BCH CODES DECODER BASED ON EUCLID ALGORITHM

B I Filippov[1]
[1]*Novosibirsk State Technical University, Department of Information Security, Novosibirsk City, Russian Federation*
filippov-boris@rambler.ru

DOI: 10.36724/2664-066X-2021-7-2-14-17

ABSTRACT

In the process of algebraic decoding of BCH codes over the field GF(q) with the word length n = qm-1, correcting t errors, both in the time and frequency domains, it is necessary to find the error locator polynomial ?(x) as the least polynomial for which the key equation. Berlekamp proposed a simple iterative scheme, which was called the Berlekamp-Messi algorithm, and is currently used in most practical applications. Comparative statistical tests of the proposed decoder and decoder using the Berlikamp-Messi algorithm showed that they differ slightly in decoding speed. The proposed algorithm is implemented in the environment in Turbo Pascal and can be used for the entire family of BCH codes by replacing the primitive Galois polynomial.

KEYWORDS: *Berlekamp-Messi algorithm, Euclidean algorithm, BCH codes, Galois polynomial, decoder*

I. INTRODUCTION

In the process of algebraic decoding of BCH codes over the field *GF(q)* with the word length $n = q^m-1$, correcting *t* errors, both in the time and frequency domains, it is necessary to find the error locator polynomial $\Lambda(x)$ as the least polynomial for which the key equation [1]

$$\sum_{k=0}^{n-1} \Lambda_k e_{j-k},\ j = 0,1,...,n-1. \quad (1)$$

The degree of the polynomial $\deg \Lambda(x) \le t$ and $\Lambda_0=1$, so (1) takes the form:

$$e_j = -\sum_{k=1}^{2t} \Lambda_k e_{j-k},\ j = 0,1,...,n-1,$$

and it is possible to cyclically obtain all e_j and Λ_k components.

For non-binary BCH codes, in addition to the error locator equation, it is necessary to find a polynomial of error values *E(x)* in the frequency space, which is associated with $\Lambda(x)$ and the error syndrome *S(x)* equation, which in this case is also a key equation [2].

$$E(x) = (\Lambda(x)\cdot S(x)) \bmod x^{2t}, \quad (2)$$

at that, $\deg \Lambda(x) \le t$, and $\deg E(x) \le t-1$.

II. FORMULATION OF THE PROBLEM

In the first published procedures for solving the key equation, standard matrix inversion methods were used. However, later, Berlekamp proposed a simple iterative scheme, which was called the Berlekamp – Messi algorithm, and is currently used in most practical applications [1, 3]. More recently, it was shown that the solution of a key equation can also be obtained using the Euclidean algorithm. **The purpose of this work** is to develop an algorithm for decoding BCH codes based on the Euclidean algorithm, which is simple and versatile, and software for experimental research and comparison with the Berlekamp-Messi algorithm.

III. ALGORITHM FOR SOLVING THE KEY EQUATION

The solution of equation (3) can be obtained using the Euclidean algorithm.

The Euclidean algorithm is a recurrent method for determining the greatest common divisor of two polynomials (or two integers) over the field *GF(q)*.

For example, if $\deg s(x) \ge \deg r(x) \ge 0$, then in accordance with the Euclidean algorithm

$$\begin{aligned}
s(x) &= d_1(x)\cdot r(x) + r_1(x),\\
r(x) &= d_2(x)\cdot r_1(x) + r_2(x),\\
r_1(x) &= d_3(x)\cdot r_2(x) + r_3(x),\\
&\dots\dots\dots\dots\dots\dots\\
r_{n-2}(x) &= d_n(x)\cdot r_{n-1}(x) + r_n(x),\\
r_{n-1}(x) &= d_{n+1}(x)\cdot r_n(x) + 0.
\end{aligned} \quad (3)$$

As a consequence, it turns out that

$$r_n(x) = a(x)s(x) + b(x)r(x), \quad (4)$$

where $a(x)$ and $b(x)$ - polynomials over the field $GF(q)$.

From intermediate iterations (4), it can be noted that each subsequent equation is obtained from the two previous ones according to the following rule

$$r_i(x) = r_{i-2}(x) - q_i(x)\cdot r_{i-1}(x),$$

where $d_i(x)$ - quotient from dividing polynomials $r_{i-2}(x)$ by $r_{i-1}(x)$ for non-negative degrees *x*

$$d_i(x) = \left| \frac{r_{i-2}(x)}{r_{i-1}(x)} \right|. \quad (5)$$

The connection of the Euclidean algorithm with the problem of solving the key equation (3) becomes obvious if we represent equation (4) in the form

$$b(x)r(x) \equiv r_n(x) \bmod s(x).$$

Then, assuming that $s(x) = x^{2t}$, and $b(x) = S(x)$, $r(x) = \Lambda(x)$, $r_n(x) = E(x)$, get the key equation (2) in the form $\Lambda(x)S(x) \equiv E(x) \bmod x^{2t}$.

