PROCEEDINGS OF THE YEREVAN STATE UNIVERSITY

Physical and Mathematical Sciences 2012, № 2, p. 14–21

Mathematics

CODE VOLUME BOUNDARIES IN THE ADDITIVE CHANNEL

V. K. LEONT'EV[1], G. L. MOVSISYAN[2], Zh. G. MARGARYAN[3*]

[1] *Computer Centre, Russian Academy of Sciences, Moscow, Russia*
[2] *BIT Group, Moscow, Russia*
[3] *Chair of Discrete Mathematics and Theoretical Informatics YSU, Armenia*

One of the problems in the theory of coding is the code building of a maximum volume for the proposed additive channel. In this paper we have found and consequently presented the upper and the lower bounds for the code volume, which corrects the errors of the additive channel.

***Keywords*:** additive channel, upper and lower bounds, error-correcting.

Introduction. We consider an additive communication channel introduced in [1], as some information transformer, which is the generalization of the classic binary channel with limited number of distortions 0→1, 1→0. Many notions and facts in the present paper originate from the classic coding theory and are the direct analogues of the well known results [1–6].

The "noise" generated by the additive channel results to a word at the channel exit that is different from that at the channel entrance. This leads to necessity for introducing standard in the coding theory notions of corrective code, relay speed, decoding, etc.

One of the problems of the coding theory is construction of a code of the maximum volume for the given channel. In the present work upper and lower bounds for the error correcting code volume were obtained for the additive channel.

Codes in the Additive Channel. Let $B=\{0,1\}$ be the binary alphabet and B^* be the set of all words of finite length over the alphabet B, and $B^n=\{0,1\}^n$. It is convenient to consider in this paper the set B^n as an n-dimensional space over the field $B=\{0,1\}$.

If $A=\{y_0,y_1,\ldots,y_m\}$ is a subset in B^n, then the notion of an additive channel A is associated with A in the following way.

Each vector $x\in B^n$ is transformed in the channel A into one of the vectors of the following form: $y=x\oplus y_s$, $s=\overline{0,m}$, where $\oplus$ is the addition operation in the space B^n (addition modulo 2).

[*] E-mail: jiromr@mail.ru

Definition 1. For any $x \in B^n$ the set

$$A^t(x) = \left\{ u \oplus y : u \in A^{t-1}(x),\ y \in A \right\}$$

is could the *t*-order neighbourhood of x with respect to A. Here we assume that $A^0(x) = \{x\}$.

As the cardinality of number of elements in the *t*-order neighbourhood does not depend on the vector x, we denote it by $A^t = | A^t(x) |$.

Definition 2. We will say that the code $V = \{v_0, v_1, ..., v_N\}$ corrects errors of the additive channel $A = \{y_0, y_1, ..., y_m\}$ if $A^1(v_i) \cap A^1(v_j) = \varnothing,\quad i \neq j.$

Equivalently, *V* corrects the errors of A, if

$$v_i \oplus y_s \neq v_j \oplus y_r \tag{1}$$

or, in the symmetric form, $v_i \oplus v_j \neq y_s \oplus y_r$.

It is clear that the expressions above are symmetrical with respect to the pair (*A*, *V*), therefore, the notions of “error” generation and “error” correction have the same nature.

Statement 1. If the code *V* corrects the errors of the additive channel *A*, then the code *A* corrects errors of the additive channel *V*.

Note that the following estimate is given in [4] for the cardinality of number of elements in the code *V*, correcting the errors of the additive channel $A = \{y_0, y_1, ..., y_m\}$:

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

The code V, for which the upper bound is attained, is called a perfect code correcting the errors of the additive channel A.

To describe the “interrelations” of the additive channel *A* and its error-correcting code V, it is convenient to introduce the following binary predicate $X(A, V)$:

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

The predicate $X(A, V)$ has the following properties:

a) $X(A, V) = X(V,\ A)$.

