Mathematical Problems of Computer Science 32, 14–22, 2009.

One Error and in the Given Interval Two Error Correcting Code for the Additive Communication Channel

Artur Kh. Ghandilyan[1] and Zhirayr G. Margaryan[2]
[1]Russian-Armenian (Slavonic) State University
[2]Yerevan State University
artur.ghandilyan@gmail.com

Abstract

In this paper error correcting codes in the additive noisy communication channel are discussed. The system of boolean equalities are examined based on the Hamming parity check matrix. The metrical properties of the solutions of that system of equalities are examined based on Hamming distance. It is constructed a code based on the set of the solutions of above mentioned system of boolean equalities and it is proved that the constructed code is correcting any single error and any two errors which occur in the given interval.

1. Introduction

Error correcting code theory was established in the 1940s by well known works of Shannon [1] and Hamming [2]. Error-correcting codes (or just codes) are clever ways of representing data so that one can recover the original information even if parts of it are corrupted. The basic idea is to judiciously introduce redundancy so that the original information can be recovered even when parts of the (redundant) data have been corrupted. Perhaps the most natural and common application of error correcting codes is for communication. For example, when packets are transmitted over the Internet, some of the packets get corrupted or dropped. To deal with this, multiple layers of the TCP/IP stack use a form of error correction called CRC Checksum [3]. Codes are used when transmitting data over the telephone line or via cell phones. They are also used in deep space communication and in satellite broadcast (for example, TV signals transmitted via satellite). Codes also have applications in areas not directly related to communication. For example, codes are used heavily in data storage. CDs and DVDs work fine even in presence of scratches precisely because they use codes. Codes are used in Redundant Array of Inexpensive Disks (RAID) [4] and error correcting memory [5]. Codes are also deployed in other applications such as paper bar codes, for example, the bar code used by UPS called MaxiCode [6].

2. System of the boolean equalities based on Hamming's parity check matrix

Let's discuss the following system of equalities based on Hamming's parity check H_k [2] matrix.

$$H_k * X^T = A \qquad (1)$$

where $X = \{(x_1, x_2, ..., x_n) / \forall x_i \in \{0,1\}, \quad n = 2^k - 1\}$, and $A = \begin{pmatrix} a_1 \\ a_2 \\ ... \\ a_k \end{pmatrix}$, $a_i \in Z$.

From system of equalities (1) it is obvious that when $a_i > 2^{k-1}$ then the system of equalities will not have a solution. And from the H_k it is obvious that if $\exists i, j (i \neq j)$ such that $|a_i - a_j| > 2^{k-2}$ then again the system of equalities will not have a solution.
Therefore we will discuss the cases when $0 \le a_i \le 2^{k-1}$.
Now let's investigate the set of the solutions of system of equalities (1).

Let $M(a_1, a_2, ..., a_k)$ be the set of solutions for the system of equalities (1).
From system (1) it is obvious that $M(0,0,...,0) = \{(0,0,...,0)\}$ and $M(2^{k-1}, 2^{k-1}, ..., 2^{k-1}) = \{(1,1,...,1)\}$.

Definition 1: Let the negation of the collection $A = \begin{pmatrix} a_1 \\ a_2 \\ ... \\ a_k \end{pmatrix}$, $0 \le a_i \le 2^{k-1}$ be the following collection $\overline{A} = \begin{pmatrix} \overline{a_1} \\ \overline{a_2} \\ ... \\ \overline{a_k} \end{pmatrix}$, where $\overline{a_i} = 2^{k-1} - a_i$, $i = \overline{1,k}$. It is obvious that $\overline{\overline{A}} = A$.

Definition 2: We will say that $K \subseteq B^n$ non empty set is a code and the $x = (x_1, x_2, ..., x_n)$ elements of it are code words if the $H_k * x^T = 0$ system of equalities takes place.

Statement 1: $|M(a_1, a_2, ..., a_k)| = |M(\overline{a_1}, \overline{a_2}, ..., \overline{a_k})|$, in other words there is a one-to-one correspondence between $M(a_1, a_2, ..., a_k)$ and $M(\overline{a_1}, \overline{a_2}, ..., \overline{a_k})$ sets.

