Mathematical Problems of Computer Science 21, 2000, 101–103.

A construction of a class of codes correcting probable errors

Sosina S. Martirosyan

Institute for Informatics and Automation Problems of NAS RA and YSU

Abstract

In this article a new class of error correcting codes are considered.A construction method for a parameter class for QAM is obtained,which gives codes with the cardinality bigger then the known codes for other modulations.

Let $X \in \{0,1,\ldots,q-1\}^n$.

As a result of an error in a communication channel vector X may turn into vector X' $\left(X' \in \{0,1,\ldots,q-1\}^n\right)$whose at most t components differ from the corresponding components of X either by $+1$ or -1. Let we are also given the vector $T\left(X'\right)\left(T\left(X'\right) \in \{0,1,-1\}^n\right)$ together with the vector X'. Besides we also know that the residue of the ith components of X' and X is equal to the ith component of $T\left(X'\right)$ or 0 $\left(i=\overline{1,n}\right)$.

Here the signs $\oplus$ and $\ominus$ denote the following operations:

$i \ominus j = (i-j) \bmod q-1$ for $\forall i, j$, except the case when $i=0, \quad j=1$ and $0 \ominus 1 = 0$;

$i \otimes j = (i+j) \bmod q-1$ for $\forall i, j$ except the case when $i=q-1, \ j=1$ and $q-1 \oplus 1 = q-1$.

We'll call the vector $T\left(X'\right)$ to be the *probable error vector of the vector* X.

Definition 1. *We'll call code L of length n over the q alphabet that corrects no more than $(\pm1)\,t$ errors, when for each received vector its probable error vector is known, as the code correcting $(\pm1)\,t$ probable errors.*

We'll denote the cardinality of code L by $M(n,q,t)$.

In this paper we'll give a method to construct codes correcting $(\pm1)\,t$ most probable errors, using t error-correcting binary codes.

Let $X \in \{0,1,\ldots,q-1\}^n$.

Definition 2. *We call the vector $r(X)$ to be the vector of evenness and oddness of X, if its ith component $\left(i=\overline{1,n}\right)$ is 0 when the ith component of X is even and is 1 when it is odd.*

Let L be a code correcting $(\pm1)\,t$ probable errors.

Lemma. From the vectors $X'$and $r(X)$ $(X \in L)$ we can obtain the vector X.

Proof. It follows from the definition of the code L that the vector $T\left(X'\right)$ is also known to us.

Let l denote that vector whose ith component $\left(i=\overline{1,n}\right)$ is equal to the absolute value /modulus? of the residue of the ith components of $r\left(X'\right)$ and $r\left(X\right)$. Note that the ith component $\left(i=\overline{1,n}\right)$ of l is equal to 0 if no error has occurred and to 1 if an error has occurred in the channel.

And let m denote that vector whose ith component $\left(i=\overline{1,n}\right)$ is equal to the product of the ith components of l and $T\left(X'\right)$.

By definition of $T\left(X'\right)$ we have

$$X=X'-m.$$

Let C be a binary code of length n and minimum Hamming distance d. Let $A_2\left(n_1\, d\right)$ denote cardinality of the code.

Now we'll construct the following code (denote it by Γ).

Code construction. For any X $\left(X\in\{0,1,\ldots,q-1\}^n\right)$, $X\in\Gamma$, if $r\left(X\right)\in C$.

Note that the cardinality of the code is $A_2\left(n,\ d\right)\cdot\left(\frac{q}{2}\right)^n$ for even q.

Let's t denote $d-1$.

Theorem. *Code* Γ *is a code correcting* $(\pm1)\,t$ *probable errors.*

Proof. Suppose as a result of an error in the communication channel vector X $\left(X\in\Gamma\right)$ has turned into vector X'. Since C is a code correcting at most t errors and by the construction of Γ we have that $r\left(X\right)\in C$, then we can obtain the vector $r\left(X\right)$ from the vector $r'\left(X\right)$. Hence, using the Lemma we may obtain the vector X from the vectors X', $r\left(X\right)$ and $T\left(X'\right)$.

Codes given by this method could be represented in a systematic form. And since the general case depends on the choice of C we'll illustrate this representation method by an example. It could also be generalized to all cases.

Example. Let $n=16,\quad q=32$.

We'll take the code obtained by adding over-all parity check to Hamming code of length 15 as the binary code. Let C_0 denote this code and $A_2\left(16,\ 4\right)=2^{11}$ denote cardinality of the code. Using the method mentioned above we'll construct code Γ_0 with the cardinality

$$M\left(16,\ 32,\ 3\right)=\left(\frac{32}{2}\right)^{16}\cdot2^{11}=32^{15}.$$

It follows from the Theorem that this is a code correcting (±1) 3 probable errors.

