Postprint: RS Decoding Optimization and Simulation under CCSDS for Satellite Communications

Authors: Bingrui Wang, Yang Xiaofei, Yao Xingzhong

Date: 2019-04-01T00:00:00+00:00

Abstract

To address the inflexibility in the key step of error value computation in Reed-Solomon (RS) decoding, a more general solution algorithm is proposed. This algorithm incorporates multiple primitive element operations, making it universally applicable to different parameters. To mitigate the excessive computational complexity when solving the error value polynomial in this algorithm, an optimization method based on the characteristics of the Galois field is proposed, thereby halving the number of operations and saving storage resources. For another step in RS decoding, namely solving the error locator polynomial with high iterative complexity, a fast iteration count search algorithm is presented through detailed analysis of compensation differences, reducing the iterative complexity by an order of magnitude from $O(n^2)$ to $O(n)$. Taking RS(255,223) under the Consultative Committee for Space Data Systems (CCSDS) standard in satellite communications as the specific research object, data simulation analysis and bit error rate testing were conducted in combination with the optimized decoding algorithm. Experimental results demonstrate that adopting the improved error value computation algorithm and optimized iteration count search algorithm can achieve efficient and fast decoding.

Full Text

Improved RS Decoding Algorithm and RS Decoding Simulation under CCSDS Standard in Satellite Communications

Wang Bingrui[1,2], Yang Xiaofei[2], Yao Xingzhong[3] [1]School of Software, Nanyang Normal University, Nanyang Henan 473007, China; [2]School of Optics & Electronics, Huazhong University of Science & Technology, Wuhan 430074, China; [3]Rocket Army Academy, Beijing 100085, China

Abstract: This paper proposes a more general algorithm to address the inflexibility in solving error values, a critical step in Reed-Solomon (RS) decoding. The algorithm incorporates multiple primitive element operations, making it universally applicable to different parameters. To reduce the excessive computational complexity involved in solving the error value polynomial, an optimization method based on Galois field characteristics is proposed, which eliminates half of the operations and saves storage resources. To tackle the problem of high iterative complexity when solving the error location polynomial, a fast search algorithm for iteration times is presented through detailed analysis of compensation differences, reducing the iterative complexity from $O(n^2)$ by an order of magnitude to $O(n)$. Taking RS(255, 223) under the Consultative Committee for Space Data Systems (CCSDS) standard in satellite communications as the specific research object, the paper conducts data simulation analysis and bit error rate testing combined with the optimized decoding algorithm. Experimental results demonstrate that the improved error value solving algorithm and optimized iteration search algorithm enable effective and fast decoding.

Key words: Reed-Solomon (RS) code; Galois field; error value polynomial

0 Introduction

Reed-Solomon (RS) codes can correct both random errors and burst errors, with stronger capability for the latter. RS codes are widely used in data storage and communications. With the development of Internet of Things technology, an increasing number of devices are being connected and generating massive amounts of data. Cloud-based storage technology has become mainstream by offloading compute-intensive tasks to edge devices. Wang et al. [?] proposed a new fog computing-based architecture for data synchronization and adopted RS codes to ensure security. Demirkan and Silvus [?] combined soft-output Viterbi algorithm and proposed a multilevel interleaved RS code architecture for perpendicular magnetic recording. Li et al. [?] proposed two RS decoding methods for burst Rayleigh fading channels with additive white Gaussian noise. In regions containing only additive white Gaussian noise, only error correction processing is required, while in burst fading regions, both error and erasure correction processing are performed. In nanoscale communications that use molecules as information carriers, molecular communication represents a new paradigm. In diffusion-based molecular communication, system performance is susceptible to inter-symbol interference caused by consecutive molecular crossings. To address this issue, Dissanayake et al. [?] employed RS codes to improve transmission reliability. In direct-detection optical systems based on single-mode fiber, Chen et al. [?] experimentally demonstrated RS-coded multi-symbol interleaved real-time orthogonal frequency division multiplexing signal transmission, marking the first adoption of RS codes in real-time optical OFDM systems. Erasure codes such as Luby transform and Raptor provide resilient erasure distribution for computer networks. Borujeny and Ardakani [?] proposed a class of erasure codes based on RS codes that guarantee zero reception overhead.

