CYBERNETICS AND CONTROL THEORY

1965

SovietRxiv

Abstract

Full Text

CYBERNETICS AND CONTROL THEORY

S. I. SAMOILENKO

CONSTRUCTION OF CYCLIC ERROR-CORRECTING CODES AND ANALYSIS OF THEIR CORRECTING CAPABILITY

(Presented by Academician A. I. Berg on 2 XII 1964)

1. A number of methods are known for constructing codes of various types that correct independent or burst errors. Cyclic codes, which are convenient for implementation, are of particular importance. Methods for constructing and analyzing cyclic codes are based on the theory of ideals in the linear commutative algebra of polynomials modulo $x^n - 1$ with coefficients from Galois fields ([1]). Another approach to the construction of such codes is also possible, based on the use of the cyclic properties of square matrices. The use of cyclic properties of matrices for implementing certain correcting codes is known from the literature, for example those of Abramson, Fire, Bose–Chaudhuri ([2]).

The purpose of the present work is to use the cyclic properties of square matrices for constructing cyclic error-correcting codes and analyzing their correcting capabilities.

2. A cyclic binary error-correcting code can be described by a certain set of matrices $H_1, H_2, \dots, H_k$, one of which is a check matrix.

The matrices $H_1, H_2, \dots, H_k$ are constructed as follows:

$$\begin{aligned} H_1 &= [x_1 \quad Tx_1 \quad T^2x_1 \dots T^{n_1-1}x_1] \\ H_2 &= [x_2 \quad Tx_2 \quad T^2x_2 \dots T^{n_2-1}x_2] \\ &\dots\dots\dots\dots\dots\dots\dots \\ H_k &= [x_k \quad Tx_k \quad T^2x_k \dots T^{n_k-1}x_k], \end{aligned} \tag{1}$$

where T is some square $r \times r$ matrix; in the case of binary codes the elements of the matrix have the values 0 or 1; x_i is some r-symbol column vector not coinciding with any vector from the previously constructed matrices $H_1, H_2, \dots, H_{i-1}$. For binary codes the elements of the vectors x_i are 0 or 1; H_i are check and quasi-check matrices (the check matrix will be denoted by an asterisk: H_j^*); r is the number of redundant symbols in the code combination; n_i is some number for which $T^{n_i}x_i = x_i$.

Any of the matrices H_i can be used as the check matrix of some correcting code. In this case the code will be cyclic; that is, if the binary vector

$$B = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_{n_i} \end{bmatrix}$$

is a code word,

$$H_i^* B \equiv 0 (\mathrm{mod} 2), \tag{2}$$

then the vector

$$B' = \begin{bmatrix} b_{n_i} \\ b_1 \\ \vdots \\ b_{n_i - 1} \end{bmatrix}$$

is also a code word, and for it condition (2) is satisfied.

The proof follows from the fact that

$$\begin{aligned} TH_i^* B = T(x_i b_1 \oplus T x_i b_2 \oplus ... \oplus T^{n_i - 1} x_i b_{n_i}) = \\ = b_1 T x_i \oplus b_2 T^2 x_i \oplus ... \oplus b_{n_i} x_i = B' H_i = 0, \end{aligned} \tag{3}$$

if (2) is satisfied. (Here and below the sign $\oplus$ denotes addition modulo 2.)

From the general class of square matrices T, for constructing codes we choose a set of matrices that realize such transformations of the vectors x_i as are easily implemented by technical devices. Thus, in particular, if the encoding and decoding process is carried out using shift registers, then the matrix T takes the form

$$T = \begin{bmatrix} -a_{11} & a_{12} & ... & a_{1r} \\ 1 & a_{22} & ... & a_{2r} \\ a_{31} & 1 & ... & a_{3r} \\ \vdots & & & \\ a_{r1} & a_{r2} & ... & 1 a_{rr} \end{bmatrix}. \tag{4}$$

If, moreover, it is required that in the individual adders of the register feedback circuits there be no simultaneous summation of signals arriving from more than two register cells, then matrix (4) takes the form

$$S = \begin{bmatrix} -a_1 & a_2 & ... & a_r \\ 1 & 0 & ... & 0 \\ 0 & 1 & ... & 0 \\ \cdot & \cdot & & \\ 0 & 0 & ... & 1 \quad 0 \end{bmatrix}. \tag{5}$$

The cyclic properties of the matrix S, and consequently also the characteristics of the matrices H_i, are determined from an analysis of the characteristic polynomial (3)

$$\varphi(y) = y^r + a_1 y^{r-1} + ... + a_r. \tag{6}$$

3. The correcting capabilities of some arbitrary code can be estimated by analyzing $\varphi(y)$, and determined exactly by considering the set of matrices H_i.

It is known that, in order to detect an error e_i, it is necessary that

$$H^* e_i \neq 0, \tag{7}$$

where

$$e_i = \begin{bmatrix} e_{i1} \\ e_{i2} \\ \cdot \\ \cdot \\ e_{in} \end{bmatrix}$$

is the error vector, whose elements e_{ij} are equal to 0 if the j-th symbol of the code combination has been received correctly, or to 1 if this symbol is distorted.

In order for the code to correct some set of errors, it is necessary, in addition to (7), that

$$H^* e_i \neq H^* e_j, \quad \text{for all } i, j, \text{ if } i \neq j. \tag{8}$$

Taking into account that

$$H^* = [x, Sx, S^2 x, ..., S^{n-1} x], \tag{9}$$

from conditions (7) and (8) one can obtain that, for detection of the error e_i, it is necessary that

$$e_{i1} E \oplus e_{i2} S \oplus ... \oplus e_{in} S^{n-1} \neq 0, \tag{7a}$$

and for correction of errors e_i and e_j it is necessary that

$$(e_{i1} \oplus e_{j1})E \oplus (e_{i2} \oplus e_{j2})S \oplus ... \oplus (e_{in} \oplus e_{jn})S^{n-1} \neq 0 \tag{8a}$$

for all i, j, if $i \neq j$.