Proof: First let's prove that for $\forall x \in M(a_1, a_2, ..., a_k)$ the following is true $\overline{x} \in M(\overline{a_1}, \overline{a_2}, ..., \overline{a_k})$. By definition the negation of the $x = (x_1, x_2, ..., x_n)$ vector will be $\overline{x} = (1 - x_1, 1 - x_2, ..., 1 - x_n)$. As long as $x \in M(a_1, a_2, ..., a_k)$ then $H_k * x^T = A$. Now let's prove that $H_k * \overline{x}^T = \overline{A}$, so $\overline{x} \in M(\overline{a_1}, \overline{a_2}, ..., \overline{a_k})$. Let's multiply both sides of $H_k * x^T = A$ system of equalities by -1 and add 2^{k-1} to the both sides of the system of equalities. As long as in each row of H_k matrix [2] there are 2^{k-1} ones, then after above mentioned transformation we will get the following $H_k * \overline{x}^T = \overline{A}$, which means that $\overline{x} \in M(\overline{a_1}, \overline{a_2}, ..., \overline{a_k})$. From here we can say that $|M(a_1, a_2, ..., a_k)| \le |M(\overline{a_1}, \overline{a_2}, ..., \overline{a_k})|$. With similar logic we can prove that for any $x \in M(\overline{a_1}, \overline{a_2}, ..., \overline{a_k})$ the negation of it will belong to $M(a_1, a_2, ..., a_k)$, therefore

$|M(a_1,a_2,...,a_k)| \geq |M(\bar{a}_1,\bar{a}_2,...,\bar{a}_k)|$. From here we can say that $|M(a_1,a_2,...,a_k)| = |M(\bar{a}_1,\bar{a}_2,...,\bar{a}_k)|$ and the function of the correspondence is the negation. ┘

Statement 2: In order $x \in M(a_1,a_2,...,a_k)$ and $x \in M(\bar{a}_1,\bar{a}_2,...,\bar{a}_k)$ to be true it is necessary and sufficient that $a_i = 2^{k-2}$, $i = 1,2,...,k$.

Proof: $\Rightarrow$ First let's prove the necessity part. We have $x \in M(a_1,a_2,...,a_k)$ and $x \in M(\bar{a}_1,\bar{a}_2,...,\bar{a}_k)$, from here we can say that the following systems of equalities take place $H_k * x^T = A$ and $H_k * x^T = \bar{A}$. The left parts of these systems of equalities are the same, so the right sides should be the same as well, $A = \bar{A}$, where $A = \begin{pmatrix} a_1 \\ a_2 \\ ... \\ a_k \end{pmatrix}$, $0 \leq a_i \leq 2^{k-1}$, $\bar{A} = \begin{pmatrix} \bar{a}_1 \\ \bar{a}_2 \\ ... \\ \bar{a}_k \end{pmatrix}$,

$\bar{a}_i = 2^{k-1} - a_i$, $i = \overline{1,k}$ from here $a_i = 2^{k-1} - a_i \Rightarrow a_i = 2^{k-2}$. Necessity part is proven.

$\Leftarrow$ Now let's prove the sufficiency part. We have $a_i = 2^{k-2}$, $i = \overline{1,k}$, it is easy to see that $\bar{a}_i = 2^{k-1} - a_i = 2^{k-2}$. Therefore $A = \bar{A} \Rightarrow M(a_1,a_2,...,a_k) = M(\bar{a}_1,\bar{a}_2,...,\bar{a}_k)$ $\Rightarrow x \in M(\bar{a}_1,\bar{a}_2,...,\bar{a}_k)$ and $x \in M(a_1,a_2,...,a_k)$.

Corollary 1: $M(a_1,a_2,...,a_k) = M(\bar{a}_1,\bar{a}_2,...,\bar{a}_k)$ the equality takes place when $A = \bar{A}$, which means that $a_i = 2^{k-2}$, $i = \overline{1,k}$.