RS codes have very broad applications. This paper focuses on research, analysis, and optimization of two key steps in RS decoding algorithms: solving the error location polynomial and solving error values. When solving the error location polynomial, search iteration operations are required with complexity O(n²). As the values of parity bits and code length continue to increase, the complexity becomes high. This paper proposes an improved method to reduce search complexity, which is highly significant. In specific RS code designs, many parameters are introduced, making the coefficients involved in calculations small and symmetric. Small coefficients facilitate computation, and symmetric coefficients can save storage. For example, if the first 16 data items among 32 data items are symmetric with the last 16 data items, only half the data needs to be stored. RS code parameters are flexibly designed, requiring a universal algorithm for solving error values. However, the error value solving algorithm introduced in literature [?] involves relatively single parameters. Therefore, this paper presents a more general error value solving algorithm with certain significance. Under the Consultative Committee for Space Data Systems (CCSDS) standard for satellite communications, specific numerical analysis and bit error rate simulation testing were conducted for RS(255,223) based on the improved algorithm.

1 Solving the Syndrome

For a set of error information not exceeding the error correction capability of RS codes, the RS decoding algorithm can detect errors, determine the error location polynomial, find error positions, calculate error values, and ultimately correct them. The decoding flowchart is shown in Figure 1.

[Figure 1: see original paper]

For convenience of study, we define the following polynomials. The information polynomial can be expressed as $c(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{k-1}x^{k-1}$. The encoded polynomial is $c(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{n-1}x^{n-1}$. The error polynomial generated in the channel is $e(x) = e_0 + e_1x + e_2x^2 + \cdots + e_{n-1}x^{n-1}$. The received polynomial can be written as $r(x) = r_0 + r_1x + r_2x^2 + \cdots + r_{n-1}x^{n-1}$. The relationship between polynomials (2), (3), and (4) is $r(x) = e(x) + c(x)$.

The polynomial expression containing t errors is $e(x) = e_{j_1}x^{j_1} + e_{j_2}x^{j_2} + \cdots + e_{j_t}x^{j_t}$, where $e_{j_1}, e_{j_2}, \dots, e_{j_t}$ are error values and $j_1, j_2, \dots, j_t$ are error positions. $X_j = \alpha^j$ represents the error position as a whole and is not the product of j and t. For convenience of expression, we use Y_i to replace e_{j_i} and X_i to replace x^{j_i}.

The generator polynomial is defined as $g(x) = \prod_{i=1}^{2t}(x - \alpha^{C+b+i})$, where C and b are constants and α is a primitive element in the Galois field. For the CCSDS standard, C takes the value 11 and b takes the value 111. Substituting $x = \alpha^{C+b+i}$ into $r(x)$ yields values called syndromes, denoted as s_i.

Since α^{C+b+i} is a root of $g(x)$, substituting $x = \alpha^{C+b+i}$ into $c(x)$ gives 0. Observing the syndrome expression, we find that syndromes can be implemented using cyclic iteration. RS decoding aims to determine error values Y_1 to Y_t and error positions X_1 to X_t. However, direct solution is difficult, so indirect methods are generally used.

The error location polynomial is defined as $\sigma(x) = \prod_{i=1}^{t}(1 - X_i x) = 1 + \sigma_1 x + \sigma_2 x^2 + \cdots + \sigma_t x^t$.

The Berlekamp-Massey (BM) algorithm is generally used to solve the error location polynomial [**?**, **?**]. Let μ be the iteration number, $\sigma^{(\mu)}(x)$ be the error polynomial at iteration μ, d_μ be the discrepancy at iteration μ, and l_μ be the degree of the next polynomial $\sigma^{(\mu+1)}(x)$. To solve for $\sigma(x)$, we must verify the discrepancy d_μ. The expressions are as follows:

If $d_\mu = 0$, then $\sigma^{(\mu+1)}(x) = \sigma^{(\mu)}(x)$. If $d_\mu \neq 0$, then we correct $\sigma^{(\mu)}(x)$ by finding a previous iteration ρ before iteration μ such that $d_\rho \neq 0$ and $2\rho - l_\rho$ is maximized. Then we have $\sigma^{(\mu+1)}(x) = \sigma^{(\mu)}(x) - d_\mu d_\rho^{-1} x^{\mu-\rho} \sigma^{(\rho)}(x)$. Operating according to this procedure from the first iteration until the $2t$-th iteration ends, finding the ρ-th iteration is a key step in the BM algorithm.

