Armenian Journal of Mathematics
Volume 1, Number 3, 2008, 1–6

Algebraic communication channels*

V. K. Leontiev and Gh. L. Movsisyan
Moscow State University, Moscow, Russia

Abstract. Modern information theory studies various communication channels modelling certain situations. The basic matter of the present research is the information transmission process from a source to a receiver, and main parameters are the throughput/carrier capacity/transmission capacity and the information transmission speed.

Key words: Information theory, algebraic communication channels, words transformation.
Mathematics Subject Classification 2000: 94A13

In the same time in any communication channel transformation of some words in others occurs, i.e. certain word function is realized. After focusing our attention exactly on this fact, a number of new situations arises. We consider them in the present paper.

Let $B = \{a_1, a_2, ...a_m\}$ is a finite alphabet and let B^* is a set of all words of a finite length over the alphabet B. By a word function T we mean a mapping $B^* \xrightarrow{T} B^*$, which we generally consider as identically defined.

Instances:

1) if $B = \{0,1\}$ and $B^n = \{0,1\}^n$, then a word function of a form $B^n \to B$ is an ordinary/usual Boolean function depended on no more than n variables;
2) The word function of a form $f(x, y) = xy$ is called a concanetation.

*** Presented at the First International Algebra and Geometry Conference in Armenia, 16–20 May, 2007, Yerevan**

3) Consider a mapping $B^n \to B^n$ of the following form

$$T_y(x) = x \oplus y,$$

(1)

where $x, y \in B^n$, y is a parameter, which defines a mapping T, *and* $\oplus$ is an operation of summation by $\bmod 2$. The transformation collection $\{T_y(x)\}$ defines an additive communication channel. It is clear, that a transformation (1) is a special case of a general Affine transformation B^n into itself given by means of a Boolean matrix A and a vector и вектора b :

$$y = A_x + b$$

(2)

In other words, we can think that a collection of matrices $\{A_1, A_2, ...A_m\}$ is given, and every word x at the entry can be transformed in one of the following words at the exit: $y_1 = A_1 x + b_1, ...y_m = A_m x + b_m$. Channels of a form (1) are a generalization of the well-known additive communication channel , see [3], [1].

In the general case it is convenient to think that there is a finite word set $M \subseteq B^*$ and a transformation group $T = \{T_i\}$ such that $T(M) \subseteq M$.

Thus, every transformation belonging to a family T transfers a word from M into a word from the same set.

Definition. A family of transformations $T^* \subseteq T$ defines an algebraic channel, if the following condition is satisfied $T_i \in T^* \to T_i^{-1} \in T^*$

(3)

This condition requires that any "transformed" word could be returned at the initial form by means of "the same" transformations. The following definition duplicates a standard definition of an error-correcting code.

Definition. A set $V \subseteq M$ we call a code correcting errors of a channel T^*, if a condition

$T_i(u) \neq T\ (v)$

(4)

is satisfied for all $T_i, T_j \in T$ and for all words $u, v \in V$.

The condition (4) ensures an invertibility of every transformation from T on “the restriction” на "сужении" $V \subseteq M$ and, by virtue of this fact, possibility to restore the initial message by its “image”.

Definition. A neighbourhood of a 1-st order of a word $v \in M$ we call a word set $S^1(v)$**,** generated by a family of transformations T, i.e.

$$S^1(v) \overset{def}{=} \{T_i(v), T_i \in T\}$$

(5)

A neighbourhood of higher orders are defined inductively according to a formula

$$S^K(v) = (S^1(S^{K-1})(v))$$

(6)

In standard terms $S^1(v)$ is a column of the decoding table generated by word $v \in V$.

Every maximum efficiency code correcting errors of a channel Каждый код максимальной мощности, исправляющий ошибки канала T^* we call an optimal code, and the efficiencies of the corresponding code we denote by мы назовем оптимальным, а мощности соответствующего кода обозначим через $A(M, T^*)$.

The following statement represents standard boundary of a density packing method and a Varshamov-Hilbert boundary in terms of first and second order neighbourhoods [1], [2]

Let $S^1(M) = \min_{v \in M} |S^1(v)|$

$$S^2(M) = \max_{v \in M} \left| S^2(v) \right|$$

(7)

Theorem 1. The following estimations are valid

$$\frac{M}{S^2(M)} \le A(M, T^*) \le \frac{M}{S^1(M)}$$

(8)

A standard algorithm for construction of a code V, whose efficiency satisfies lower boundary from equation (8), consists in the following

1) As a point v_1 of a code V we choose an arbitrary word from a set M and construct a second order neighbourhood $S^2(v_1)$ of this word.
2) As a point v_2 we choose an arbitrary word $M_1 = M / S^2(v_1)$.
3) As a point v_K we choose an arbitrary word from $M_{K-1} = M / \bigcup_{i=1}^{K-1} S^2(v_i)$.
4) An algorithm finishes its work by a choice opportunity absence.

An efficiency of a code V constructed by means of this algorithm depends on a next point choice strategy. However, there are special classes of channels T^*, for which described procedure always leads to the code with the same efficiency $A(M, T^*)$.

Theorem 2. If a family of transformations T^* is a subgroup of a group T, then an optimal code efficiency is calculated by the following formula:

$$A(M,T^*)=\frac{1}{\left|T^*\right|}\sum_{Ti\in T}N(Ti)$$

(9)

where $N(T_i)$ is a number of fixed points of the transformation $T_{i,}$ i.e

$$N(T_i)=\left|v\in M:T_i(v)=v\right|$$

(10)

The formula (9) is a classic Burnside schema (see [4]) applied to the described above situation.

Corollary 1 [1]. If $T^*=\{y_1,y_2,...y_m\}$ is an additive channel generated by a group $G=\{y_1,y_2,...y_m\}$, i.e.

$$T_i(v)=v\oplus y \qquad i=\overline{1,m}$$

(11)

then the equity

$$A(B^n,G)=\frac{2^n}{m}$$

(12)

is valid.

Corollary 2. If $T^*=\{T_i\}$ is a group of cyclical shift on B^*, i.e.

$$T_K=(x_1,x_2,...x_n)=(x_{n-\kappa,}x_{n-\kappa+1}...)$$

then we have

$$A(B^n,T^*)=\frac{1}{n}\sum_{d/n}2^d\varphi\left(\frac{n}{d}\right)$$

and $\varphi(p)$ is the Euler function (function of a positive integer p is defined to be the number of positive integers less than or equal to p that are coprime to p).

Literature.

1. V. K. Leontiev, Gh. L. Movsisyan. On additive communication channel.
   Dokl. NAN Armenii. 2004 vol.104 №1, 23-28.
2. V. K. Leontiev, Gh. L. Movsisyan, Zh. G. Margaryan. Perfect codes in additive channels. Dokl. RAN. 2006., vol. 411 №3, 306-308.
3. M. E. Deza. Efficiency of detection and correction of noises. Problems of information transmission, 1965, vol.1, №3, 29-39.
4. J. De Braine. Theory of counting of Polya. Sb. "Prikladnaya combinatornaya matematika". 1968, M."Mir" 61-106.