Description of Encoding and Decoding of Binary Cyclic Codes in a Class Sequential Machines

Fikrat Feyziyev[1], Lidiya Ramazanova[2], Mehrdad Arablu Babavand Aslan[3]
[1,2]Sumgait State University, Sumgait, Azerbaijan
[3]Parsabad Moghan Branch, Islamic Azad University, Parsabad Moghan, Iran
[1]*FeyziyevFG@mail.ru*, [3]*babaVand@yahoo.com*

***Abstract*— The question of description of encoding and decoding on the base Meggit's theorem of binary cyclic codes in class sequential machines is considered. Formulas for the description of the logical of detection and correction of mistakes in cyclic of superfluous codes are thus offered.**

***Keywords*— sequential machines; cyclic codes; encoding; decoding; Meggit's theorem**

I. Introduction

Let the set B is a cyclic code [1, 2] in length n over the Galois field $GF(2)$ and the code words have the form n-dimensional vectors $c=(c_0,c_1,...,c_{n-1})$.

Let $g(x)=g_{n-k}x^{n-k}+...+g_1x+g_0$ is generator polynomial of the code B. Polynomial $g(x)$ is a divisor of the polynomial x^n+1 and the code B consists of all the product of the polynomial $g(x)$ by polynomials on degree at most $k-1$ [1]. Each vector can be represented by x a polynomial in the form

$$c(x)=c_{n-1}x^{n-1}+...+c_1x+c_0\,.$$

Let's

$$B(x)=\{c(x)=c_{n-1}x^{n-1}+...+c_1x+c_0\,|(c_0,...,c_{n-1})\in B\}.$$

Set $B(x)$ have the structure of the sub ring of ring $GF(2)[x]/(x^n+1)$ [1], where are defined the operations of addition and multiplication by $\mathrm{mod}\,(x^n+1)$ follows:

$$p_1(x)\cdot p_2(x)=R_{x^n+1}[p_1(x)p_2(x)] \qquad (1)$$

This record $R_{x^n+1}[p_1(x)p_2(x)]$ is the remainder obtained by dividing the product $p_1(x)$ and $p_1(x)$ in the ring $GF(2)[x]$ by a polynomial x^n+1, i.e. product on the left side of (1) is a product by $\mathrm{mod}\,(x^n+1)$. Clearly, the cyclic shift can be written down as follows:

$$c'(x)=x\cdot c(x)=R_{x^n+1}[x\cdot c(x)]\,.$$

Let $i=(i_0,i_1,...,i_{k-1})$ is arbitrary k-dimensional vector over $GF(2)$. Then each k-dimensional information vector i can be encoded in B by the formulas

$$c(x)=i(x)\cdot g(x)\,.$$

Let instead of the data word i is transferred the polynomial $c(x)$, i.e. its coefficients, on a connection channel and on the other end of the connection channel polynomial

$$\upsilon(x)=\upsilon_{n-1}x^{n-1}+...+\upsilon_1x+\upsilon_0$$

is received. This means that the received n-dimensional vector, which formed from the coefficients of the polynomial $\upsilon(x)$. Let's $e(x)$ is error polynomial, i.e.:

$$e(x)=\upsilon(x)+c(x)\,.$$

Let's $s(x)$ is syndrome polynomial, i.e.

$$s(x)=R_{g(x)}[\upsilon(x)]\,.$$

It is clear that

$$\begin{aligned} s(x)&=R_{g(x)}[\upsilon(x)]=\\ &=R_{g(x)}[c(x)+e(x)]=R_{g(x)}[e(x)]. \end{aligned} \qquad (2)$$

Let's

$$e(x)=e_{n-1}x^{n-1}+...+e_1x+e_0,$$

$$s(x)=s_{n-k-1}x^{n-k-1}+...+s_1x+s_0.$$

The problem of decoding the received polynomial $\upsilon(x)$ consist in finding in it those positions, which are happened mistakes in them, their correction and calculation of data polynomial.

II. The Description of Encoding of Data Words

When encoding of data words the encoder works n cycles. In the initial k cycles are moves to the input sequence $i_0,i_1,...,i_{k-1}$, and in the subsequent cycles $n-k-1$ are moves to the input zero. The output of the encoder must be obtained from the coefficients of the polynomial code sequence $c_0,c_1,...,c_{n-1}$. The works of encoder can be represented by the following sequential machine (SM) [1], described by the following equation:

$$y[t]=\sum_{\alpha=0}^{n-k} g_\alpha z[t-\alpha],\ t=0,1,\ldots,n-1, GF(2) \quad ,$$

where $z[t]$ and $y[t]$ are the input and $y[t]$ output sequences of the encoder respectively, and g_α, $\alpha=0,1,\ldots,n-k$ are the coefficients of the generator polynomial.

