Journal of Information Security, 2016, 7, 165-171
Published Online April 2016 in SciRes. http://www.scirp.org/journal/jis
http://dx.doi.org/10.4236/jis.2016.73012

Construction of New Codes from Given Ones in an Additive Channel

Garib Movsisyan

BIT Group, Moscow, Russia
Email: garib@hkzap.ru

Received 18 February 2016; accepted 8 April 2016; published 11 April 2016

Abstract

In the present work, a construction making possible creation of an additive channel $A \subseteq B^n$ of cardinality s and rank r for arbitrary integers s, r, n ($r \le \min(n, s-1)$), as well as creation of a code $V \subseteq B^n$ correcting errors of the channel A is presented.

Keywords

Additive Channel, Golay Code, Classical Coding Theory, T-Order Neighborhood, Correcting Code, Binary Alphabet, Cardinality

1. Introduction

We consider an additive communication channel introduced in [1] as some transformer of information which is a generalization of the classical binary channel with a limited number of distortions: $0 \to 1, 1 \to 0$. Many notions and facts in the present paper have taken their roots in classical coding theory and are direct analogues of well known results [1]-[6].

The "noise" generated by an additive channel leads to a word at the exit of the channel which differs from the transmitted one. This circumstance makes one to find the leads to creation of necessary initial prerequisites for introducing standard notions of an error correcting code in the coding theory, as well as the notions of the speed of communication, decoding etc.

Thus, the problem of constructing new codes from known ones has certain interest for coding theory. In this work, using certain combinatory constructions, some new codes for additive communication channels are constructed (also see [7] [8]). This problem has particular interest especially if new codes are "optimal" in one of

How to cite this paper: Movsisyan, G. (2016) Construction of New Codes from Given Ones in an Additive Channel. *Journal of Information Security*, **7**, 165-171. http://dx.doi.org/10.4236/jis.2016.73012

well known senses.

2. Codes in an Additive Channel

Let $B=\{0,1\}$ be a binary alphabet; B^* be the set of all words with finite lengths in the alphabet B, and $B^n=\{0,1\}^n$. In this paper it is convenient to take the set B^n as an n-dimensional vector space in the field $B=\{0,1\}$ of 2 elements.

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

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

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

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

Definition 1. *The following set*:

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

is called the t-order neighborhood with respect to A of any vector $x\in B^n$, and $A^o(x)=\{x\}$.

As the cardinality of the t-order neighborhood does not depend on the vector x, we use the denotation: $A^t=|A^t(x)|$.

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*:

$$A^1(v_i)\cap A^1(v_j)=\varnothing, \text{ for } i\neq j.$$

An equivalent writing of this condition has the following form:

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

or here is another one which is symmetrical to the preceding one:

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

Below, without loss of generality, we take:

$$y_0=(00\cdots0)\in A,\ v_0=(00\cdots0)\in V.$$

Let us note that for the cardinality of the code V correcting the errors of the additive channel $A=\{y_0,y_1,\cdots,y_m\}$ the following limits hold true [3]:

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

Besides, the code V for which the upper limit is reached is called the perfect code correcting the errors of the additive channel A.

To describe 'interrelations' of the additive channel A and the code V correcting the errors of this channel, the following convenient two-place predicate $X(A, V)$ is introduced:

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

If the cardinality of the channel A is fixed, then there exist $\binom{2^n}{|A|}$ various additive channels and, as usual, consideration of the following upper limit of the cardinality of the corresponding correcting codes is expedient:

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

here $V(A)$ is the code of the maximum volume correcting the errors of the channel A.

The Hamming metric is a standard and mostly used metric in theory of coding, defined by the following func-

tion:

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

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

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

It is clear that choosing another basis $M = \{y_1, y_2, \cdots, y_n\}$ we generate another metric:

$$x = \sum_{i=1}^{n} \beta_i y_i \to \|x\|_M = \sum_{i=1}^{n} \beta_i .$$

A more general procedure of metric generation is as follows. For a given subset $M = \{y_1, y_2, \cdots, y_m\} \subseteq B^n$ and a vector $x \in B^n$ we consider all expansions of x with respect to M, that is, the expansions of the following form:

$$x = \sum_{i=1}^{m} \alpha_i y_i . \tag{1}$$

And for each such representation, we juxtapose the following number:

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

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

$$\|x\|_M = \begin{cases} \min\left\{\sum \alpha_i\right\}, \text{with respect to representation } (1), \\ \infty, \text{ if there is not such representation.} \end{cases} \tag{2}$$

The function $\| \ \|_M$ is a metric (below, the MLM metric) for an arbitrary subset $M \subseteq B^n$ (see [6]).

