is the set of the (stationary) points* y *of the transformation, that is*:

$$N(y)=\left\{A\in\binom{B^n}{m};A+y=A\right\}.$$

Lemma 7. *The number of the solutions* $X\in\binom{B^n}{2m}$ *of the following equation*:

$$y+X=X, \tag{8}$$

is $\binom{2^{n-1}}{m}$, *if* $y\neq 0$.

Proof. According to Lemma 3, Equation (8) is equivalent to the system of the following equations:

$$\begin{cases} x_{i_1}+x_{i_2}=y \\ x_{i_3}+x_{i_4}=y \\ \quad\vdots \\ x_{i_{2m-1}}+x_{i_{2m}}=y, \end{cases} \tag{9}$$

where the partition $J=\{(12),(34),\cdots,(2m-1,2m)\}$ is chosen for the sake of certainty. Let us note that the following equation:

$$x+z=y, \tag{10}$$

has exactly 2^{n-1} solutions for $x,z\in B^n$ and it does not depend on y if $y\neq 0$. Indeed, choosing an x we get: $z=x+y$. Further, if (x,z) and (u,v) are two solutions of Equation (10), then either these solutions do not overlap, or they coinside. Indeed, we get $x+z+u+v=0$, from $x+z=y$ and $u+v=y$; consequently, it follows from $x=u$ that $z=v$ In the same way, if $x=v$, then $z=u$ Thus, all the solutions of system (9) can be obtained by choosing m pairs from 2^{n-1} pairs, which are solutions of (10).

Theorem 1. *The following equalities are valid*:

$$\left|L_{2m}^n\right|=\frac{1}{2^n}\left(\binom{2^n}{2m}+\left(2^n-1\right)\binom{2^{n-1}}{m}\right), \tag{11}$$

$$\left|L_{2m+1}^n\right|=\frac{1}{2^n}\binom{2^n}{2m+1}. \tag{12}$$

Proof. We get from Burnside's Lemma:

$$\left|L_k^n\right|=\frac{1}{2^n}\left|N(0)\right|+\frac{1}{2^n}\sum_{y\neq 0}\left|N(y)\right|=\frac{1}{2^n}\binom{2^n}{k}+\frac{1}{2^n}\sum_{y\neq 0}\left|N(y)\right|.$$

Then, for the case $k=2m$, taking into account Lemma 7, we get:

$$\left|N(y)\right|=\binom{2^{n-1}}{m}$$

For $y\neq 0$. This directly proves Formula (11).

For the case $k=2m+1$, taking into account Corollary 2, we get: $\left|N(y)\right|=0$ for all $y\neq 0$, which proves formula (12).

Thus, the above statements make, more or less, possible to know the structure of the stabilizer G_A of the set $A\in\binom{B^n}{m}$ and to find the number of the transitive sets $\left|L_m^n\right|$ which are generated by the action of the group B^n on $\binom{B^n}{m}$.

Let us also note that, according to Corollary 1, $\left|G_A\right|\le 2^t$, if $m=2^t(2q+1)$, where $A\in\binom{B^n}{m}$. On the other hand, as Example 1 shows, for any subgroup $A\in\binom{B^n}{2^t}$ and for any collection of contiguous classes $H_{i_1},\cdots,H_{i_k}$ of the group B^n in regard to A, then the set $M=\bigcup_{j=1}^{k}H_{i_j}$ is in the family $\binom{B^n}{2^t\cdot k}$ and $\left|G_M\right|\ge 2^t$

For an odd k $(k=2q+1)$ the cardinality of the set M is equal to $2^t(2q+1)$, and its stabilizer G_M has 2^t elements. This shows that it is possible to draw the above mentioned boundary for the stabilizers of the considered sets. The following example of a contiguous class $A=\left\{y\in B^n:\|y\|\equiv 1(\bmod 2)\right\}$ with the stabilizer $G_A=\left\{y\in B^n:\|y\|\equiv 0(\bmod 2)\right\}$ illustrates the above mentioned considerations, because $\left|G_A\right|=2^{n-1}$. Thus, the estimate $\left|G_A\right|\le 2^t$ for the case $\left|A\right|=2^t(2q+1)$ is not so bad evaluation for the cardinality of the stabilizer of the set A. The "average" value of this boundary in the whole interval of the cardinalities $\left[1,2^n\right]$, is $n/2$ and this can serve as a "realistic" boundary for the cardinality of the stabilizer for a uniform distribution on the family of the sets $\binom{B^n}{m}$.

The family L^n of all transitive sets $G(A)$, where $A\subseteq B^n$, generates the partition 2^{B^n}:

$$2^{B^n}=\bigcup_{G(A)\in L^n}G(A). \tag{13}$$

As $L^n = \bigcup_{m=1}^{n} L_m^n$, then, according to Theorem 1, we have for the numbers $|L_n|$ of the transitive sets the following equality:

Corollary 4.

$$|L_n| = \frac{1}{2^n}\sum_{i=0}^{[n/2]}\left(\binom{2^n+1}{2i+1} + (2^n-1)\binom{2^{n-1}}{i}\right).$$

Shifts and Additive Channels. One of the applications of the above considerations are the so called additive channels.