Further we'll represent this code in a systematical form.

We'll establish a one-to-one correspondence between 32^{15} vectors of code Γ_0 and vectors of the set $\{0,1,\ldots,31\}^{15}$ of the same number.

First, we'll split the set of 2^{15} binary vectors of length $n=15$ into 16 non-intersecting /disjoint?? classes of vectors in the following form $\left(\left(N\left[0\right],N\left[1\right],\ldots N\left[15\right]\right)\right.$ denotes these classes of vectors):

Let $l=\left(l_1,l_2,\ldots,l_{15}\right)$ be an arbitrary binary vector.

$l\in N\left[0\right]$ if $l'=\left(l_1,l_2,\ldots,l_{15},\varepsilon\right)\in C_0$, $\varepsilon=0$ or 1;

$l \in N[0]$ and $l_6 \in N[i]$, $i = \overline{1,15}$, if $l' = \left(l_1, l_2, \ldots, l_{i-1}, \overline{l_i}, l_{i+1}, \ldots, l_{15}, \varepsilon\right) \in C_0$, $\varepsilon = 0$ or 1.

There will be 2^{11}vectors (since there are 2^{11}vectors in C_0) in each class.

Further we'll show that these classes of vectors are non-intersecting.

Now suppose the contrary that there exists an $l^0(l_1, l_2, \ldots, l_{15})$ binary vector such that

Case1. $l^0 \in N[0]$ and $l^0 \in N[k]$ for any k, $k = \overline{1,15}$. This implies that the vectors $l'(l_1, l_2, \ldots, l_{15}, \varepsilon_1)$ and $l''\left(l_1, l_2, \ldots, \overline{l_k}, \ldots, l_{15}, \varepsilon_2\right)$ $(\varepsilon_1; \varepsilon_2 = 0$ or1) belong to code C_0, which is a contradiction, since the minimal Hamming distance of code C_0 is $4\,(d = 4)$.

Case 2. $l^0 \in N[i]$ and $l^0 \in N[j]$ for any i and j, $i \neq j$, $\left(i, j = \overline{1,15}\right)$. This implies that the vectors $l' = \left(l_1, l_2, \ldots, l_{i-1}, \overline{l_i}, l_{i+1}, \ldots, l_{15}, \varepsilon_1\right)$ and
$l'' = \left(l_1, l_2, \ldots, l_{j-1}, \overline{l_j}, l_{j+1}, \ldots, l_{15}, \varepsilon_1\right)$ $(\varepsilon_1; \varepsilon_2 = 0$ or1) belong to code C_0,which is a contradiction since the minimal Hamming distance of code C_0 is $4\,(d = 4)$.

This contradiction proves our assertion that these classes of vectors are non-intersecting.

Let X be an arbitrary vector $X \in \{0, 1, \ldots, 31\}^{15}$ $(X = (X_1, \ldots x_{15}))$.
Now we'll consider the vector $r(X)$ $(r(X) = (r_1, \ldots, r_{15}))$.

Case1. $r(X) \in N[0]$. This implies that the vector $r'(X) = (r_1, r_2, \ldots, r_{15}, \varepsilon) \in C_0$ $(\varepsilon = 0$ or1). For this case let vector

$$Y = (X_1, X_2, \ldots, X_{15}, \varepsilon)$$

correspond to vector X. Vector Y belongs to code Γ_0 by the construction of Γ_0.

Case 2. $r(x) \in N[i]$ for any i, $i = \overline{1,15}$. This implies that the vector $r'(X) = (r_1, r_2, \ldots, r_{i-1}, \overline{r_i}, r_{i+1}, \ldots r_{15}, \varepsilon) \in C_0$ $(\varepsilon = 0$ or1). For this case let vector

$$Y = (X_1, X_2, \ldots, X_{i-1}, X_i \oplus 1, X_{i+1}, \ldots X_{15}, 2i + \varepsilon)$$

correspond to vector X. Vector Y belongs to code Γ_0 by the construction of Γ_0.

Now let $Y = (Y_1, Y_2, \ldots, Y_{15}, Y_{16})$.
If $Y_{16} = 2i + \varepsilon$ $(\varepsilon = 0$ or1), then we may bring the vector
$X = (Y_1, Y_2, \ldots, Y_{i-1}, Y_i \ominus 1, Y_{i+1}, \ldots, Y_{15})$ $X \in \{0, 1, \ldots, 31\}^{15}$ in correspondence with vector Y.

Remark. Here the signs $\oplus$ and $\ominus$ denote the following operations:

$i \oplus 1 = i + 1 \qquad i = \overline{0,30}$
$31 \oplus 1 = 0$
$i \ominus 1 = i - 1 \qquad i = \overline{0,31}$.
$0 \ominus 1 = 31$