2.2 Improved Search Algorithm

Based on the previous analysis, when all $d_\mu \neq 0$, the degrees of any three consecutive iterations will not be equal, nor will they all be unequal. Therefore, the degree of $\sigma(x)$ will increase with two consecutive equal values, i.e., the pattern 0, 0, 1, 1, 2, 2, ⋯, $t-1$, $t-1$, t. Meanwhile, the iteration number μ increases from 1 to $2t$ with a difference of 1. The value of $2\mu - l_\mu$ increases with the iteration number.

Thus, when all $d_\mu \neq 0$, the ρ-th iteration we seek is the most recent iteration before μ where $d_\rho \neq 0$, and $\rho = \mu - 1$. This is the improved search algorithm. At this point, we obtain the improved expression $\sigma^{(\mu+1)}(x) = \sigma^{(\mu)}(x) - d_\mu d_{\mu-1}^{-1} x \sigma^{(\mu-1)}(x)$.

On the basis of the improved search algorithm, when encountering $d_\mu = 0$, we find the most recent iteration ρ before μ where $d_\rho \neq 0$, compare the size of $2\rho - l_\rho$, and save the maximum value, requiring only one comparison.

The original BM algorithm requires $t(1 + 2t)$ searches with complexity O(n²). The improved algorithm requires only $2t$ searches with complexity O(n), reducing the complexity by an order of magnitude.

2.1 Original Solving Algorithm

According to RS coding theory [**?**], we have $s(x) = \sum_{i=1}^{2t} s_i x^{i-1} = \sum_{i=1}^{2t} \sum_{k=1}^{t} Y_k X_k^{C+b+i} x^{i-1}$.

3 Solving Error Locations

For RS(n, k), the reciprocals of values that make equation (11) equal to zero are the error positions. There are n test values $\alpha^0, \alpha^1, \alpha^2, \dots, \alpha^{n-1}$. Substituting these into equation (11) yields $\sigma(\alpha^{-j_m}) = 0$ for $1 \le m \le t$. Observing equation (15), we can solve it using cyclic iteration, which becomes $\sigma(x) = \prod_{i=1}^{t}(1-X_i x)$. Taking the first derivative gives $\sigma'(x) = \sum_{m=1}^{t}(-X_m)\prod_{i=1,i\neq m}^{t}(1-X_i x)$.

4.1 General Algorithm for Solving Error Values

Building upon the error value solving algorithm introduced in literature [**?**], we derive a formula suitable for multiple standards. All syndrome values are determined real integers that can be written in polynomial form: $s(x) = s_1 + s_2 x + s_3 x^2 + \cdots + s_{2t} x^{2t-1}$.

Substituting into equation (22) yields $s(x) = \sum_{i=1}^{2t}\sum_{k=1}^{t} Y_k X_k^{C+b+i} x^{i-1}$. Combining with equation (10), $s(x)$ can also be expressed as $s(x) = \sum_{k=1}^{t} Y_k X_k^{C+b+1} \frac{1-(X_k x)^{2t}}{1-X_k x}$, where Y_k are error values and jk as a whole represents error positions with values $j_1, j_2, \dots, j_t$.

After finding error locations, the values of X_k are known. The first term in this expression is a constant. Therefore, $s(x)$ can be expressed as $s(x) = \sum_{k=1}^{t} \frac{Y_k X_k^{C+b+1}}{1-X_k x}$. Combining with equation (21) gives $w(x) = s(x)\sigma(x) = \sum_{k=1}^{t} Y_k X_k^{C+b+1} \prod_{i=1,i\neq k}^{t}(1-X_i x)$. The error values we need to solve are Y_k.

When $s(x)$ and $\sigma(x)$ are determined, $w(x)$ is known. Since RS code operations are performed in the Galois field, we further simplify equation (25) to $Y_m = \frac{w(X_m^{-1})}{X_m^{C+b}\sigma'(X_m^{-1})}$. This is the formula derived in this paper for solving error values, suitable for multiple parameters.