From the Hamilton-Cayley theorem it is known that any square matrix satisfies its own characteristic equation. Therefore conditions (7a), (8a) will be satisfied if the polynomials

$$e_i(y) = e_{i1} + e_{i2}y + ... + e_{in}y^{n-1}, \tag{10}$$

$$e_{i/j}(y) = (e_{i1} \oplus e_{j1}) + (e_{i2} \oplus e_{j2})y + ... + (e_{in} \oplus e_{jn})y^{n-1} \tag{11}$$

are not divisible by $\varphi(y)$.

As applied to the correction of interdependent errors, it can be shown that if the vectors e_i contain no more than Δ nonzero elements, then some e_{ij} are divisible by (6) provided that the number of nonzero elements in (6) is less than $2\Delta + 1$. Consequently, in order for the code to correct all errors of weight Δ or less, it is necessary that the number of nonzero elements in $\varphi(y)$ exceed 2Δ, i.e.

$$[\varphi_\Delta(y)] > 2\Delta, \tag{12}$$

where $[\varphi_\Delta(y)]$ is the number of nonzero elements in the characteristic equation of the matrix S.

Let us now consider the requirements on the cyclic properties of the matrix S. First of all, it should be noted that, in order to construct a code containing codewords of length n symbols, it is necessary that at least one cycle of the matrix S have length equal to or exceeding n.

It can be shown that if the sum of some columns of the matrix H_i is contained in the matrix H_j, then all sums of the cyclic shifts of these columns of H_i will also be contained in H_j. It follows from this that if, in evaluating the correcting capabilities of the code, one takes into account only those errors e_i for which $H^* e_i \neq T_i^{jH^{*e}}$ $(j = 1, 2, ..., n-1)$ (the number of such errors includes all errors of multiplicity $\Delta < n$, if n is a prime number, or all except for a small part if n has divisors), then it may be considered that, for correction of all errors of multiplicity Δ or less, it is necessary that

$$Z_n n \geq \sum_{i=1}^{\Delta} C_n^i, \tag{13}$$

where Z_n is the number of cycles of the matrix S of length n.

In the case of correcting burst errors of length d or less, an analogous consideration gives that

$$Z_n n > 2^{d-1}(n-d+2)-1. \tag{14}$$

The right-hand side of (14) is equal to the number of different burst errors of length not exceeding d, in a codeword of length n.

4. Analysis of the correcting capabilities of an arbitrary cyclic code can be carried out by considering the distribution among the H_i of the syndromes $H^* e_i$ corresponding to various e_i. Thus, for example, for a code generated by a matrix with characteristic equation $\varphi(y) = y^4 + y^3 + y^2 + y + 1$, the matrices H_i have the form:

$$H_1 = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}; \quad H_2 = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}; \quad H_3 = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \end{bmatrix},$$

and the correcting capabilities of the code when using the matrix H_1^* as the check matrix will be completely determined by the syndrome distribution table (see Table 1). (Here the error form determines the locations of the distorted symbols in the code combination. The number of errors of a given form is equal to the number of different errors that can be formed by cyclically shifting the given error.)

Table 1

Error type	Error type	Number of errors of the given form	Matrices	Matrices	Matrices	Matrices
error multiplicity	error form		0	H_1	H_2	H_3
1	(1)	5	0	5	0	0
2	(1, 2)	5	0	0	5	0
2	(1, 3)	5	0	0	0	5
3	(1, 2, 3)	5	0	0	5	0
3	(1, 2, 4)	5	0	0	0	5
4	(1, 2, 3, 4)	5	0	5	0	0
5	(1, 2, 3, 4, 5)	1	1	0	0	0

From the analysis of this table one can determine all the capabilities of the code. Thus, in particular, the code under consideration can be used for correcting all errors of multiplicity 2 or less, for correcting single errors and detecting errors of multiplicity 2 and 3, for correcting single and double adjacent errors and detecting the remaining double errors and half of the triple errors, for detecting all errors of multiplicity less than 5, or for some other sets of errors.

The construction of tables of the distribution of errors among H_i can be carried out with the aid of a computer, which makes it possible to analyze arbitrary cyclic codes constructed in accordance with the method described.

5. The method presented for constructing and analyzing cyclic correcting codes makes it possible to search for and construct codes satisfying specified requirements (length of the code combination, correctable errors, redundancy), and also to analyze the correcting capabilities of arbitrary cyclic codes described by matrices of type (5). In this case the construction and analysis of different codes are carried out by a unified method, independently of the types of errors corrected by the code, the number of redundant symbols, and the length of the code combination, which makes it possible to carry out the construction and analysis of various cyclic codes uniformly with the aid of a computer.

Scientific Council on Cybernetics
under the Presidium of the Academy of Sciences of the USSR

Received
26 XI 1964

REFERENCES

1. A. A. Kharkevich, *Combating Interference*, Moscow, 1963.

2. J. E. Meggitt, Trans. Inform. Theory, No. 4, 234 (1961); Russian transl. in the collection *Coding Theory*, ed. E. L. Blokh, Moscow, 1964, p. 225.

3. B. Elspas, *Cybernetic Collection*, ed. A. A. Lyapunov and O. B. Lupanov, No. 7, 1963, p. 90.

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