This property immediately follows from the symmetry of the error-correcting condition (1).

b) $X(A \oplus x, V \oplus y) = X(V, A)$ for any $x, y \in B^n$.

c) $X(A, V) = X(TA, TV)$, where *T* is any invertible linear transformation *T*: $B^n \to B^n$ [1].

The property c) shows that the channels *A* and *TA* for any invertible linear transformation *T* share the same properties in the sense of error-correcting, therefore, it is natural to consider such channels as the same.

One of the main problems for the given channel A is the determination of the upper and lower bounds of the error-correcting code $V(A)$ of the maximum volume for the channel A. If the number of the elements of the channel A is fixed, then there are $\binom{2^n}{|A|}$ different additive channels and, as usual, it is reasonable to consider the maximum and the minimum of the cardinalities of error-correcting codes:

$$\overline{D_k}(n)=\max_{|A|=k}|V(A)|,\qquad \underline{D_k}(n)=\min_{|A|=k}|V(A)|.$$

The meaning of these functions were considered in [1] for the group code class and is obvious enough and it hardly needs in additional comments.

It is clear that there are as many additive channels as there are Boolean functions and, as the properties b) and c) show, some of them do not essentially differ from each other. Is not clear what the classification of such channels looks like, but the following definition correspond to the general point of view.

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

The equivalence makes possible to look for the additive channels with the "best" and "worst" correcting properties for each $m<2^n$.

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

Statement 3. If $X(A,V)=1$, then $|A\cap V|\le 1$.

It follows from the preceding statements that, without loss of generality, we can assume that:

a) if $\{A\}$ is the class of additive channels equivalent to A, then it is sufficient to solve the problem for any representative of this class;

b) the additive channel A contains the zero vector, which can be interpreted as possibility of errorless transfer of the signal through the channel.

It follows from the equality $X(A,V)=1$ that $X(V,A)=1$, hence, analogical statement holds for the code V too; i.e. it is sufficient to consider only codes containing the zero vector.

Thus, it follows from $X(A,V)=1$ that the sets A and V can overlap only at zero, and we must look for the elements of the code V in $\{B^n\setminus A\}\cup\{(00...0)\}$. Further we denote

$$y_0=(00...0)\in A,\ \ v_0=(00...0)\in V.$$

The Code Volume Bound in the Additive Channel. Let $A=\{y_0,y_1,...,y_m\}$ and $\{y_0,y_1,...,y_r\}$ be a basis in A. Let us consider any basis $\{z_0,z_1,...,z_n\}$, in the space B^n, where $z_i=y_i,\ \ i=\overline{1,r}$, and let f be a linear invertible transformation $f:B^n\to B^n$, defined as follows:

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

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

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

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

The following statements hold.

Lemma 1. The image $f(V(A))$ of the code $V(A)$ is a maximum code for the channel $f(A)$ and $|V(A)|=|V(f(A))|$.

Proof. Since $X(A,V(A))=1,\ X(f(A),f(V(A)))=1,$ we have $|V(f(A))|\geq|f(V(A))|=|V(A)|$. On the other hand, from $X(f(A),V(f(A)))=1$ we obtain: $X(f^{-1}(fA)),f^{-1}(V(f(A)))=1, f^{-1}(V(f(A)))=1.$

Hence, $f^{-1}(V(f(A)))$ is a error-correcting code for the channel A, that is

$$|V(f(A))|\leq|V(A)|.$$

The Lemma is proved.

We denote $C\times D=\{(xy)\in B^{n_1+n_2};\ x\in C,\ y\in D\}$ for any $C\subseteq B^{n_1},D\subseteq B^{n_2}$.

It is obvious that $|C\times D|=|C|\times|D|$ and $B^{n_1}\times B^{n_2}=B^{n_1+n_2}$.