3. Constructing New Codes from the Given Ones in an Additive Channel

Let $A = \{y_0, y_1, \cdots, y_m\} \subseteq B^n$ and $\{y_1, y_2, \cdots, y_r\}$ be a basis for A. We consider an arbitrary basis $\{z_1, z_2, \cdots, z_n\}$ of 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:

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

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

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

It is clear that if $(\alpha_1 \alpha_2 \cdots \alpha_n) \in f(A)$, then $\alpha_i = 0$ for all $i = \overline{r+1, n}$.
According to [9], the following statement holds true.

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

Theorem 1. *For all* $0 \le m \le 2^n - 1$ *the following inequality holds true*:

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

Corollary 1. *If* $m = 2^s - 1$, *then* $\bar{D}_{m+1}(n) = 2^{n-s}$.
This corollary can be paraphrased as follows.

If $m=2^S-1$, (*s is an integer*), *then there exists a channel* $A\subseteq B^n$ *with the cardinality* $m+1$ *for which* $V(A)$ *is a perfect code.*

Anyhow, one cannot assert that the condition $|A|=2^s$ is sufficient. This means that $V(A)$ is not always a perfect code for $|A|=2^s$.

Example 1. For instance, if $n=90$ there does not exist a perfect code correcting the errors of the additive channel $A^2(y_0)$, where $A\setminus y_0\subseteq B^{90}$ is the basis, and $A^2=2^{12}$.

For Hamming metric the proof of this fact can be found in [10], and this proof states that there does not exist a binary perfect code correcting binary errors except the trivial ones. And for the MLM metric, this fact is established in [11] by the following theorem.

Theorem 2. *The non-trivial perfect codes, correcting the errors of the additive channel* $A^t(y_0)$, *exist only for the following values of n and t*:

(*a*) $n=2^e-1, t=1$,

(*b*) $n=23, t=3$.

If $A=\{y_0,y_1,\cdots,y_m\}$ is an arbitrary additive channel, then the set A generates a MLM metric in B^n, given by formula (2). The statement presented below shows [11] that the ability of the code $V=\{v_0,v_1,\cdots,v_N\}$ of correcting the errors of the additive channel can be formulated in terms of the MLM metric generated by the set A.

Lemma 2. *The code V corrects the errors of the additive channel A, if the following conditions hold true*:

$$\rho_A(v_i,v_j)\geq 3,\ i,j=1,N.$$

Now we consider the set $A_1=((A\setminus y_m)\times 0)\cup e_{n+1}$, as well as the code $V_1=(V\times 0)\cup((V\times 0)\oplus(y_m 0)\oplus e_{n+1})$.

Theorem 3. *The code* $V_1\subseteq B^{n+1}$ *corrects the errors of the additive channel*

$A_1=\{y_0 0, y_1 0,\cdots,y_{m-1}0,e_{n+1}\}\subseteq B^{n+1}$.

Proof. Taking into account **Lemma 2**, it is sufficient to prove that the following inequality holds true:

$$\rho_{A_1}(v_i,v_j)\geq 3;\ v_i,v_j\in V_1, i\neq j.$$

Let us consider two cases:

1) $v_j\oplus v_j\in V\times 0$.

Then it is not difficult to prove that

$$\rho_{A_1}(v_i,v_j)=\rho_A(\tilde{v}_i,\tilde{v}_j),$$

where $v_i=\tilde{v}_i\alpha, v_j=\tilde{v}\alpha$, $\alpha\in\{0,1\}$, $\tilde{v}_i,\tilde{v}_j\in v$.

As $X(A,V)=1$, then it follows from Lemma 2 that $\rho_{A_1}(v_i,v_j)=\rho_A(\tilde{v}_i,\tilde{v}_j)\geq 3$.

2) $v_j\oplus v_j\in(V\times 0)\oplus(y_m 0)\oplus e_{n+1}$.

Then $\rho_{A_1}(v_i,v_j)=\rho_A(\tilde{v}_i,(\tilde{v}_j\oplus y_m))$. As $\tilde{v}_i,\tilde{v}_j\oplus y_m\in V$, then it follows from **Lemma 2** that $\rho_{A_1}(v_i,v_j)=\rho_A(\tilde{v}_i,\tilde{v}_j\oplus y_m)\geq 3$. Consequently, again applying to **Lemma 2**, we get $X(A_1,V_1)=1$.

The theorem is proved.

Without any loss of generality we can take $y_i=e_i, i=\overline{1,r(A)}$.

