ELECTRICAL ENGINEERING

V. M. OSTIANU

1960

SovietRxiv

Abstract

Full Text

ELECTRICAL ENGINEERING

V. M. OSTIANU

CONSTRUCTION OF NONBINARY SELF-CORRECTING CODES AND AN ESTIMATE OF THE NUMBER OF SIGNALS IN THEM

(Presented by Academician V. S. Kulebakin, 9 III 1960)

In many areas of engineering, nonbinary signals have become widespread, i.e., signals consisting of elementary symbols of several types. If signals are transmitted with errors and it is desirable to correct these errors, correcting codes are used. The problem of constructing nonbinary correcting codes in its most general form was formulated in the works of M. A. Gavrilov ([1,2]).

In the present communication a linear method* is proposed for constructing nonbinary correcting codes, on the basis of which the number of signals in these codes is estimated.

The results presented here are a development of the works of R. R. Varshamov ([3,4]) for the base of the code $b > 2$.

1. The set of b^n sequences of the form $a = (a_1, \dots, a_n)$, where each symbol a_i takes a value in the residue class modulo b, forms an additive abelian group $G_{n,b}$. In $G_{n,b}$ the distance $\rho(a', a'')$ between any pair of its elements a' and a'' is defined as the number of nonmatching symbols, i.e.

$$\rho(a', a'') = \sum_{i=1}^{n} \delta_i, \qquad \text{where } \delta_i = \begin{cases} 0, & \text{if } a_i' = a_i'', \\ 1, & \text{if } a_i' \neq a_i''. \end{cases}$$

For each $a \in G_{n,b}$, the norm $\|a\| = \rho(a, 0)$ is defined as the number of symbols a_i different from zero.

It is known from the literature ([2,6]) that, for it to be possible to correct d erroneously received symbols, it is necessary and sufficient that the pairwise distances between signals in the code be not less than $D = 2d+1$. In connection with this the question arises: for what values of n, d, and N is it possible to select in $G_{n,b}$ a set of N signals with pairwise distances not less than D**.

For nonbinary signals the necessary condition ([7]) is known:

$$N \leqslant \frac{b^n}{\sum_{i=0}^{d} C_n^i (b-1)^i}. \tag{1}$$

2. For the linear coding method with a prime base of the code $b = p$, we obtained ([8]) a sufficient condition in the form

$$N \leqslant \frac{p^n}{\sum_{i=0}^{D-1} C_n^i (p-1)^i}. \tag{2}$$

* The principle of linear coding is described in work ([5]).

** Everywhere below we shall assume that D is odd, since the case of even D is easily reduced to the case of odd D.

If signals a are used to transmit messages $\alpha = (\alpha_1, \dots, \alpha_m)$ from $G_{n,p}$, then $N = p^m$. Setting $n = m + h$, one can write conditions (1) and (2) in the form

$$p^h \geq \sum_{i=0}^{d} C_n^i (p-1)^i, \tag{1'}$$

$$p^h \geq \sum_{i=0}^{D-1} C_n^i (p-1)^i. \tag{2'}$$

We shall show that the sufficient condition $(2')$ can be weakened:

$$p^h > \sum_{i=0}^{D-2} C_{n-1}^i (p-1)^i. \tag{2"}$$

In order to specify a linear coding method, it is enough to specify m linearly independent elements of the group $G_{n,p}$—a basis. Let us take as the basis the signals

$$l^i = e^i c^i = (e_1^i, e_2^i, \dots, e_m^i, c_1^i, c_2^i, \dots, c_h^i) \quad (i = 1, 2, \dots, m),$$

where $e^i = (e_1^i, e_2^i, \dots, e_m^i)$ and $e_j^i = 1$, if $i = j$; $e_j^i = 0$, if $i \neq j$, while $c^i \in G_{h,p}$. Then any signal a^t $(t = 0, 1, \dots, p^m - 1)$ of the code obtained in this way will have the form

$$a^t = \sum_{q=1}^{m} s_q l^q, \tag{3}$$

where s_q takes values in the residue class modulo p.