Statement 3: For any $(a_{i_1}, a_{i_2}, ..., a_{i_k})$ permutation of $(a_1,a_2,...,a_k)$ vector the following holds true $|M(a_1,a_2,...,a_k)| = |M(a_{i_1}, a_{i_2}, ..., a_{i_k})|$.

Proof: Let's take $\forall x \in M(a_1,a_2,...,a_k)$. From equation (1) we can say that $H_k * x^T = A$. Let's construct the (k,k) dimensional B matrix of transformation. In the j-th row of matrix B we assign the value one to i_j-th element, and for the other elements we assign zero value, where $j = \overline{1,k}$. Now let's multiply the both parts of the equation with B matrix, then we will get $B * H_k * x^T = B * A$. It is obvious that $B * A = \begin{pmatrix} a_{i_1} \\ a_{i_2} \\ ... \\ a_{i_k} \end{pmatrix}$. In the mentioned equation we can make the following transformation $B * H_k = H_k * T$, where T is $(2^k - 1, 2^k - 1)$ dimensional transformation matrix. Therefore we will get $H_k * T * x^T = B * A$, so $T * x^T \in M(a_{i_1}, a_{i_2}, ..., a_{i_k})$. So for $\forall x \in M(a_1,a_2,...,a_k)$ solution we can get $y \in M(a_{i_1}, a_{i_2}, ..., a_{i_k})$ solution with the transformation matrix. With the similar logic we can prove the other part of the statement, i.e. $\forall y \in M(a_{i_1}, a_{i_2}, ..., a_{i_k})$, we can get $x \in M(a_1,a_2,...,a_k)$ ┘.

Below is the example of how we can get the solution based on the transformation matrix.

$$k=3,\ H_3=\begin{pmatrix}0&0&0&1&1&1&1\\0&1&1&0&0&1&1\\1&0&1&0&1&0&1\end{pmatrix}.$$

Say $A=\begin{pmatrix}1\\2\\3\end{pmatrix}$, for which one of the solutions will be $x=\begin{pmatrix}1&0&1&0&0&0&1\end{pmatrix}$. For A let's take the following permutation: $A_T=\begin{pmatrix}3\\1\\2\end{pmatrix}$. The transformation B matrix will be: $B=\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}$, it is obvious that $B*A=A_T$. Now let's construct the T matrix: $B*H_k=H_k*T$, first let's calculate the left side of the equation.

$$B*H_3=\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}\begin{pmatrix}0&0&0&1&1&1&1\\0&1&1&0&0&1&1\\1&0&1&0&1&0&1\end{pmatrix}=\begin{pmatrix}1&0&1&0&1&0&1\\0&0&0&1&1&1&1\\0&1&1&0&0&1&1\end{pmatrix}$$

First let's fix the transformation of columns of the newly constructed matrix from H_3: $1\to2$, $2\to4$, $3\to6$, $4\to1$, $5\to3$, $6\to5, 7\to7$. And the T matrix will be constructed based on above transformations, therefore the T matrix will be the following

$$T=\begin{pmatrix}0&1&0&0&0&0&0\\0&0&0&1&0&0&0\\0&0&0&0&0&1&0\\1&0&0&0&0&0&0\\0&0&1&0&0&0&0\\0&0&0&0&1&0&0\\0&0&0&0&0&0&1\end{pmatrix}$$

Now let's multiply the T matrix with x^T and we will get the solution

$$Tx^T=\begin{pmatrix}0&1&0&0&0&0&0\\0&0&0&1&0&0&0\\0&0&0&0&0&1&0\\1&0&0&0&0&0&0\\0&0&1&0&0&0&0\\0&0&0&0&1&0&0\\0&0&0&0&0&0&1\end{pmatrix}\begin{pmatrix}1\\0\\1\\0\\0\\0\\1\end{pmatrix}=\begin{pmatrix}0\\0\\0\\1\\1\\0\\1\end{pmatrix}$$

So we got that $y=\begin{pmatrix}0&0&0&1&1&0&1\end{pmatrix}$.