Applying **Theorem 3** sequentially to the pair $A,V\subseteq B^n$, we construct the pair $A_i,V_i\subseteq B^{n+i}$:

$$A_i=\left(\left(A\setminus\left(\bigcup_{j=1}^{i}y_{r(A)+j}\right)\right)\times 0^i\cup\left(\bigcup_{j=1}^{i}e_{r(A)+j}\right)\right),$$

$$V_i=\bigcup_{z=(z_1z_2\cdots z_i)\in B^i}\left((V\times 0^i)\oplus x(z)\right),$$

where the vector $x(z)\in B^{n+i}$ is defined in the following way:

$$x(z)=\sum_{j=1}^{i}z_j\left(y_{r(A)+j}\oplus e_{r(A)+j}\right).\qquad(3)$$

The code V_i is the combination of 2^i various shifts of $x(z)$ for $V\times 0^i$, where $x(z)$ are some vectors chosen in a "convenient" way.

From this we have:

$$A_i, V_i \subseteq B^{n+i}, |V_i| = 2^i |V|, r(V_i) \geq r(V_{i-1}), X(A_i, V_i) = 1.$$

Now, the proof of the following theorem is not difficult.

Theorem 4. *If* $X(A,V)=1; A,V \subseteq B^n$, *then for any integer r, satisfying the condition* $r(A) \leq r \leq \min(n, |A|-1)$, *there exists such a pair* $A_i, V_i \subseteq B^{n+i}$ *that*:

$$X(A_i, V_i) = 1; r(A_i) = r.$$

Corollary 2. *If* $X(A,V)=1; A,V \subseteq B^n$ *there exist such* A_i, V_i *satisfying the condition* $X(A_i, B_i)=1$, *for which*:

$$\frac{\log|V_i|}{\log|B^{n+i}|} \underset{i\to\infty}{\to} 1.$$

In other words the communication speed for the pair A_i, V_i tends to the unit.

Corollary 3. *For any integers,* s, r, n, *satisfying the condition* $s \leq r \leq \min(n, 2^s - 1)$, *there exists such an additive channel* $A_i \subseteq B^{n+i}$, that $|A_i| = 2^s; r(A_i) = r$, *for which* $V(A_i)$ *is the perfect code.*

Proof. To prove this statement it is sufficient to apply **Theorem 3** to the pair $A = B^s \times 0^{n-s}$, $V = \{0^s \times B^{n-s}\}$. Then we obtain:

$$A_i = \left(B^s \times 0^{n-s} \setminus \bigcup_{j=1}^{i} y_{r(A)+j} \right) \times 0^i \cup \left(\bigcup_{j=1}^{i} e_{r(A)+j} \right),$$

$$V_i = 0^s \times B^{n-s} \times B^i = 0^s \times B^{n-s+i}.$$

It follows from these that $|A_i| = 2^s$ and *i* can be chosen in such a way that $r(A_i) = r$, as well as: $|V_i| = \frac{2^{n+i}}{|A_i|}$.

Q.E.D.

Example 2. Let us consider the additive channel $A^3(y_0) \subseteq B^n$; $A^3(y_0)$ (is a 3-order neighborhood), where $A = \{y_0 = \overline{y}_0 \times 0^{n-23}, y_1 = \overline{y}_1 \times 0^{n-23}, \cdots, y_{23} = \overline{y}_{23} \times 0^{n-23}\}$ and $\{\overline{y}_1, \overline{y}_2, \cdots, \overline{y}_{23}\} \subseteq B^{23}$ is a basis for B^{23}.

It follows from Lemma 1 and Theorem 2 that the code $V = (G \times H_A) \times 0^{n-23}$ (where *G* is the binary perfect code of Golay [10] and H_A is the matrix having the rows which are the vectors of the basis $\{\overline{y}_1, \overline{y}_2, \cdots, \overline{y}_{23}\}$) and it is the perfect code correcting the errors of the additive channel $A^3(y_0)$ in the MLM metric.

Applying the above-described method (**Theorem 3**), we get the channel:

$$A_i = \left(\left(A \setminus \left(\bigcup_{j=1}^{i} y_{23+j} \right) \right) \times 0^i \cup \left(\bigcup_{j=1}^{i} e_{23+j} \right) \right),$$

And the code

$$V_i = \bigcup_{z=(z_1 z_2 \cdots z_i) \in B^i} \left((V \times 0^i) \oplus x(z) \right),$$

where

$$x(z) = \sum_{j=1}^{i} z_j (y_{23+j} \oplus e_{23+j}).$$

The following holds true for the constructed pair:

$$X(A_i, V_i) = 1,$$

It follows from here and **Theorem 1** that the constructed code $V_i \subseteq B^n$ is perfect and it corrects the errors of

the additive channel A_i.

Let us consider the partitioning of the set $W_s = \{A, |A| = 2^s, s \le n\}$ into the classes $W_{s+i} = \{A \subseteq W, r(A) = s+i\}$.

It follows from the preceding theorem that for arbitrary s, i, satisfying the condition $0 \le i \le \min(n-s, 2^s - s - 1)$, there exists a channel $A_i \in W_{s+i}$ for which $V(A_i)$ is the perfect code. Theorem 4 makes possible to construct these channels and the perfect codes correcting the errors of these channels.