Let

$$\tilde{A}=\{\tilde{y}_0,\tilde{y}_1,...,\tilde{y}_m\}\subseteq B^{n_1}\text{ and } A=\tilde{A}\times 0^{n_2}=\{y_0,y_1,...,y_m\}\subseteq B^{n_1+n_2},$$

where $y_i=(\tilde{y}_i0^{n_2}),\ i=\overline{0,m}.$

Lemma 2. If $X(\tilde{A},\tilde{V})=1$ for some $\tilde{V}\subseteq B^{n_1}$, then $X(A,V)=1,$ where $V=\tilde{V}\times B^{n_2}\subseteq B^{n_1+n_2}$.

Proof. Assume that $X(A,V)=0$, which means that there are $v_i,v_j\in V$ and $y_l,y_s\in A$ such that $v_i\oplus v_j=y_l\oplus y_s,\ i\neq j,\ l\neq s$.

Let

$$v_i=(\tilde{v}u_1),\ \tilde{v}\in\tilde{V},\ u_1\in B^{n_2}\text{ and } v_j=(\tilde{u}u_2),\ \tilde{u}\in\tilde{V},\ u_2\in B^{n_2}.$$

Then

$$v_i\oplus v_j=(\tilde{v}u_1)\oplus(\tilde{u}u_2)=((\tilde{v}\oplus\tilde{u})(u_1\oplus u_2)).$$

Hence, it follows from the definition of A that $u_1=u_2$. Consequently, $\tilde{v}\neq\tilde{u}$, implying that $\tilde{v}\oplus\tilde{u}=\tilde{y}_l\oplus\tilde{y}_s$, which contradicts to $X(\tilde{A},\tilde{V})=1$.

The Lemma is proved.

Let

$$V(A)=\{v_0,v_1,...,v_N\}\subseteq B^{n+n_2},\text{ where } v_i=(a_ib_i),\ a_i\in B^{n_1},\ b_i\in B^{n_2},\ i=\overline{0,N}.$$

Also let $\{\tilde{v}_0,\tilde{v}_1,...,\tilde{v}_{N_1}\}\in B^{n_1}$, $\{\tilde{u}_0,\tilde{u}_1,...,\tilde{u}_{N_2}\}\subseteq B^{n_2}$ are the maximum cardinality subsets from $\{a_0,a_1,...,a_N\}$ and $\{b_0,b_1,...b_N\}$ respectively, satisfying the conditions: $\tilde{v}_i \neq \tilde{v}_j$, where $i, j \in (0, N_1)$, $\tilde{u}_i \neq \tilde{u}_j$, $i, j \in (0, N_2)$.

We want to prove that $\left\{\tilde{u}_0, \tilde{u}_1, ..., \tilde{u}_{N_2}\right\} = B^{n_2}$.

If there is some element $u \in B^{n_2} \setminus \left\{\tilde{u}_0, \tilde{u}_1, ..., \tilde{u}_{N_2}\right\}$, then for any v, v_i, $i = \overrightarrow{0, N}$, and for $d \in B^{n_1}$ the vector $v_i \oplus (du)$ can be represented in the form (ab), where $a \in B^{n_1}$, $b \in B^{n_2}$, $b \neq (00...0)$. As the vector $y_s \oplus y_t$, $s \neq t$, can be represented in the form $(c0^{n_2})$ with $c \in B^{n_1}$, we deduce that $X(A, Q) = 1$ for the code $Q = V(A)U(du) \subseteq B^{n_1+n_2}$, which contradicts to the fact that $V(A)$ is a maximum code. Let us consider the set

$$M_b = \left\{v \in B^{n_1};\, v \in \left\{v_0, v_1, ..., v_{N_1}\right\};\, (vb) \in V(A)\right\}$$

for any vector $b \in B^{n_2}$.

Since $X(\tilde{A}, M_b) = 1$ for any $u, v \in M_b$, $u \neq v$, $u \oplus v = \tilde{y}_s \oplus \tilde{y}_t$, $s \neq t$, then $ub \oplus v\tilde{b} = y_s \oplus y_t$ for $b, \tilde{b} \in B^{n_2}$. This contradicts to the fact that $X\left(A, V\left(A\right)\right) = 1$. It is obvious that:

1. $M_b \bigcap M_{\tilde{b}} = \varnothing$,
2. $\bigcup\limits_{b \in B^{n_2}} M_b = V(A)$,
3. $\left|M_b\right| \leq \left|V(\tilde{A})\right|$.