3. Metrical properties of the solutions of the system of equalities

Now let's examine the metrical properties of the solutions based on Hamming distance [7]. First let's remember the definition of the Hamming distance: the distance of $x=(x_1,x_2,...,x_n)$ and $y=(y_1,y_2,...,y_n)$ vectors is the following $d(x,y)=\sum_{i=1}^{n}(x_i \oplus y_i)$.

Let $M(1)$ be the union of such $M(a_1,a_2,...,a_k)$-s, for which $\forall a_i \bmod 2=1$, $i=\overline{1,k}$
$M(1)=\bigcup_{(a_1,a_2,...,a_k),a_i \bmod 2=1, i=\overline{1,k}} M(a_1,a_2,...,a_k)$.

Let $M(2)$ be the union of such $M(a_1,a_2,...,a_k)$-s, for which $\forall a_i \bmod 2=0$, $i=\overline{1,k}$
$M(2)=\bigcup_{(a_1,a_2,...,a_k),a_i \bmod 2=0, i=\overline{1,k}} M(a_1,a_2,...,a_k)$.

Statement 4: $\forall x,y \in M(2)$ solutions $d(x,y)\geq 3$.
Proof: Let's take $\forall x,y \in M(2)$, from here we can say that $H_k * x^T = A$ and $H_k * y^T = B$ such that any element of A and B are even numbers. If we consider the above mentioned equation based on binary sum (by modulo two) then we will get the Hamming equation: $H_k * x^T = 0$, $H_k * y^T = 0$ and based on [2] we can say that $d(x,y)\geq 3$.┘

Corollary 2: $M(2)$ is a single error correction code, so it is error correcting code for the following error code vectors

$$E=\begin{Bmatrix} e_1=\{0,0,0...,0\} \\ e_2=\{1,0,0...,0\} \\ e_3=\{0,1,0,...,0\} \\ ... \\ e_{n+1}=\{0,0,...,0,1\} \end{Bmatrix}$$

Statement 5: For $\forall x=(x_1,x_2,...,x_n)\in M(2)$ and $x\neq 0$ solution $\sum_{i=1}^{n} x_i \geq 3$.

Proof: Let's take $\forall x \in M(2)$, therefore $H_k * x^T = A$ such that any element of A is an even number. If we consider the above mentioned solution based on binary sum (by modulo two) then we will get the Hamming equation $H_k * x^T = 0$. It is obvious that $y=(0,0,...,0)\in M(2)$. Therefore from Statement 4 $d(x,y)\geq 3$. But as long as $y=(0,0,...,0) \Rightarrow d(x,y)=\sum_{i=1}^{n} x_i$. From here we can say that $\sum_{i=1}^{n} x_i \geq 3$.

Statement 6: For any $\forall x,y \in M(1)$ solutions $d(x,y)\geq 3$.
Proof: Let's take $\forall x,y \in M(1)$, therefore $H_k * x^T = A$ and $H_k * y^T = B$ such that any element of A and B are odd numbers. Here the sum is by modulo two as well. So we get the following

$H_k * x^T = \begin{pmatrix} 1 \\ \dots \\ 1 \end{pmatrix}$, $H_k * y^T = \begin{pmatrix} 1 \\ \dots \\ 1 \end{pmatrix}$. After summing the two equations to each other we will get $H_k * (x^T \oplus y^T) = \begin{pmatrix} 0 \\ \dots \\ 0 \end{pmatrix}$. Based on Statement 5 we can say that the number of ones of $(x^T \oplus y^T)$ vector is not less than 3, which in turn means that $d(x,y) \geq 3$.

4. Non linear code for noisy additive symmetrical communication channel

Let's do some transformation in the columns of the Hamming parity check H_k matrix in the following way. in first k columns let's write the columns (in binary representation in acceding order), which contain one zero, then other columns in acceding order.