4.2 Optimization of the Evaluation Formula

Define an error value polynomial $w(x) = s(x)\sigma(x)$. The highest degree of $s(x)$ is $2t$, and the highest degree of $\sigma(x)$ is t. Their multiplication would produce degree $3t$, requiring modulo x^{2t+1} operation: $w(x) = s(x)\sigma(x) \mod x^{2t+1}$.

In equation (26), $w(x)$ is a polynomial of degree t composed of t factors, requiring $2t$ multiply-accumulate operations. When solving for $w(x)$, we don' t need to involve all terms of $s(x)$ and $\sigma(x)$. Only the constant term and coefficients with degree less than $t+1$ need to participate, while terms with degree greater than $t+1$ can be omitted, saving half the operations. Thus we have $w(x) = \left(\sum_{i=0}^{t} s_i x^i\right)\left(\sum_{j=0}^{t} \sigma_j x^j\right) \mod x^{t+1}$.

5 RS Decoding Simulation Test for CCSDS in Satellite Communications

The tested RS code is RS(255, 223) under the CCSDS standard [?]. The input information data consists of 223 information symbols: 1, 2, 3, ···, 221, 222, 223. After RS encoding, the 32 parity symbols are [223, 143, 243, 66, 0, 177, 182, 232, 176, 79, 114, 129, 85, 7, 223, 153, 129, 150, 94, 238, 241, 200, 6, 100, 229, 108, 173, 61, 98, 107, 173, 240]. The 255 encoded data symbols are [1, 2, 3, ···, 222, 223, 223, 143, 243, 66, 0, 177, 182, 232, 176, 79, 114, 129, 85, 7, 223, 153, 129, 150, 94, 238, 241, 200, 6, 100, 229, 108, 173, 61, 98, 107, 173, 240], corresponding to the transmitted information polynomial from left to right.

To verify the accuracy of the proposed RS decoding algorithm, we set the first 16 of the 32 parity symbols to values 1 through 16, transforming the encoded data to [1, 2, 3, ···, 222, 223, 1, 2, 3, ···, 14, 15, 16, 129, 150, 94, 238, 241, 200, 6, 100, 229, 108, 173, 61, 98, 107, 173, 240], corresponding to the received polynomial $r(x)$. The calculated syndrome is [80, 194, 209, 59, 138, 42, 166, 186, 62, 249, 35, 8, 226, 71, 92, 184, 126, 58, 88, 203, 99, 42, 131, 225, 17, 110, 48, 216, 73, 7, 102, 241].

Applying the improved search algorithm yields the error location polynomial coefficients [68, 40, 156, 53, 121, 91, 24, 126, 158, 88, 97, 123, 31, 134, 146, 251], totaling 16 values. The 32 discrepancy values d_μ are [80, 152, 138, 172, 10, 243, 237, 13, 158, 140, 78, 176, 247, 19, 23, 206, 167, 130, 179, 70, 171, 205, 79, 193, 220, 31, 197, 55, 172, 205, 224, 178], totaling 32 values. The degrees l_μ produced at each run are [0, 0, 1, 1, 2, 2, 3, 3, 4, 4, 5, 5, 6, 6, 7, 7, 8, 8, 9, 9, 10, 10, 11, 11, 12, 12, 13, 13, 14, 14, 15, 15], totaling 32 values. These values verify the correctness of the improved BM search algorithm.

Next, the error locations are found to be [224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239], with corresponding error values [222, 141, 240, 70, 5, 183, 177, 224, 185, 69, 121, 141, 88, 55, 208, 137]. In the Galois field, adding the error values from the received information at the error positions to the error values calculated by RS decoding yields the correct result. That is, adding [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16] and [222, 141, 240, 70, 5, 183, 177, 224, 185, 69, 121, 141, 88, 55, 208, 137] produces [223, 143, 243, 66, 0, 177, 182, 232, 176, 79, 114, 129, 85, 7, 223, 153]. These corrected 16 values equal the first 16 of the 32 parity symbols after encoding, confirming that the originally introduced 16 errors have been corrected.