Consequently, $\left|V\left(A\right)\right| = \left|\bigcup\limits_{b \in B^{n_2}} M_b\right| = \sum\limits_{b \in B^{n_2}} \left|M_b\right| \leq \sum\limits_{b \in B^{n_2}} \left|V\left(A\right)\right| = \left|V\left(\tilde{A}\right)\right| 2^{n_2}$.

From this mequality and Lemma 2 we obtain that $\left|V(A)\right| = \left|V\left(\tilde{A}\right)\right| 2^{n_2}$, that is:

Lemma 3. For any A of the mentioned type $\left|V(A)\right| = \left|V\left(\tilde{A}\right)\right| 2^{n_2}$, and $V(\tilde{A}) \times B^{n_2}$ is the maximum error-correcting code for the channel A.

In the rest we denote the rank of any subset $M \subseteq B^n$ by $r(M)$.

According to Lemma 1, we can always assume that the vectors of the channel $A = \left\{y_0, y_1, ..., y_m\right\} \subseteq B^n$ have the form $y_i = \left(\tilde{y}_i 0^{n-r(A)}\right)$, $i = \overline{0, N}$.

Consequently,

$$\tilde{A} = \left\{\tilde{y}_0, \tilde{y}_1, ..., \tilde{y}_m\right\} \subseteq B^{r(A)} \text{ and } \left]\log_2\left(m+1\right)\right[\leq r\left(A\right) \leq m.$$

Statement 4. If $r\left(A\right) = \left]\log_2\left(m+1\right)\right[$, then $\left|V\left(A\right)\right| = 2^{n -]\log_2(m+1)[}$.

Proof. According to Lemma 3, $V\left(A\right) = V\left(\tilde{A}\right) 2^{n -]\log_2(m+1)[}$, where $r\left(\tilde{A}\right) = \left]\log_2\left(m+1\right)\right[$. As $V(\tilde{A}) \leq 2^{n - \left[\frac{2^{]\log_2(m+1)[}}{m+1}\right]}$ and $\left]\log_2\left(m+1\right)\right[- 1 < \log_2\left(m+1\right)$, hence, $1 \leq \dfrac{2^{]\log_2(m+1)[}}{m+1} < 2$, consequently, $\left|V\left(\tilde{A}\right)\right| = 1$.

Statement 5. If $r(A)=m,$ then $\left|V(A)\right| \le \left[\dfrac{2^m}{(m+1)}\right]2^{n-m}$. The proof follows from Lemma 3, taking into account the Hamming's upper bound.

Lemma 4. If for the channel $A=\{y_0,y_1,...,y_m\}$ $r(A)<m,$ then there are $C,V\subseteq B^n$, $X(C,V)=1$ such that $r(C)=r(A)+1$ and $|V|=|V(A)|$, $|C|=m+1$.

Proof. From the condition $r(A)<m$ it follows that one can choose an element $y\in\tilde{A}$ such that $r\left(\tilde{A}\setminus y\right)=r(A)$. Let $y=\tilde{y}_m$. We consider the set

$$\tilde{C}=\left\{(\tilde{y}_0 0),(\tilde{y}_1 0),...,(\tilde{y}_{m-1}0),\, e_{r(A)+1}\right\}\subseteq B^{r(A)+1}.$$

It is obvious that $r(\tilde{C})=r(\tilde{A})+1=r(A)+1$, $|\tilde{C}|=|A|=m+1$.