Example 3.

$$A_i = \left(\left(\left(B^s \times 0^{n-s}\right) \setminus \bigcup_{j=1}^{i} y_{s+j}\right) \times 0^i \cup \left(\bigcup_{j=1}^{i} e_{s+j}\right)\right)$$

$$V_i = V(A_i) = \bigcup_{z=(z_1 z_2 \cdots z_i) \in B^i} \left(\left(0^s \times B^{n-s} \times 0^i\right) \oplus x(z)\right)$$

$$i = \overline{1, \min(n-s, 2^s - s - 1)}.$$

Let us again come back to the definition of the perfect code. The standard definition of the perfect code means that it is a set correcting the errors of an additive channel in the MLM metric in which the upper limit of the cardinality of the code is reached. Such a definition provides fixation of the code cardinality, leaving wide room only for maneuvering for its geometrical form. But the definition of the perfect code correcting the errors of the *t*-order neighborhood (for Hamming metric, correcting the *t*-multiple errors) means partitioning of the space B^n into non-intersecting *t*-order neighborhoods (a sphere of a *t*-radius) for the given metric.

It is obvious that there is a "geometrical sense" in the second definition, which is strictly definite, stating the *t*-order neighborhood (that is, the multiplicity *t* of an error for Hamming metric). The parameter *t* defines the neighborhood uniquely (a sphere of the radius *t*) and, consequently, the cardinality of the neighborhood as well, which equals A^t (that is, the cardinality of the sphere, $\sum_{i=0}^{t} C_n^i$).

Taking these considerations into account, one can conclude that these two notions do not always coincide. To demonstrate this fact, let us discuss the following example.

Example 4. A perfect code in the 'geometrical sense' does not exist for $n = 90$, $t = 2$. (See [10] or **Theorem 2** for the MLM metric case). In this case, the channel is a 2-order neighborhood: $A^2(y), y \in B^{23}$. A perfect code correcting the errors of the additive channel $\overline{A}$ in the space B^{90} with rank 90 does exist, which follows from the preceding example.

Consequently,

$$V_{78} = \bigcup_{z=(z_1 z_2 \cdots z_{78}) \in B^{78}} x(z),$$

where $x(z)$ is defined as in (3), is perfect in B^{90}, for the following channel:

$$A_{78} = \left(\left(\left(B^{12} \setminus \bigcup_{j=1}^{78} y_{12+j}\right) \times 0^{78}\right) \cup \left(\bigcup_{j=1}^{78} e_{12+j}\right)\right).$$

It is clear that the channel $\overline{A} = A_{78}$ differs from the channel $A^2(y)$ for any $y \in B^{90}$.

References

[1] Deza, M.E. (1965) Comparison of Arbitrary Additive Noises with Respect to Efficiency of Their Detection and Correction. *Problemi Peredachi Informacii*, **1**, 29-39. (in Russian)

[2] Leontiev, V.K. and Movsisyan, G.L. (2004) On Additive Communication Channels. *Dokladi AN of Armenia*, **104**, 23-27. (in Russian)

[3] Leontiev, V.K., Movsisyan, G.L. and Margaryan, J.G. (2006) Perfect Codes in Additive Channels. *Dokladi RAN*, **411**, 306-309. (in Russian)

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

[5] Leontiev, V.K., Movsisyan, G.L. and Margaryan, J.G. (2010) Codes in Additive Channels. *Dokladi of AN of Armenia*, **110**, 334-339. (in Russian)

[6] Leontiev, V.K., Movsisyan, G.L. and Margaryan, J.G. (2011) Correction of Errors in an Additive Channel. Russian-Slavyanski University, *Vestnik Fiziko-Matematicheskikh Nauk, Yerevan*, **2**. (in Russian)

[7] Movsisyan, G.L. (2013) Partition and Perfect Codes in Additive Channels. *Open Journal of Discrete Mathematics*, **3**, 112-122.

[8] Movsisyan, G.L. (2013) Dirichlet Regions and Perfect Codes in Additive Channels. *Open Journal of Discrete Mathematics*, **3**, 137-142.

[9] Leontiev, V.K., Movsisyan, G.L. and Margaryan, J.G. (2011) Limits of a Code Volume in an Additive Channel. Report at the Conference in the Russian-Slavyanski University, Yerevan. (in Russian)

[10] MacWilliams, F.J. and Sloane, N.J.A. (1979) The Theory of Error-Correcting Codes. Moscow "Svyaz". (in Russian)

[11] Leontiev, V.K., Movsisyan, G.L. and Margaryan, J.G. (2012) Geometry of the Additive Channel. *Reports at NAS, Armenia*, **112**. (in Russian)