For bit error rate testing, BPSK modulation and additive white Gaussian noise were adopted in a MATLAB environment. The RS code uses the CCSDS RS(255, 223) code, where one symbol is 8 bits, the code length is 255 symbols, and the information length is 223 symbols. The encoding coefficients are [1, 91, 127, 86, 16, 30, 13, 235, 97, 165, 8, 42, 54, 86, 171, 32, 113, 32, 171, 86, 54, 42, 8, 165, 97, 235, 13, 30, 16, 86, 127, 91, 1]. After one million test runs using the improved decoding algorithm, the bit error rate curve was obtained and compared with the theoretical uncoded BPSK curve, as shown in Figure 2.

[Figure 2: see original paper]

As observed in Figure 2, the RS(255,223) curve basically matches the theoretical value when the signal-to-noise ratio is 0-4 dB. However, as the signal-to-noise ratio continues to increase, the RS(255,223) curve becomes steep and the bit error rate drops rapidly. At a bit error rate of 10^{-7}, RS(255,223) achieves a 5 dB gain over uncoded BPSK, thereby verifying the correctness of the improved decoding algorithm.

6 Conclusion

This paper conducted an in-depth analysis of RS decoding algorithms, studying syndrome calculation, error location polynomial solving, error location determination, and error value calculation. The BM algorithm is typically used to solve the error location polynomial. A key step in the BM algorithm is searching for a specific iteration, and this paper analyzed an improved search algorithm that reduces search complexity by an order of magnitude. For error location solving, a more general formula was derived by combining traditional algorithms. Taking RS(255,223) under the CCSDS standard as the research object, the improved decoding algorithm was used to solve error locations and error values, followed by specific numerical experiments and bit error rate testing. The test results demonstrate that the improved decoding algorithm can achieve fast and correct decoding, verifying its correctness. Future work includes: (a) optimizing the syndrome module to judge error conditions based on syndrome values; and (b) implementing high-speed parallel RS decoders and low-power serial RS decoders in hardware circuits.

References

[1] Wang Tian, Zhou Jiyuan, Liu Anfeng, et al. Fog-based computing and storage offloading for data synchronization in IoT [J]. IEEE Internet of Things Journal, 2018, DOI: 10.1109//JIOT.2018.2875915.

[2] Demirkan I, Silvus G. Multilevel Reed–Solomon codes for PMR channels [J]. IEEE Trans on Magnetics, 2016, 52(2): 1-8.

[3] Li Yong, Huang Xiang, He Jiguang, et al. On soft-information-based error and erasure decoding of Reed-Solomon codes in burst rayleigh fading channels [J]. IEEE Trans on Communications, 2018, DOI: 10.1109//TCOMM.2018.2872033.

[4] Dissanayake M B, Deng Y, Nallanathan A, et al. Reed Solomon codes for molecular communication with full absorption receiver [J]. IEEE Communications Letters, 2017, 21(6): 1-4.

[5] Chen Ming, Xiao Xin, Li Xinying, et al. Improved BER performance of real-time DDO-OFDM systems using interleaved Reed–Solomon codes [J]. IEEE Photonics Technology Letters, 2016, 28(9): 1014-1017.

[6] Borujeny R R, Ardakani I M. A new class of rateless codes based on Reed–Solomon codes [J]. IEEE Trans on Communications, 2016, 64(1): 1-13.

[7] Zhang Zongcheng. Error Correction Coding Principles and Applications [M]. Beijing: Publishing House of Electronics Industry, 2003: 100-150.

[8] Moon T K. Error correction coding: mathematical methods and algorithms [M]. Hoboken: Wiley, 2005: 235-280.

[9] Massey J L. Shift-register synthesis and BCH decoding [J]. IEEE Trans on Information Theory, 1969, 15(1): 122-127.

[10] Park J I, Lee K, Choi C S, et al. High-speed low-complexity Reed-Solomon decoder using pipelined Berlekamp-Massey algorithm and its folded architecture [J]. Journal of Semiconductor Technology & Science, 2010, 10(3): 193-202.

[11] Jorge C M, Patrick G F. Essentials of error-control coding [M]. Hoboken: Wiley, 2006: 100-153.

[12] CCSDS Secretariat. CCSDS 131.0-B-3 Blue Book, TM synchronization and channel coding [S]. Washington DC: Management Council of CCSDS, 2017.

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