Let $V(\tilde{A})=\left\{v_0,v_1,...,\tilde{v}_{N_1}\right\}$. We construct the following code $\tilde{V}_1$:

$$\tilde{V}_1=\left\{((V(\tilde{A})\times 0)\cup((V(\tilde{A})\times 0)\oplus(y0)\oplus e_{r(A)+1})\right\}.$$

Since for any $i,j\in\overline{0,N_1}$ we have $(\tilde{v}_i 0)\ne(\tilde{v}_j 0)\oplus(y0)\oplus\left(e_{r(A)+1}\right)$, then $\left|\tilde{V}_1\right|=2\left|V(\tilde{A})\right|$.

Next we prove that $X\left(\tilde{C},\tilde{V}_1\right)=1$.

Let us assume that there exist some pairs of vectors $a_1,a_2\in\tilde{V}_1$, $a_1\ne a_2$, and $b_1,b_2\in\tilde{C}$, $b_1\ne b_2$, such that

$$a_1\oplus a_2=b_1\oplus b_2. \qquad (2)$$

Let us consider the following cases:

1. If $a_1=(\tilde{v}_i 0)$, $a_2=(\tilde{v}_j 0)$, $i\ne j$, then $b_1=(\tilde{y}_s 0)$, $b_2=(\tilde{y}_l 0)$ for $s,l\in(0,m-1)$, $s\ne l.$

Hence, $\tilde{v}_i\oplus\tilde{v}_j=\tilde{y}_s\oplus\tilde{y}_l$, and this contradicts to $X\left(\tilde{A},V\left(\tilde{A}\right)\right)=1$.

2. If $a_1=(\tilde{v}_i 0)$, $a_2=(\tilde{v}_j 0)\oplus(y0)\oplus\left(e_{r(A)+1}\right)$, then, using (2), we obtain

$$b_1\oplus b_2=(\tilde{y}_l 1),\ l\in(0,m-1).$$

That is $\tilde{v}_i\oplus\tilde{v}_j\oplus\tilde{y}_m=\tilde{y}_l$, and this contradicts to $X(\tilde{A},V(\tilde{A}))=1$, too.

3. If $a_1=(\tilde{v}_i 0)\oplus(y0)\oplus\left(e_{r(A)+1}\right)$, $a_2=(\tilde{v}_j 0)\oplus(y0)\oplus\left(e_{r(A)+1}\right)$, $i,j\in(0,N_1)$, then

$$b_1\oplus b_2=(\tilde{y}_s\oplus\tilde{y}_l,0),\ s,l\in(0,m-1),\ s\ne l.$$

Consequently, $\tilde{v}_i\oplus\tilde{v}_j=\tilde{y}_l\oplus\tilde{y}_s$, and this is a contradiction. Hence, $X\left(\tilde{C},\tilde{V}_1\right)=1$.

Let us consider the set $C=\tilde{C}\times 0^{n-r(\tilde{C})}\subseteq B^n$ and the code $V=\tilde{V}_1\times B^{n-r(\tilde{C})}$ that corrects the errors of C. It follows from Lemma 2 that $X(C,V)=1$, because $r\left(\tilde{C}\right)=r(A)+1$, and then, taking into account Lemma 3, we get

$$|V| = |\tilde{V}_1| 2^{n-r(\tilde{C})} = 2|V(\tilde{A})| 2^{n-r(A)-1} = |V(A)|.$$

The Lemma is proved.

Theorem. For any $1 \le m+1 \le 2^n$

$$2^{n-]\log_2(m+1)[} \le \bar{D}_{m+1}(n) \le \left[\frac{2^m}{(m+1)}\right] 2^{n-m}.$$

Proof. Since $]\log_2(m+1)[\le n$, then there are $]\log_2(m+1)[$ linearly independent vectors in B^n generating a subspace that contains some channel $A \subseteq B^n$ with

$$r(A) =]\log_2(m+1)[, \quad |A| = m+1.$$

According to Statement 4 and as was obtained by other methods in [2], $\bar{D}_{m+1}(n) \ge 2^{n-]\log_2(m+1)[}$.