Thus, to solve the key equation, the Euclidean algorithm should be applied until the condition $\deg E_i(x) < t$. The description of the method for solving the key equation is summarized for the BCH codes correcting *t* errors:

1. Apply the Euclidean algorithm to $s(x) = x^{2t}$ and $b(x) = S(x)$,
2. Adduc

$$d_i(x) = \left| \frac{r_{i-2}(x)}{r_{i-1}(x)} \right| = \left| \frac{E_{i-2}(x)}{E_{i-1}(x)} \right|,$$

$$E_i(x) = E_{i-2}(x) - d_i(x)\cdot E_{i-1}(x),$$

$$\Lambda_i(x) = \Lambda_{i-2}(x) - d_i(x)\cdot \Lambda_{i-1}(x);$$

3. Use initial conditions:

$$\Lambda_{-1}(x) = 0, \Lambda_0(x) = 1,$$

$$E_{-1}(x) = x^{2t}, E_0(x) = S(x);$$

4. op, when $\deg E_i(x) < t$;

5. Adduc $n = i,\ \Lambda(x) = \Lambda_n(x),\ \ E(x) = E_n(x).$

To calculate $d(x)$ in algorithm (5), we use the simplified iterative procedure proposed in [2]

$$d_{b-a-i} = \frac{1}{r_a}\left(S_{b-i} - \sum_{j=0}^{i-1} d_{b-a-j} r_{a-j-i}\right) = \left|\frac{E_{i-2}(x)}{E_{i-1}(x)}\right|,$$

where $b = \deg s(x),\ a = \deg r(x)$, and the degree of the quotient $d(x)$ is (*b*-*a*) and depends on $r(x)$ only through the coefficients of this polynomial $r_a, r_{a-1}, ..., r_{b-a}$.

This procedure for calculating the quotient must be repeated at each step of the Euclidean algorithm so that at the first step it has the form:

$$d_1 = \frac{S_{2t}}{E_{(2t-1)}};\quad d_0 = d_1 \cdot \frac{E_{(2t-2)}}{E_{(2t-1)}};$$

and on the intermediate and last iteration steps:

$$d_{(j-i)} = \frac{E_{(b-i)}^{(n-2)} - \sum_{ii=0}^{i-1} d_{(b-ii)} \cdot E_{(a-i-ii)}^{(n-1)}}{E_a^{(n-1)}},$$

where $b = \deg[E^{(n-2)}(x)],\ \ a = \deg[E^{(n-1)}(x)]$; $j = (b-a)$; $i = 0, ..., j$; the superscript of the coefficients $E_{(i)}^{(j)}$ indicates the iteration number, and the lower one the degree of x of the equation $E^{(j)}(x)$, at which this coefficient should be taken.

After solving the key equation using the Euclidean algorithm, the positions and error values in the received codeword are determined as usual by the solution of $\Lambda(x)$ and $E(x)$ [2]. In the first case, the roots of the equation $\Lambda(x)$ are found using the Chen procedure [2], given that the i[th] symbol is erroneous if $\Lambda(\alpha^{-i})$=0 or:

$$\Lambda(\alpha^{-i}) = \sum_{k=0}^{t} \Lambda_k \alpha^{-ik} = 0. \qquad (6)$$

It remains to find all values of *i* for which equality (6) is satisfied.

The error values in the *i* positions can be determined using the Forney algorithm

$$e_i = -\frac{E(\alpha^{-i})}{\Lambda'(\alpha^{-i})} = -\frac{\sum_{k=0}^{t} E_k \alpha^{-ik}}{\Lambda'(\alpha^{-i})},$$

where $\Lambda'(\alpha^{-i})$ - derivative $\Lambda(x)$ at $x = \alpha^{-i}$ for a binary Galois field is

$$\Lambda'(x) = \Lambda_1 + \Lambda_3 x^2 + \Lambda_5 x^4 + ...$$

The decoding algorithm for non-binary BCH codes (Reed Solomon codes) using the Euclidean algorithm for solving the key equation is shown in Figure 1. The most complex operations are Fourier transforms at the beginning and at the final stage of decoding (Forney procedure). Therefore, the BCH binary decoder is faster.

The decoding process requires the computation of Galois field elements and the multiplication of field elements. Since the multiplication operation is reduced to the summation of the exponents of the elements, the elements of the Galois field should be defined both in the form of the exponents of the powers of the elements and in the binary representation.

IV. RESEARCH RESULTS

Consider the decoding process of the binary BCH code (63,51), which corrects ≤ 3 errors in the Galois field GF(2^6) over a primitive polynomial

$$p(x) = x^6 + x^5 + 1.$$

Three errors occurred in the channel in the 42nd, 21st and 16th symbols and the error polynomial has the form

$$e(x) = x^{42} + x^{21} + x^{16}.$$

1. Calculating the syndrome of errors in the frequency space:

$$S(x) = \alpha^{33}x^5 + \alpha^3 x^4 + \alpha^{48}x^3 + \alpha^6 x^2 + \alpha^{47}x + \alpha^{33}.$$

2. nding the solution of the key equation using the Euclidean algorithm:

$E_0(x) = S(x)$, a $V_0(x) = 1$.