We call any subsets $A = \{y_0, y_1, \cdots, y_m\} \subseteq B^n$ additive channel [3] [4], if it carries out the following dictionary function:

$$x' = x + y_i, \text{Где } i = \overline{0,m}. \tag{14}$$

Thus, any word x, if transmitted through the additive channel A, is transformed into one of the words x' of (14), in the result of the shift by the vector y_i.

Definition 1 [5]. *We define the* k *th order neighbourhood of the vector,* $v \in B^n$, *in regard to* $C \subseteq B^n$, *as follows*:

$$C^k(v) = \{u + y: \ u \in C^{k-1}(v), \ y \in C\}, \ C^0(v) = \{v\}.$$

Definition 2. *The code,* $V = \{v_0 \cdots, v_N\}$, *corrects the errors of the additive channel* $A = \{y_0, \cdots, y_m\}$ *if the following condition holds true*:

$$A^1(v_i) \bigcap A^1(v_j) = \varnothing \quad \text{where} \quad i, j = \overline{0,N} \quad i \neq j.$$

The **equivalent definition** has the following form: *The code* $V = \{v_0, \cdots, v_N\}$ *corrects the errors of the additive channel* $A = \{y_0, \cdots, y_m\}$ *if the following condition holds true*:

$$v_i + v_j \neq y_r + y_s, \quad \text{where} \quad i, j = \overline{0,N}, \quad r, s = \overline{0,m}, \quad i \neq j. \tag{15}$$

As the k order cardinality does not depend on the vector v we denote:

$$A^k = |A^k(v)|.$$

Let us note that for the cardinality of the code V correcting the errors of the additive channel $A = \{y_1, \cdots, y_m\}$ the following boundaries hold true [3] [4]:

$$\frac{2^n}{A^2} \leq |V| \leq \frac{2^n}{A^1} \tag{16}$$

Actually, condition (15) makes possible to decode the initial message at the channel output through a standard "decoding table" of any word.

If one takes the sphere of radius t with the centre at zero as A, then he gets the classic channel through which there take place no more than *t* distortions of the form: $0 \to 1, 1 \to 0$.

The main problem when investigating a given additive channel A is the building the code V of the maximum cardinality, correcting the errors of the channel A. Consequently, each additive channel generates its own coding theory, and the possibilities of examining and sorting out all these communication tools are rather limited. At the same time, some most simple considerations show that many of these additive channels are equivalent (identical) in the sense of their content. Indeed, the channels, A and $A + y$, are equivalent for any $y \in B^n$, in the sense that any code V ,correcting the errors of the additive channel A corrects the errors of the additive channel $A + y$ as well, and vice versa. The above classification of the additive channels is based on these considerations. In particular, one can always consider that $(0 \cdots 0)$ belongs to the channel A otherwise one could pass to the equivalent channel including the zero vector, without any loss of generality.

Another definition of equivalence of additive channals is directly connected with the error correcting code.

Let $X(A,V)$ be a predicate given on the Cartesian product $2^{B^n} \times 2^{B^n}$ or:

$$X(A,V)=\begin{cases}1; & \text{if the code } V \text{ corrects the errors of the channel } A;\\ 0; & \text{if not.}\end{cases}$$

Definition 3 [5]. *The two additive channels* A *and* C *are equivalent if the following condition holds true for all* $V \subseteq B^n$:

$$X(A,V)=X(C,V). \tag{17}$$

Actually, condition (17) means that if the code V corrects the errors of the channel A, then the code V corrects the errors of the channel C as well, and vice versa. In particular, if:

$$T_x(A)=A+x,$$

(that is, $T_x(A)$ is a shift transformation) then:

$$T_x(A)\sim T_y(A),$$

for any pair of points $x, y \in B^n$,where the tilde sign $(\sim)$ means the notion of equivalence introduced above. We denote the equivalence class including the channel A by $M(A)$.

Example. $A=\{(000),(100),(101)\}, C=\{(010),(110),(111),(011)\}$.

One easily can see that these channels are equivalent though $|A|=3,$ and $|C|=4.$

Actually, in the general case, the channel cardinality is not any obstacle for classification and, in some certain cases, it defines the channel equivalence one to one.

Statement 2. *For any channel* A *with the cardinality* $|A|>2^{n-1}+1$ *the followingtakes place*:

$$M(A)=M(B^n).$$

Proof. It follows from (16) that any code V for which either $X(A,V)=1$, or $X(B^n,V)=1$, is consisted of one vector. On the other hand, for any code V consisted of one vectorthe following equality is valid:

$$X(A,V)=X(B^n,V)=1,$$

that is:

$$M(A)=M(B^n).$$

Q. E. D.

Note that the following example excludes the possibility of the contrary statement.

Example.

7) *Let*: $A=\{(0000),(1000),(0100),(0010),(0001),(1111)\}$. *Then*: $M(A)=M(B^n)$, *if* $|A|<2^3$.