III. The Description of Decoding of the Received Binary Codes Word

The description of process the decoding of received words we will also implement in a class SM. If the d - the minimum distance in the cyclic code B, then each polynomial error of weight less than $d/2$ corresponds to a single syndrome polynomial [1]. For detection mistakes in received polynomial, theirs correction and the find from them the data polynomials using a special method based on table of syndrome polynomials and corresponding polynomial error. In [1] this method also is generalized on the base of theorem Meggitt's. According to this theorem [1] can be accepted

$$R_{g(x)}[x\,e(x)\,(\mathrm{mod}\,x^n+1)]=R_{g(x)}[x\,s(x)].$$

From (2) follows that, if syndrome polynomial $s(x)$ corresponds to the error polynomial $e(x)$, then syndrome polynomial

$$s'(x)=xs(x)(\mathrm{mod}\,g(x))$$

corresponds to the error polynomial

$$e'(x)=xe(x)(\mathrm{mod}\,x^n+1).$$

It gives the possible to memorize in the table not all syndrome polynomials and the corresponding error polynomials to them. Memorizing in the table a specific syndrome polynomial $s(x)$ and the corresponding to them polynomial error $e(x)$, the error polynomial can be defined for all polynomials of syndrome polynomial $s(x)$, which are obtained from the following

$$s'(x)=\underbrace{R_{g(x)}[R_{g(x)}[\ldots[R_{g(x)}}_{\nu}[s(x)]\ldots]].$$

Syndrome polynomials $s'(x)$ corresponds to the polynomial error $e'(x)$, where

$$e'(x)=x^\nu e(x)(\mathrm{mod}\,x^n+1).$$

Can be memorized in the table those syndrome polynomials, leading coefficient which is a unity. Such polynomials we will call basic syndrome polynomials. Basic syndrome polynomials we will written as

$$s^b(x)=s^b_{n-k-1}x^{n-k-1}+\ldots+s^b_1x+s^b_0.$$

Let's $s(x)$ is basic syndrome polynomial. If the syndrome polynomial $s'(x)$ is not a basic syndrome polynomial, but with a several steps it the shift to the right from them accepts a polynomial, that coincides with the basic syndrome polynomials $s(x)$, then $s(x)$ is called syndrome polynomial, relating to the basic syndrome polynomials $s(x)$.

The coefficients of the polynomial $\upsilon(x)$ are moves to inputs of the decoder. In the decoder polynomial $\upsilon(x)$ is divided by a generator polynomial $g(x)$, the obtained remainder accepts as syndrome polynomial. For calculation of a syndrome polynomial, can be use a binary SM [3], described by the following equation:

$$\begin{cases} z_\alpha[0]=\upsilon_\alpha,\ \alpha=0,1,\ldots,n-1, \\ z_{n-\beta-\alpha}[\beta]=z_{n-\beta-\alpha}[\beta-1]+ \\ \quad +z_{n-\beta}[\beta-1]g_{n-k-\alpha}, GF(2), \\ \alpha=1,\ldots,n-k, \\ z_{n-\beta-\alpha}[\beta]=z_{n-\beta-\alpha}[\beta-1], \\ \alpha=n-k+1,\ldots,n-\beta, \beta=1,2,\ldots,k. \end{cases} \quad (3)$$

The value of the output sequence of the SM (3) is the coefficients of syndrome polynomial, i.e.

$$s_{n-k-\alpha}=z_{n-k-\alpha}[k],\ \alpha=1,2,\ldots,n-k. \quad (4)$$

The decoder, after calculation of a syndrome polynomial scheme (3), (4) should verifying: there were mistakes (error) or not.

If $s(x)=0$, then errors no occurred. If $s(x)\neq 0$, then errors occurred. In this case, the decoder should be correct the errors. If the polynomial $s(x)$ is a basic syndrome polynomial, then accepts $\nu=0$ and $s^b(x)\equiv s(x)$, i.e.

$$s^b_\alpha=s_\alpha,\ \alpha=0,1,\ldots,n-k-1.$$

In the case, where the polynomial $s(x)$ is not a basic syndrome polynomial, then find of the corresponding to basic syndrome polynomial $s(x)$ it is necessary to shift to the right until the leading coefficient does not become unit. This amount of shift can be define on the base of the following recurrent formula:

$$\begin{cases} \nu=0,\quad p=1; \\ p:=p(s_{n-k-i}+1),\ GF(2), \\ \nu:=\nu+p,\quad i=1,2,\ldots,n-k-1. \end{cases} \quad (5)$$