The process of solving the iterations is shown in Table 1.

TABLE I

PROCESS OF CALCULATION OF ERROR LOCATOR EQUATION

r	0	1	2	3
Deg [E_{r-1}]	5	5	4	3
$d_r(x)$		$\alpha^{30}x + \alpha^{44}$	$\alpha^{20}x + \alpha^{40}$	$\alpha^{60}x + \alpha^{24}$
$V_r(x)$	0	$\alpha^{30}x + \alpha^{44}$	$\alpha^{50}x^2+\alpha^2x+\alpha^{42}$	$\alpha^{47}x^3+\alpha x^2+\alpha x+\alpha^{31}$
$E_r(x)$	$S(x)$	$\alpha^{13}x^4+\alpha^{28}x^3 +\alpha^5x^2+ +\alpha^{17}x+\alpha^{14}$	$\alpha^{16}x^3+\alpha^{33}x^2+\alpha^{33} x+\alpha^{12}$	$\alpha^{28}x^3+\alpha^{48}x^2+\alpha^{17}x +\alpha^{36}$

3. Transform the resulting error locator equation into a temporary space (Fourier transform). We obtain an equation $v(x)$, it values of the field elements of which

from x^{63} to x^0 (from left to right) are shown below in decimal representation:

(29, 39, 44, 32, 36, 45, 33, 23, 40, 41, 47, 49, 22, 50, 43, 24, 42, 12, 50, 46, 0, 33, 57, 2, 52, 32, 19, 3, 39, 18, 57, 21, 45, 4, 56, 1, 50, 12, 2, 42, 14, 0, 45, 17, 20, 12, 0, 31, 39, 25, 60, 33, 57, 5, 30, 40, 5, 6, 8, 48, 32, 40, 2).

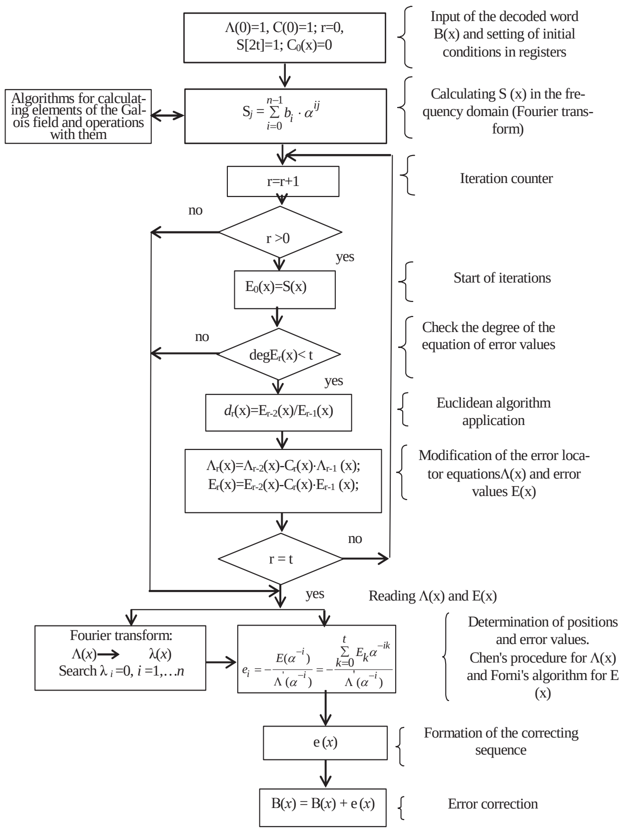

Fig. 1. Algorithm for decoding BCH codes
by the Euclidean algorithm for non-binary codes

4. Zero val s of field elements occur at x^{42}, x^{21} and x^{16}, which indicates the position of errors.

V. Conclusions

Comparative statistical tests of the proposed decoder and decoder using the Berlikamp-Messi algorithm showed that they differ slightly in decoding speed. The algorithm proposed in Figure 1 is implemented in the Turbo Pascal environment and can be used for the whole family of BCH codes by replacing the primitive Galois field polynomial.

References

[1] Clark J and Kane J 1987 *Coding with error correction in digital communication systems* (Moscow: Trans. from English/Ed. Tsybakov B S, Pub.: Radio and communication) 392 p.

[2] Blehut R 1986 *Theory and Practice of Error Control Codes* (Moscow: Trans. from English/Ed. Zigangirov K Sh, Pub.: World) 576 p.

[3] Filippov B I 2015 *Radio engineering systems (Novosibirsk: Filippov B I, NSTU Publishing House) 386 p.*