Let's consider the following system of equalities

$$H'_k * x^T = A \tag{2}$$

Let C be the set of solutions of (2) with the condition on A that each element of it can be divided by 4.

$$C = \bigcup_{a_i \bmod 4 = 0, i=\overline{1,k}} M(a_1, a_2, \dots, a_k)$$

Let's consider the following error vectors:

$$E = \begin{Bmatrix} e_1 = \{0,0,0\dots,0\} \\ e_2 = \{1,0,0\dots,0\} \\ e_3 = \{0,1,0,\dots,0\} \\ \dots \\ e_{n+1} = \{0,0,\dots,0,1\} \\ e_{n+2} = \{\overbrace{1,1,0\dots,0}^{k},0\dots0\} \\ \dots\dots \\ e_{n+1+C_k^2} = \{\overbrace{0,0,\dots1,1}^{k},0\dots0\} \end{Bmatrix} \tag{3}$$

Theorem 1: The C code is detecting any single error and any single error which occur in the first k places. In other words C code is correcting the E (3) set of error vectors.

Proof: We have the following system of equalities $H'_k * x^T = A$, where

$A = \begin{pmatrix} a_1 \\ a_2 \\ \dots \\ a_k \end{pmatrix}$, $0 \leq a_i \leq 2^{k-1}$, $i = \overline{1,k}$, $a_i (\text{mod}) 4 = 0$, and $H'_k * y^T = B$, where $B = \begin{pmatrix} b_1 \\ b_2 \\ \dots \\ b_k \end{pmatrix}$, $0 \leq b_i \leq 2^{k-1}$,

$b_i(\text{mod})4=0$, $i=\overline{1,k}$. In order to prove the theorem it is enough to prove that for $\forall x,y\in C$ the following is true $x\oplus e_i \neq y\oplus e_j$, where $i\neq j$, $1\le i,j\le n+1+C_k^2$.

For proving the theorem lets use the rejection method; i.e. let's assume that $\exists x,y\in C$ $\exists e_i,e_j\in E, i\neq j$, such as $x\oplus e_i = y\oplus e_j$.

From equation $x\oplus e_i = y\oplus e_j$ we can say that $x\oplus y = e_i\oplus e_j \Rightarrow x = e_i\oplus e_j\oplus y$.

Now let's number the possible variants from $e_i\oplus e_j$ expression.

1. One 1 in any place
2. Two 1-s in any place
3. Two 1-s in first k places, and one 1 in the remaining $n-k$ places
4. Three 1-s in the first k places
5. Four 1-s in the first k places

It is obvious that in this case $k\ge 4$.

Let's examine 1) and 2) cases:

It is obvious that these cases are for one error correction codes. As long as $x,y\in C \Rightarrow$ $H_k'*x^T=A$ and $H_k'*y^T=B$ and from the fact that $a_i(\text{mod})4=0$ and $b_i(\text{mod})4=0$, therefore they are even numbers, so based on Statement 4 we can say that $d(x,y)\ge 3$. So, based on Hamming theorem [2], we can say that it is detecting and correcting any single error, hence the cases 1. and 2. are covered.

Now let's examine the case 3).

Suppose that ones are in the q,r,t places, where $1\le q,r\le k$ and $(k<t\le n)$. Based on $x=e_i\oplus e_j\oplus y$ assumption we can say that we can express the components of $x=(x_1,x_2,\dots,x_n)$ vector by the components of y vector's components in the following way $x_q = y_q\oplus 1$, $x_r=y_r\oplus 1$, $x_t = y_t\oplus 1$ and $x_l=y_l$ where $l\neq q,r,t$.

We have $x,y\in C \Rightarrow H_k'*x^T=A$ (4) and $H_k'*y^T=B$ (5).