At calculation of the formula (5) values of ν is the necessary number of shift of a polynomial $s(x)$. Using the syndrome polynomial $s(x)$ and the value ν found by the scheme (5) we can find the coefficients of the basis syndrome polynomial $s^b(x)$, to which relating the $s(x)$, following recurrent formula:

$$\begin{cases} s^b_{n-k-1-\gamma}=s_{n-k-1-\gamma-\nu},\ \gamma=0,1,\ldots,n\text{-}k\text{-}1\text{-}\nu; \\ s^b_{\gamma-1}=0,\quad \gamma=1,\ldots,\nu. \end{cases}$$

Let the number of all polynomials basic syndrome equally to M. Let the coefficients of the β -th basic syndrome polynomial are

$$S_\alpha^{(\beta)}, \ \alpha = 0,1,\ldots,n-k-1 .$$

Let's the coefficients of the error polynomial corresponding to the β -th basic syndrome polynomial are

$$e_\alpha^{(\beta)}, \ \alpha = 0,1,\ldots,n-1 .$$

On of coefficients of the basis syndrome polynomial $s^b(x)$ from the table, can be find the number of the error polynomial. This can be accomplished by the following recurrent formula:

$$\begin{cases} j = 1, \ p = 1; \\ P_\beta = \prod_{\alpha=0}^{n-k-1} \left(s_\alpha^b + S_\alpha^{(\beta)} + 1 \right), GF(2), \ \beta = 1,\ldots,M; \\ p := p(P_\beta + 1), \ GF(2), \\ j := j + p, \qquad \beta = 1,\ldots,M. \end{cases} \tag{6}$$

After completing the calculations in (6) value j is the number of basic syndrome polynomial of the in the table, that matches $s^b(x)$. Thus, the corresponding polynomial error will be the

$$e^{(j)}(x) = e_{n-1}^{(j)} x^{n-1} + \ldots + e_1^{(j)} x + e_0^{(j)} .$$

In the case $\nu = 0$ we accept

$$e_\alpha = e_\alpha^{(j)}, \ \alpha = 0,1,\ldots,n\text{-}1 .$$

In the case $\nu \geq 1$ for find the error polynomial $e(x)$, corresponding to the polynomial $s(x)$, it is possible to use following equality

$$e^{(j)}(x) = x^\nu e(x) (\bmod x^n + 1) .$$

Therefore, from the last equality, we receive:

$$\begin{cases} e_\alpha = e_{\nu+\alpha}^{(j)}, \ \alpha = 0,1,\ldots,n\text{-}1\text{-}\nu ; \\ e_{n-\nu+\alpha} = e_\alpha^{(j)}, \ \alpha = 0,1,\ldots,\nu - 1. \end{cases}$$

After finding the polynomial errors $e(x)$ can be corrected polynomial $\upsilon(x)$ on the base following formula:

$$\upsilon_\alpha := \upsilon_\alpha + e_\alpha, \quad \alpha = 0,1,\ldots,n-1, \ GF(2).$$

Further, for finding the data polynomial $i(x)$ necessary to divide a corrected received polynomial $\upsilon(x)$ by a polynomial $g(x)$. For the implementation of the process of division can use a binary SM, described by the following equation:

$$\begin{cases} y_\alpha[0] = \upsilon_\alpha, \ \alpha = 0,1,\ldots,n-1, \\ y_{n-\beta-\alpha}[\beta] = y_{n-\beta-\alpha}[\beta - 1] + y_{n-\beta}[\beta - 1] g_{n-k-\alpha}, GF(2), \\ \qquad \alpha = 1,\ldots,n-k, \\ y_{n-\beta-\alpha}[\beta] = y_{n-\beta-\alpha}[\beta - 1], \\ \ \alpha = n-k+1,\ldots,n-\beta, \\ i_{k-\beta}[\beta] = y_{n-\beta}[\beta - 1], \ \beta = 1,2,\ldots,k. \end{cases}$$

IV. Conclusion

Thus, the formulas are accepts for the encoding data words and description of detecting and correcting errors in the received code words in the class of the SM. The process of encoding and decoding can be realized by software or a circuit.

References

[1] Richard E. Blahut, Theory and practice of error control codes. M: World, 1986, 576 p.

[2] William Cary Huffman, Vera Pless. Fundamentals of Error-Correcting Codes. Cambridge University Press, 2003.

[3] Feyziyev F.G., Faradzheva M.R. Modular sequential machines: The main theoretical and applied results, Baku, Elm, 2006, 234 p.