Now let us go back to Example 6. We have:

$$G(A)\neq G(C),\quad |G(A)|=8,\quad |G(C)|=4.\quad M(A)=M(C)=G(A)\bigcup G(C).$$

It is obvious that this example is not an exception; therefore, we can use the following equality:

$$G(A)=\{T_x(A), x\in B^n\},$$

where $G(A)$ is the transitive set of the channel A in regard to the group of transformation B^n. We get:

$$G(A)\in M(A).$$

Taking into account (13), we state the following:

Theorem 2. *For any channel* $A\subseteq B^n$ *there exist the channels* $A_1,\cdots,A_k$ *from* B^n, *such that the partition* $M(A)=\bigcup_{i=1}^{k}G(A_i)$ *is unique.*

This theorem shows the connection between the classes of equivalence for communication channels and the transitive sets of subsets B^n, which are generated through the the action of the group B^n on them.

Though the expansion of $M(A)$ is unique, the transitive sets included in the expansion are generated by different collections of "basic" channels, $A_1, A_2, \cdots, A_k$.

We reduced the investigation of communication channels to the investigation of transitive sets, and thus the investigation of the latter is reduced to that of the classes of equivalence, which can further be described introducing the relations of partial order:

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

Consequently, we came to the necessity of introducing of an invariant of an equivalence class, characterizing the given order.

An invariant of any $M(A)$ is the set $A^2(0)$, including the zero vector, and this is its difference from the set $A + A$ which was defined above.

Theorem 3. *For any channels* $A = \{y_0, \cdots, y_{m_1}\}$ *and* $C = \{z_0, \cdots, z_{m_2}\}$ *the following holds*:

$$A \sim C \rightleftarrows A^2(0) = C^2(0)$$

Proof. Let: $A^2(0) = C^2(0)$, and the code $V = \{v_1, \cdots, v_N\}$ corrects the errors of the channel A. Then, taking into account (15), we have:

$$v_i + v_j \ne y_r + y_s, \text{ where } i, j = \overline{0, N}, \ r, s = \overline{0, m_1}, \ i \ne j.$$

Consequently, $v_i + v_j \notin C^2(0)$, which means that the code V corrects the errors of the channel C.

If $A^2(0) \ne C^2(0)$, then—without any loss of generality—we can assume that there exist $y \in A^2(0)$ and $y \notin C^2(0)$. We consider the code $V = \{0, y\}$. Let us show that V corrects the errors of the channel C, but does not correct the errors of the channel A. To prove this it is sufficient to show that both channels A and C include the zero point, and it can be done applying the shift transformation. Obviously, this transformation does not change the sets $A^2(0)$ and $C^2(0)$. The code $V = \{0, y\}$ corrects the errors of the channel C, because:

$$y + z_i \ne 0 + z_j.$$

But $y \in A + A$, that is, $y = y_i + y_j$. Hence:

$$y + y_i = 0 + y_j,$$

that is, the code V does not correct the errors of *A*. Q. E. D.

Unfortunately, the answer to the question: "is every set from B^n invariant under action of any equivalence class" is negative. For instance, all sets having cardinality 3 or 5 have no invariants from B^n.

Statement 3. *An equivalence class does not include more than one group.*

Proof. Let the channels, C_1 and C_2 be groups from $M(A)$. It follows from the following obvious equalities:

$$M(C_1) = C_1^2(0) = C_1,$$
$$M(C_2) = C_2^2(0) = C_2,$$

that $C_1 = C_2$. Q. E. D.

Statement 4. *If the group,* A, *is the equivalence class invariant of some channel* C, *then* $A \in M(C)$ *and it has the maximum cardinality in that equivalence class.*

In other words, a group channel is a "preferable generator" in its equivalence class.

Concluding, we note that the preceding definitions are symmetrical in regard to the pair (A,V) and, consequently, both the generation and correction of errors have the same essence. It means that all statements in regard to the communication channels A hold true in regard to the codes V of the pair (A,V).

References

[1] Lang, S. (1968) Algebra (in Russian). Moscow, Mir.

[2] Sachkow, W.N. (1977) Combinatric Methods of Descret Mathematics (in Russian). Nauka, Moscow.

[3] Leontiev, V.K., Movsisyan, G.L. and Margaryan, J.G. (2006) Perfect Codes in Additive Channels. *Reports of RAS*, **411**,

306-309 (in Russian).

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

[5] Leontiev, V.K., Movsisyan, G.L. and Margaryan, J.G. (2010) Correction of Errors in an Additive Channel. Vol. 2, Westnik RAU, 12-25 (in Armenian).

Scientific Research Publishing (SCIRP) is one of the largest Open Access journal publishers. It is currently publishing more than 200 open access, online, peer-reviewed journals covering a wide range of academic disciplines. SCIRP serves the worldwide academic communities and contributes to the progress and application of science with its publication.

Other selected journals from SCIRP are listed as below. Submit your manuscript to us via either submit@scirp.org or Online Submission Portal.