Concerning to the upper bound, let $A \subseteq B^n$ be an additive channel satisfying

$$|A| = m+1, \quad |V(A)| = \bar{D}_{m+1}(n).$$

Let us consider the case $m \le n.$

If $r(A) = m,$ then we have, according Statement 5,

$$|V(A)| = \left[\frac{2^m}{(m+1)}\right] 2^{n-m}.$$

If $r(A) < m$, then it follows from Lemma 4 that there are pairs (A_i, V_i), $A_i \subseteq B^n$, $V_i \subseteq B^n$, $i = \overline{1, m-r(A)},$ such that $|A_i| = |A| = m+1,$ $X(A_i, V) = 1,$ $r(A_i) = r(A) + i.$ Then $\bar{D}_{m+1}(n) = |V(A)| = |V_1| = |V(A_1)| = |V_2| = |V(A_2)| = \ldots = |V_{n-r(A)}| = |V(A_{m-r(A)})|$.

As $r\left(A_{m-r(A)}\right) = m,$ then it follows from Statement 5 that

$$\bar{D}_{m+1}(n) \le \left[\frac{2^m}{(m+1)}\right] 2^{n-m}.$$

Now we consider the case when $m > n$. Let $A_1 = A \times 0^{m-n} \subseteq B^m$. As $r(A) = r(A_1), |A_1| = |A|,$ then we have from Lemma 3: $V(A_1) = V(A) \times B^{m-n}$.

Consequently, $|V(A_1)| = |V(A)| 2^{m-n}.$

According to the previous case, we get

$$|V(A_1)| \le \left[\frac{2^m}{(m+1)}\right],$$

hence, $\bar{D}_{m+1}(n) = |V(A)| = \dfrac{|V(A_1)|}{2^{m-n}} \le \left[\dfrac{2^m}{(m+1)}\right] 2^{n-m}.$

The Theorem is proved.

Corollary 1. $\underline{D}_{m+1}(n) \le 2^{n-]\log_2(m+1)[}$.

Corollary 2. If $m = 2^s - 1,$ then $\bar{D}_{m+1}(n) = 2^{n-s}.$

Corollary 2 can be formulated in the following way: for any integer $s \leq n$ there is a channel $A \subseteq B^n$ of cardinality 2^s, for which $V(A)$ is a perfect code.

But one cannot assert that the condition $|A| = 2^s$ is sufficient. That is, the maximum cardinality error-correcting code for the channel A when $|A| = 2^s$ is not always perfect.

An Example. For $n = 90$ there is no error-correcting code for the additive channel $A^2(y_0)$, where $A \setminus \{y_0\} \subseteq B^{90}$ is the basis, but $|A^2(y_0)| = 2^s$.

The proof of this statement for the metrics of Hamming can be found in [7]: the proof follows from the fact that there is no binary perfect code correcting 2-errors, except the trivial ones.

Received 05.04.2012

REFERENCES

1. **Deza M.E.** On Correcting of an Arbitrary Noise and the Worst Noise. Theory of Information Transfer. M.: Nauka, 1964, p. 26–31 (in Russian).
2. **Deza M.E.** // Problemy Peredachi Informacii, 1965, v. 1, № 3, p. 29–38 (in Russian).
3. **Leont'ev V.K., Movsisyan G.L.** // Doklady NAN RA, 2004, v. 104, №1, p. 23–27 (in Russian).
4. **Leont'ev V.K., Movsisyan G.L., Margaryan Zh.G.** // Doklady RAN, 2006, v. 411, № 3, p. 306–309 (in Russian).
5. **Leont'ev V.K., Movsisyan G.L., Margaryan Zh.G.** // Problemy Peredachi Informacii, 2008, v. 44, № 4, p. 12–19 (in Russian).
6. **Leont'ev V.K., Movsisyan G.L., Margaryan Zh.G.** // Doklady NAN RA, 2010, v. 110, № 4 (in Russian).
7. **McWilliams Ph.G., Sloane N.J.A.** The Theory of Error-Correcting Codes. M.: Svyaz, 1979, 762 p. (in Russian).