Let's write the system of equalities (4) in the collapsed way

$$\begin{cases} \alpha_{11}x_1+\alpha_{12}x_2+\dots+\alpha_{1q}x_q+\dots+\alpha_{1r}x_r+\dots+\alpha_{1t}x_t+\dots+\alpha_{1n}x_n=a_1 \\ \alpha_{21}x_1+\alpha_{22}x_2+\dots+\alpha_{2q}x_q+\dots+\alpha_{2r}x_r+\dots+\alpha_{2t}x_t+\dots+\alpha_{2n}x_n=a_2 \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ \alpha_{k1}x_1+\alpha_{k2}x_2+\dots+\alpha_{kq}x_q+\dots+\alpha_{kr}x_r+\dots+\alpha_{kt}x_t+\dots+\alpha_{kn}x_n=a_k \end{cases} \qquad (6)$$

Where H_k' is the matrix constructed from the coefficients of the system of equalities

$$H_k'=\begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \dots & & & \\ \alpha_{k1} & \alpha_{k2} & \dots & \alpha_{kn} \end{pmatrix}$$

As long as we can express the x vector by y vector, then we can do the replacement of the variables in the system of equalities (6), and we will get the following

$$\begin{cases}\alpha_{11}y_1+\alpha_{12}y_2+...+\alpha_{1q}(y_q\oplus 1)+...+\alpha_{1r}(y_r\oplus 1)+...+\alpha_{1t}(y_t\oplus 1)+...+\alpha_{1n}y_n=a_1\\ \alpha_{21}y_1+\alpha_{22}y_2+...+\alpha_{2q}(y_q\oplus 1)+...+\alpha_{2r}(y_r\oplus 1)+...+\alpha_{2t}(y_t\oplus 1)+...+\alpha_{2n}y_n=a_2\\ \cdots\cdots\cdots\cdots\cdots\cdots\\ \alpha_{k1}y_1+\alpha_{k2}y_2+...+\alpha_{kq}(y_q\oplus 1)+...+\alpha_{kr}(y_r\oplus 1)+...+\alpha_{kt}(y_t\oplus 1)+...+\alpha_{kn}y_n=a_k\end{cases} \quad (7)$$

It is obvious that the system (7) takes place. From the construction of H'_k matrix and from the fact that $1\le q,r\le k$ and $(k<t\le n)$ we can say that in the matrix there is a row which satisfies to one of the following conditions $\left[\begin{array}{l}\alpha_{pq}\neq\alpha_{pr},\alpha_{pt}=0\\ \alpha_{pq}=\alpha_{pr}=\alpha_{pt}=1\end{array}\right.$ (8)

where p is the number of that line.

Let's write the system (5) in the collapsed way.

$$\begin{cases}\alpha_{11}y_1+\alpha_{12}y_2+...+\alpha_{1q}y_q+...+\alpha_{1r}y_r+...+\alpha_{1t}y_t+...+\alpha_{1n}y_n=b_1\\ \alpha_{21}y_1+\alpha_{22}y_2+...+\alpha_{2q}y_q+...+\alpha_{2r}y_r+...+\alpha_{2t}y_t+...+\alpha_{2n}y_n=b_2\\ \cdots\cdots\cdots\cdots\cdots\cdots\\ \alpha_{k1}y_1+\alpha_{k2}y_2+...+\alpha_{kq}y_q+...+\alpha_{kr}y_r+...+\alpha_{kt}y_t+...+\alpha_{kn}y_n=b_k\end{cases} \quad (9)$$

As long as system (9) is satisfied and we have condition (8) we can say that the value of the left part of the p-th equation of (9) system is different from the same equation of the (7) system by 1, 2 or 3, therefore the value of left side of the p-th equation of (7) system can not be divided to 4, so we came to contradiction in this case.

Now let's examine the case 4)

Let's assume that ones are located in the q,r,t-th places, where $1\le q,r,t\le k$, $k\ge 4$. From the assumption $x=e_i\oplus e_j\oplus y$ we can say that the components of $x=(x_1,x_2,...,x_n)$ vector can be expressed by the components of the y vector this way, $x_q=y_q\oplus 1$, $x_r=y_r\oplus 1$, $x_t=y_t\oplus 1$ and $x_l=y_l$ when $l\neq q,r,t$.