We impose the following conditions on the elements c^i:

$$\begin{gathered}\left\|r^1 c^{i_1}\right\| \geq D-1 \quad (i_k=1,2,\ldots,m), \quad r^k \in \{1,\ldots,p-1\}, \quad k=1; \\ \left\|r^1 c^{i_1}+r^2 c^{i_2}\right\| \geq D-2 \quad (i_k=1,2,\ldots,m), \quad r^k \in \{1,\ldots,p-1\}, \quad k=1,2; \\ \ldots \\ \left\|r^1 c^{i_1}+r^2 c^{i_2}+\cdots+r^{D-1} c^{i_{D-1}}\right\| \geq 1 \quad (i_k=1,2,\ldots,m), \quad r^k \in \{1,\ldots,p-1\}, \\ k=1,2,\ldots,D-1.\end{gathered} \tag{4}$$

It can be shown that the distance between elements of the form (3), under condition (4), will be not less than D. Indeed,

$$\rho(a^i,a^j) \geq \min_t \|a^t\| \quad (a^t \neq 0,\ t=1,\ldots,p^m-1),$$

$$\|a^t\| = \left\|\sum_{q=1}^m s_q l^q\right\| = \left\|\sum_{q=1}^m s_q e^q\right\| + \left\|\sum_{q=1}^m s_q c^q\right\|.$$

If

$$\left\|\sum_{q=1}^m s_q e^q\right\| \geq D,$$

then $\|a^t\| \geq D$.

If

$$\left\|\sum_{q=1}^m s_q e^q\right\| = v < D,$$

then

$$\left\|\sum_{q=1}^m s_q c^q\right\| \geq D-v,$$

and therefore, for any i and j,

$$\rho(a^i,a^j) \geq v+D-v = D.$$

We shall choose the elements c^i successively, one after another, taking into account conditions (4).

By counting, it is established that after $k-1$ elements c^t have been chosen, there are no more than $C_{k-1}^{D-2}(p-1)^{D-2}+Q_k^1C_{k-1}^{D-3}(p-1)^{D-3}+\cdots\cdots+Q_h^{D-3}C_{k-1}^1(p-1)+Q_h^{D-2}$ elements $c\in G_{n,p}$ which, by virtue of (4), cannot be chosen as the k-th element. Here

$$Q_w^u=\sum_{i=0}^{u}C_w^i(p-1)^i.$$

In order to be able to choose all the elements c^t up to and including the m-th, it is sufficient that, when choosing the m-th element, the number of forbidden elements be less than the total number of elements in $G_{h,p}$, i.e.

$$p^h>C_{m-1}^{D-2}(p-1)^{D-2}+Q_h^1C_{m-1}^{D-3}(p-1)^{D-3}+\ldots$$
$$\ldots+Q_h^{D-3}C_{m-1}^1(p-1)+Q_h^{D-2}=Q_{n-1}^{D-2},$$

whence condition (2″) follows.

3. With a slight modification, this construction method extends to the construction of nonbinary self-correcting codes with an arbitrary base.

In conclusion, the author considers it a pleasant duty to express gratitude to Prof. M. A. Gavrilov for his attention and to R. R. Varshamov for valuable advice.

Institute of Automation and Remote Control
Academy of Sciences of the USSR

Received
7 III 1960

REFERENCES

1. M. A. Gavrilov, *Avtomatika i telemekh.*, **17**, No. 2, 1092 (1956).

2. M. A. Gavrilov, G. A. Shastova, Collection: Session of the USSR Academy of Sciences on Scientific Problems of Automation of Production, 15-20 X 1956, Scientific Problems of Telemechanization of Production Processes, 4, Publishing House of the USSR Academy of Sciences, Moscow, 1957.

3. R. R. Varshamov, DAN, **117**, No. 5, 739 (1957).

4. R. R. Varshamov, Collection of Works of the Scientific-Technical Society of Radio Engineering and Electrical Communications named after A. S.

Popov, issue 1, 1958.

5. R. R. Varshamov, Dissertation, Moscow State University, 1959.

6. R. W. Hamming, *Bell Syst. Techn. J.*, **26**, No. 2, 147 (1950).

7. H. S. Shapiro, D. L. Slotnick, *IBM J. Res. and Development*, **3**, No. 1, 25 (1959).

8. B. M. Ostianu, Collection: Industrial Telemechanics, Publishing House of the USSR Academy of Sciences, 1960.

Note: Figure translations are in progress. See original paper for figures.