From the construction of H'_k matrix and from the fact that $1\le q,r,t\le k$ and $k\ge 4$ we can say that there is a row in it which satisfies to one of the following conditions: $\alpha_{pq}\neq\alpha_{pr}$ and $\alpha_{pt}=0$ (10) where p is the number of that line.

As long as the (9) system is satisfied and taking into account the (10) fact we can say that the value of the left side of the p-th equation of (9) system will differ from the value of the left part of p-th equation of (7) system by 1 therefore that value can not be divided to 4. Again we came to the contradiction.

Let's examine case 5).

Suppose that the ones are located in the q,r,t,h-th places, where $1\le q,r,t,h\le k$. From $x=e_i\oplus e_j\oplus y$ fact we can say that the components of $x=(x_1,x_2,...,x_n)$ vector can be expressed by the components of y vector in the following way: $x_q=y_q\oplus 1$, $x_r=y_r\oplus 1$ and $x_t=y_t\oplus 1$, $x_h=y_h\oplus 1$ and $x_l=y_l$ when $l\neq q,r,t,h$.

Based on the construction of H'_k matrix and from the fact $1\le q,r,t,h\le k$ and $k\ge 4$ we can say that there is a line in the matrix which satisfies to the following condition $\alpha_{pq}=\alpha_{pr}=\alpha_{pt}=1$ and $a_{ph}=0$ (11) where p is the number of that line.

As long as the (9) system is satisfied and from the fact (11) we can say that the value of the left side of the p-th equation of (9) system will different from the value of the left side of the

p-th equation of (7) system by 1 or 3. Therefore the p-th equation of (7) system can not be satisfied. Again we came to the contradiction.

So for all 5 cases we came to the contradiction. Therefore our assumption that $\exists x, y \in C$ $\exists e_i, e_j \in E$, $i \neq j$, and $x \oplus e_i = y \oplus e_j$ is not true. So the code C is correcting any single error and any two errors which occur in the first C places.
Theorem is proved.

References

[1] C. E. Shannon, "A mathematical theory of communication", *Bell System Technical Journal*, 27(2). pp. 379-423 and 623-656, 1948.
[2] R. W. Hamming, "Error Detecting and Error Correcting Codes", *Bell System Technical Journal*, 29(2). pp. 147-160, 1950.
[3] L. L. Peterson and B. S. Davis, *Computer Networks: A Systems Approach*. Morgan Kaufmann Publishers, San Francisco, 1996.
[4] P. M. Chen, E. K. Lee, G. A. Gibson, R. H. Katz, and D. A. Patterson, "RAID: High-performance, reliable secondary storage", *ACM Computing Surveys*, 26(2). pp. 145-185, 1994.
[5] C. L. Chen and M. Y. Hsiao, "Error-correcting codes for semiconductor memory applications: A state-of-the-art review", *IBM Journal of Research and Development*, 28(2). pp. 124-134, 1984.
[6] D. G. Chandler, E. P. Batterman, and G. Shah, "Hexagonal, information encoding article, process and system", US Patent Number 4, pp. 874-936, 1989.
[7] Ф. Дж. Мак-Вильямс, *Теория кодов, исправляющих ошибки*, 1979.

Մեկ սխալի և որոշակի ինտերվալում երկու սխալ ուղղող կոդեր ադդիտիվ սիմետրիկ կապի գծերի համար

Ա. Ղանդիլյան և Ժ. Մարգարյան

Ամփոփում

Աշխատանքում դիտարկված են հայտնաբերող և ուղղող կոդեր սիմետրիկ ադդիտիվ կապի գծերում: Հետազոտված է հավասարումների համակարգը, որը կառուցված է Հեմմինգի ստուգող մատրիցի հիման վրա: Հետազոտված են այդ հավասարումների համակարգերի բուլյան լուծումների բազմությունը և նրանց մետրիկական հատկությունները: Կառուցված է ոչ գծային կոդ այդ հավասարումների համակարգի բուլյան լուծումների հիման վրա և ապացուցված է, որ այն ուղղում է կամայական մեկ սխալ ինչպես նաև կամայական երկու սխալ որոշակի ինտերվալում: