IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 20, 2019, accepted March 8, 2019, date of publication March 13, 2019, date of current version March 29, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2904718

Parameter Identification of Reed-Solomon Codes Based on Probability Statistics and Galois Field Fourier Transform

PENGTAO LIU, ZHIPENG PAN, AND JING LEI
School of Electronic Science, National University of Defense Technology, Changsha 410073, China

Corresponding author: Jing Lei (leijing@nudt.edu.cn)

This work was supported by the National Natural Science Foundation of China under Grant 61502518 and Grant 61702536. Additionally, P. Liu wants to thank Y. Feng for her invaluable company and support over the years.

ABSTRACT The parameter identification of channel codes plays a significant role in the fields of adaptive modulation and coding (AMC) as well as non-cooperative communications. In this paper, an algorithm based on probability statistics and Galois field Fourier transform (PS-GFFT) is proposed to identify the parameters of the Reed–Solomon (RS) codes. A threshold obtained by the probability statistics is used to skip wrong parameters within a candidate set, while GFFT is applied to reduce the error identification probability. Meanwhile, the upper bound on correct recognition rate of RS codes has been derived and proved, which quantifies the influence of the received codewords' length, the bit-error-rate of codewords, and the number of bits per symbol on the accuracy of parameters estimation. To the best of our knowledge, the upper bound, which is of great significance in evaluating the performance of recognition algorithms, is provided in this paper for the first time. The numerous simulation results illustrate that the proposed algorithm has better recognition performance than the existing RS codes recognition algorithms. Specifically, the correct recognition probability of the RS codes whose length is no more than 255 can be over 90% when the bit error rate of codewords is below $3 * 10^{-3}$, while the conventional algorithms have the best correct recognition probability of 10%. Furthermore, it is observed that the correct recognition rate of our proposed algorithm is close to the derived upper bound, especially for long code length, which further verifies the superiority of our proposed algorithm.

INDEX TERMS Blind recognition, Reed-Solomon codes, probability statistics, Galois field Fourier transform.

I. INTRODUCTION

The parameter recognition of channel codes in a noisy environment is a crucial problem in the information communication field [1]. It has many applications including adaptive modulation and coding (AMC) and non-cooperative communications. Besides, it could also be applied in cognitive radio systems [2]–[4]. In digital communications, forward error correcting coding is often used to protect the transmitted information against noisy channels to reduce errors during transmission [5]. However, in those cases mentioned above, the receiver has no knowledge about the parameters used to encode the information at the transmitter. Therefore, it is necessary to design an intelligent receiver [4]–[6], which is able to blindly identify the encoder parameters from the data stream received from the channel [6].

Reed-Solomon (RS) code, which is a special class of non-binary Bose-Chaudhuri-Hocquenghem (BCH) codes [7], is widely used in data storage, digital broadcasting, and deep-space communications. There are plenty of applications, the most remarkable of which include storage systems like RAID-6, digital video devices such as DVDs and Blu-ray Discs, data transmission technologies such as QR Codes and WiMAX, and deep-space systems such as satellite communications and consultative committee for space data systems standards [7]–[12]. In consequence, it is necessary to recognize RS codes parameters over a noisy environment. A typical practical application including an intelligent receiver and a non-cooperative communicator of RS codes parameter estimation is shown in Fig. 1. It should be noted

The associate editor coordinating the review of this manuscript and approving it for publication was Kan Liu.

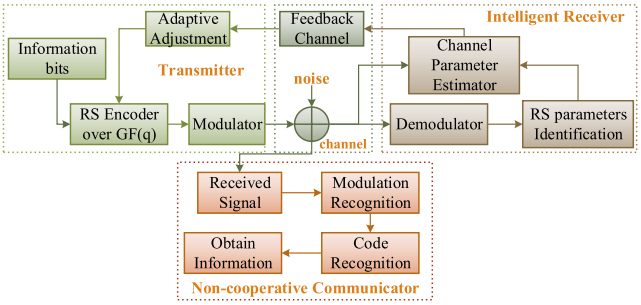


FIGURE 1. A practical application including an intelligent receiver and a non-cooperative communicator of RS codes parameter identification.

that we suppose there is no randomizer at the transmitter side. If a randomizer is used, presented methods of parameter identification of RS codes cannot be directly applied.

A wide variety of achievements have been made for the research of channel codes recognition algorithms. The syndrome posterior probability (SPP) is computed in [13] for blindly recognizing channel code from a candidate set that was used to encode a data stream. In [14], a method relied on a statistical analysis of a Euclidean distance matrix was proposed to estimate the code length of the linear block code. The paper [6] discusses recognition of binary BCH code in soft decision situations. Wu *et al.* [15] proposed a blind recognition method for BCH codes based on Galois field Fourier transform (GFFT), which can effectively identify the BCH codes in a new scenario (faster-than-Nyquist signaling system). Recently, an algorithm is proposed in [4] for error-free or severe erroneous channel conditions based on deficient rank and zero-mean-ratio values to blindly estimate LDPC code. The paper [2] uses the average likelihood difference (LD) of the parity-checks to recognize convolutional codes with computational complexity reduced. And the paper [5] proposes an algorithm to recognize convolutional and helical interleaver parameters based on the estimated value of rank-deficiency-difference. Three maximum-likelihood(ML)-based approaches for Space-Time Block Codes classification were proposed in [16].

Concerning the work related to RS codes recognition, blind recognition of RS codes was proposed firstly in [17]. The continuous zero spectrums were obtained by GFFT of codewords in order to recognize parameters of RS codes. However, as the code grows longer, the recognition process becomes more complex and time-consuming. After that, Li *et al.* [8] came up with a method to blindly recognize RS codes based on Galois field columns gaussian elimination. An improved algorithm based on matrix transformation with good efficiency and accuracy was proposed in [9], but its performance drops dramatically when the signal-to-noise ratio (SNR) decreases slightly. In [10], the algorithm for blind identification of RS code parameters was proposed and evaluated for various $M-$ary quadrature amplitude modulation schemes. Though it can recognize RS code parameters effectively after modulation, the SNR needed in the algorithm is quite high. A novel code parameter recognition technique based on the average log-likelihood ratio (LLR) of syndrome a posteriori probability (SPP) was proposed for RS codes in [11]. It is with low computational complexity, but the identification performance of the algorithm needs to be improved. Wang [12] proposed a fast RS codes recognition algorithm based on primitive element search and probability statistics. It has low complexity and relatively high recognition rate. However, when the bit-error-rate (BER) of the same codewords increases, the performance decreases sharply.

Through the description of the algorithms proposed in previous references, we find that there are still some problems in the parameter identification of RS codes. The main problem is that the existing algorithms require relatively low BER or high SNR, resulting in recognition failure under severe channel conditions. In addition, the theoretical derivation about the upper bound on correct recognition rate of algorithms hasn't been studied.

On the basis of [12], an improved algorithm of the blind recognition of RS codes based on probability statistics and GFFT (PS-GFFT) is proposed in this paper to solve the first problem mentioned above. A threshold obtained by probability statistics is used to skip wrong parameters with a high probability and conduct the next search in a candidate set. When there are not enough received codewords or when wrong code parameters pass the threshold, GFFT is applied to reduce the error identification probability and improve the correct parameter recognition rate of RS codes as much as possible. In addition, we give a thorough theoretical analysis and derive an upper bound on the correct recognition rate of RS codes. The upper Bound quantifies the influence of the number of received codeword, the bit error rate of the codewords, and the number of bits per symbol on the accuracy of parameters estimation. Numerous simulations show the recognition performance of the proposed PS-GFFT algorithm is able to outperform almost all the algorithms proposed by other researchers to the best of our knowledge. The contributions of the work are given as follows:

- In this paper, we propose an innovative algorithm based on probability statistics and GFFT for parameter identification of RS codes.
- A upper bound on the correct recognition rate of RS codes, which is of great importance in evaluating the performance of algorithms has been derived and proved in this paper.
- Numerous simulation results are presented for different cases by varying code length n, BER and SNR to validate the recognition performance and robustness of the proposed algorithm. Besides, the performance of the proposed PS-GFFT algorithm in terms of recognition accuracy and computational complexity is compared with plenty of references.

The remainder of the paper is organized as follows. Section II introduces GFFT and RS codes briefly. Details of the RS codes recognition algorithm and the derived upper bound are provided in Section III. Section IV presents some simulation results as well as complexity analysis, and conclusions are made in Section V.

II. PRELIMINARIES

A. GALOIS FIELD FOURIER TRANSFORM

Let $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ be a polynomial over Galois field $GF(q)$, where $q = 2^m$ and $n = q - 1$, m is the degree of the primitive polynomial for $GF(q)$. Let α denote the primitive element of $GF(q)$, which means that $\alpha^{q-1} = 1$ and α is a root of $x^n - 1$. Then, there comes the definition of Galois field Fourier transform (GFFT) of $c(x)$.

Definition 1: The Galois field Fourier transform of $c(x)$ is defined in [7]:

$$C(X) = C_0 + C_1X + \cdots + C_{n-1}X^{n-1}, \tag{1}$$

where for $0 \leqslant j < n$

$$C_j = c(\alpha^j) = \sum_{i=1}^{n-1} c_i\alpha^{ij}.$$

It is evident that the j-th spectral component C_j is zero if and only if α^j is a root of $c(x)$.

B. RS CODES AND THE RECOGNITION OF RS CODES

The parameters of t-error-correcting RS code with symbols from $GF(q)$, where $q = 2^m$ and $m \geqslant 3$, are given below [7]

- Codeword length $n = q - 1$;
- Number of parity check symbols $n - k = 2t$;
- Code dimension $k = q - 1 - 2t$;
- Minimum hamming distance $d_{min} = 2t + 1$.

From subsection II-A, we learned that α is the primitive element of $GF(q)$. Meanwhile, it is well-known that $\alpha, \alpha^2, \alpha^3, \cdots, \alpha^{2t}$ are the roots of the generator polynomial $g(x)$. Consequently, $g(x)$ can be described as

$$g(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^3)\cdots(x - \alpha^{2t}). \tag{2}$$

Considering parameter recognition of RS codes in AMC or non-cooperative communications, the primary question is to decide the type of parameters to be estimated. Since that RS code is determined by the primitive polynomial $p(x)$ of $GF(q)$, codeword length n, information dimension k and generator polynomial $g(x)$, the issues involved in the parameter recognition of RS codes include the identification of these four kinds of parameters.

III. RS CODES RECOGNITION ALGORITHM PS-GFFT

In this section, details of the algorithm based on probability statistics and Galois field Fourier transform are presented and the upper bound on correct recognition rate of RS codes is derived.

The parameters of RS codes to be recognized are primitive polynomial $p(x)$ of $GF(q)$, code length n, information dimension k and generator polynomial $g(x)$. The first step of the proposed algorithm is to identify $p(x)$ and n. Then, based on the recognition results of the first step, information length k and generator polynomial $g(x)$ will be identified.

A. RECOGNITION OF n AND p(x)

Before introducing PS-GFFT algorithm, several fundamental theorems are presented as follows.

Theorem 1: If α is the primitive element of $GF(2^m)$, then the probability that any random segment of length n (n symbols that means $n * m$ bits) takes α as a root is $1/2^m$ [12].

The following part of the paper will extend this theorem and prove it strictly in the **Appendix**.

Theorem 2: If α is the primitive element of $GF(2^m)$, then the probability that any random segment of length n (n symbols means $n * m$ bits) takes α^j (j is a positive integer) as a root is $1/2^m$.

What attracts us is whether an event that a random segment takes α^j as root have anything to do with the other event that the random segment takes any other roots like α^k. Hence, we propose **Theorem 3** as follows.

Theorem 3: For any random segment of length n (n symbols means $n * m$ bits) takes α^j (j is a positive integer) as a root and takes α^k (k is another positive integer) as a root is independent.

There is an undeniable fact that $\alpha, \alpha^2, \alpha^3, \cdots, \alpha^{2t}$ are the roots of the generator polynomial of RS codes. As a result, an RS codeword takes α^i $(0 < i \leqslant 2t)$ as a root. However, since the codewords are transmitted through a noisy channel, an erroneous code is likely to occur. We want to figure out the probability that the erroneous RS codeword takes α^i as a root. **Theorem 4** demonstrates that once a codeword changes any bits in the channel, there is no difference between it and a random segment in this aspect of our discussion. This is vividly presented in Fig. 2.

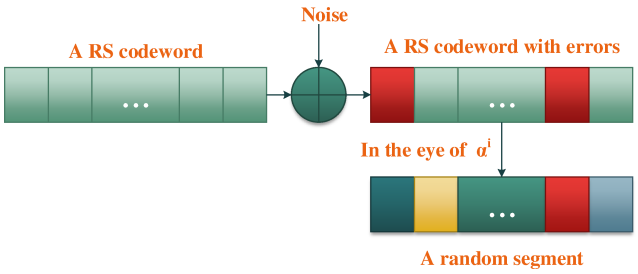


FIGURE 2. The view of α^i on the erroneous RS codeword.

Theorem 4: For an (n, k) RS codeword, if it gets p $(1 \leqslant p \leqslant n$ symbols) errors in a noisy channel, the probability that it takes α^i as a root is $1/2^m$.

The blind parameter recognition of RS codes is within a candidate set including different Galois fields ($GF(2^m)$ from $m = 3$ to $m = 8$) and corresponding primitive polynomials. A correct RS codeword is certain to take the primitive element α and α^2 as roots since α and α^2 are the roots of $g(x)$. However, the probability of a random segment or an erroneous codeword takes α and α^2 as roots is $1/2^{2m}$ according to **Theorem 2**, **3** and **4**. In consequence, the difference between the two events mentioned above can be used to find the correct coding parameters of block length n and the primitive polynomial $p(x)$ from the candidate set.

We start with the first primitive polynomial $(x^3 + x + 1)$ in the first Galois field $(m = 3)$. When the Galois field we are searching for is not the correct Galois field in the RS

encoder, the bitstream will be wrongly reshaped into multiple segments for every $n * m$ ($n = 2^m - 1$) bits. Besides, the primitive element α will change if the primitive polynomial is incorrect. In these cases, every segment is treated as a random segment. Assuming that the number of received codewords is N_l, we begin to search for the codewords that take α and α^2 as roots, leaving the codewords which satisfy the condition. Let N_r denotes the number of codewords in reserve, then N_r follows a binomial distribution $B(N_w, p_1)$. N_w is the number of segments, and it equals to $\frac{N_l * 2^m * m}{(2^{m_n}) * m_n}$, where m is the parameter of real $GF(2^m)$ and m_n is in the Galois field $GF(2^{m_n})$ at present. p_1 is the probability that each of these segments takes α and α^2 as roots, and it equals to $1/2^{2m_n}$. Let us define the probability of leaving N_r codewords as $p(N_r)$, then $p(N_r)$ is given by

$$p(N_r) = \binom{N_w}{N_r} * p_1^{N_r} * (1 - p_1)^{N_w - N_r}. \tag{3}$$

According to the properties of mean and variance of binomial distribution, we can obtain

$$\begin{aligned} E(N_r) &= N_w * p_1 \\ D(N_r) &= N_w * p_1 * (1 - p_1). \end{aligned} \tag{4}$$

If both the Galois field and the primitive polynomial we are searching for are correct, the correct codewords at this time will definitely takes α and α^2 as roots. Consequently, considering the influence of the transmission in a noisy channel, the codewords that can pass the check of α and α^2 also obey the binomial distribution $B(N_l, p_2)$. p_2 is defined as the probability that each of these segments takes α and α^2 as roots. The calculation of the probability p_2 can be divided into two parts. One part is the codewords without error, which definitely take α and α^2 as roots. The other part is erroneous codewords (bit-error-rate denotes as P_e). According to **Theorem 4**, the probability that erroneous codewords take α and α^2 as roots is $1/2^{2m}$. Thus, the parameters of the binomial distribution can be written as

$$p_2 = (1 - P_e)^{(2^m - 1) * m} + (1 - (1 - P_e)^{(2^m - 1) * m})/2^{2m} \tag{5}$$

$$\begin{aligned} p(N_r) &= \binom{N_l}{N_r} * p_2^{N_r} * (1 - p_2)^{N_l - N_r} \\ E(N_r) &= N_l * p_2 \\ D(N_r) &= N_l * p_2 * (1 - p_2). \end{aligned} \tag{6}$$

As is shown in Fig. 3, the difference of the distributions between the random segments and erroneous RS codewords can be used to set a threshold to recognize code parameters.

Considering the complexity of the binomial distribution, a simplified algorithm based on probability statistic will be proposed. According to [18], if x obeys binomial distribution $B(n, p)$, when n is large enough ($n * p \geqslant 5$), the binomial distribution approximates normal distribution, which can be expressed as

$$\lim_{n \to +\infty} \frac{x - np}{\sqrt{n * p * (1 - p)}} \sim N(0, 1).$$

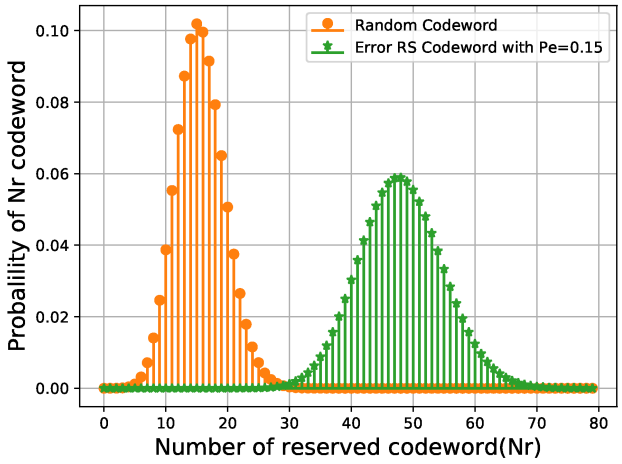


FIGURE 3. The comparison about passing α and α^2 test between random segment and error RS codeword when $N = 1000$, $m = 3$ and the bit-error-rate (P_e) is 0.15.

Accordingly, when N_w and N_l is large enough ($N_w * p_1 \geqslant 5$ *and* $N_l * p_2 \geqslant 5$), N_r obeys the normal distribution of different parameters in the two cases described above. When either the code length n or the primitive polynomial $p(x)$ by guess is wrong, the approximation can be written as

$$\lim_{N_w \to +\infty} \frac{N_r - N_w * p_1}{\sqrt{N_w * p_1 * (1 - p_1)}} \sim N(0, 1). \tag{7}$$

When both the guesses of n and $p(x)$ are right, we obtain

$$\lim_{N_l \to +\infty} \frac{N_r - N_l * p_2}{\sqrt{N_l * p_2 * (1 - p_2)}} \sim N(0, 1). \tag{8}$$

When we start approximating the binomial distribution in Fig. 3 with the normal distribution, a close result is obtained as shown in the Fig. 4.

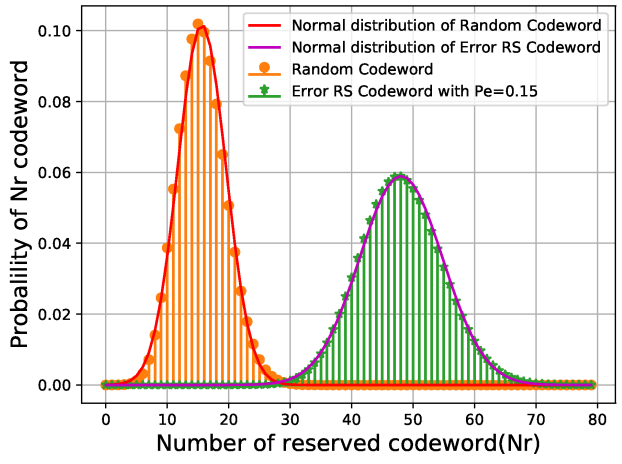


FIGURE 4. The Normal distribution approximation to the Binomial distribution when $N = 1000$, $m = 3$ and $p1$, $p2$ is calculated by Equations (3) and (5).

Due to the difference between Equations (7) and (8), we can set a threshold in order to skip the wrong parameters

in the candidate set with a high probability and conduct the next search when the code length n and primitive polynomial $p(x)$ searched are wrong. However, it should be noted that the bit-error-rate could not be easily obtained in advance during the actual transmission process. Thus, P_e and p_2 shouldn't be used in the algorithm. The probability of excluding random segments' interference is set as P_r, and the required threshold value is denoted as N_{th}. Then the probability P_r is calculated by

$$\begin{aligned} P_r &= P(N_r < N_{th}) = 1 - P(N_r \geqslant N_{th}) \\ &= 1 - Q(\frac{N_{th} - E(N_r)}{\sqrt{D(N_r)}}) \\ &= 1 - Q(\frac{N_{th} - N_w * p_1}{\sqrt{N_w * p_1 * (1 - p_1)}}), \end{aligned} \tag{9}$$

where $Q(x)$ is the Q-function, defined as $Q(x) = (1/\sqrt{2\pi}) * \int_x^{\infty} \exp(-t^2/2)dt$. Then the required threshold N_{th} is given by

$$N_{th} = N_w * p_1 + t_{P_r} * \sqrt{N_w * p_1 * (1 - p_1)}, \tag{10}$$

where t_{P_r} depends on $1 - P_r$ in the table of Q-function values [18].

When $n * p < 5$, it is not appropriate to estimate binomial distribution by normal distribution. Otherwise, it will lead to inaccurate threshold estimation, resulting in wrong code parameters passing the threshold. Therefore, Galois field Fourier transform is used to reduce parameter identification errors. According to the Equation (2), $\alpha \sim \alpha^{2t}$ are roots of the codewords. When there is an error-free codeword after transmission in a noisy channel, $2t$ continuous zero spectrums exist in its GFFT spectrums [17]. In order to reduce the number of GFFT calculations (denotes as N_{gn}), the number of codewords required for GFFT computation is preset to N_g, which means the smaller one between N_g and N_r was taken, i.e., $N_{gn} = min(N_r, N_g)$. N_r follows a binomial distribution $B(N_w, p_1)$. The probability that N_r is greater than N_g is given by

$$P(N_r > N_g) = \sum_{i=N_g+1}^{N_w} \binom{N_w}{i} * p_1^i * (1 - p_1)^{N_w - i}. \tag{11}$$

Let us take $N_w = 1280$, $m = 4$ as an example, and thus $p_1 = 1/2^{2*4}$, $N_w * p_1 = 5$. Using mathematical tools to solve the Equation (11), we get a satisfying result when N_g is equal to 10, the probability of $N_r > N_g$ is only 1.35%, which is represented in the Fig. 5. A bunch of other N_w and m are computed under different condition of $N_w * p_1$, which is shown in the Table 1. We find that when $N_w * p_1 < 5$, the probability of $N_r > 10$ is pretty small (less than 1.37%). This indicates the probability of $N_{gn} = min(N_r, N_g) = N_r$ is more than 98.63% and the probability of excluding random segments' interference is more than 98.63%. Therefore, we believe that when N_g is equal to 10, there is a good balance between the reliability of the algorithm and the computational complexity of GFFT calculation. It should be noted that N_g can take other values and we preset N_g to 10 in our simulation.

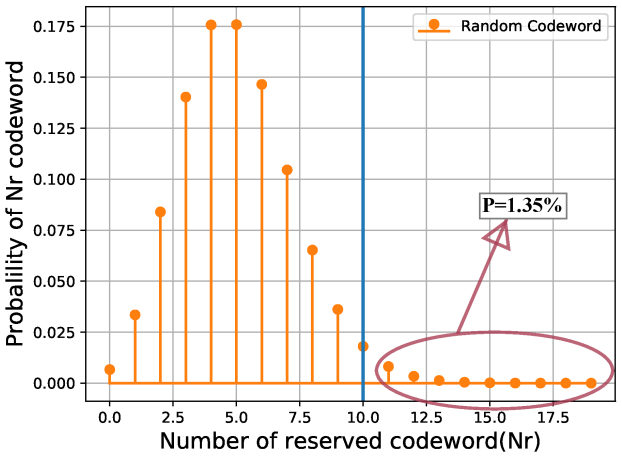


FIGURE 5. A sketch about probability of $N_r > N_g$ when $N_w = 1280$, $m = 4$ and $N_g = 10$.

TABLE 1. The probability of $N_r > N_g$ under different condition of $N_w * p_1$ and m when $N_g = 10$.

$P(N_r > N_g)$ m / $N_w * p_1$	3	4	5	6	7	8
3	0.00025	0.00028	0.00029	0.00029	0.00029	0.00029
4	0.00260	0.00280	0.00280	0.00280	0.00280	0.00280
5	0.01300	0.01350	0.01370	0.01370	0.01370	0.01370

After applying GFFT calculation to N_{gn} codewords, the even number of continuous zeros is placed in a matrix N_z. It is evident that all the N_{gn} codewords take roots of α and α^2, resulting in two consecutive zeros spectrums. However, 1-error-correcting RS codes are rarely used in the practical application and the codeword length n is mostly short, like RS(7,5) code which can be recognized correctly under high BER (0.2). Therefore, it is reasonable to increase BER required for correct recognition of t-error-correcting ($t > 1$) RS codes by reducing that of RS codes whose error correction capability is 1. To be specific, the parameters of 1-error-correcting RS codes can be identified correctly when $N_{gn} = N_g$ and all the entries in the matrix N_z is equal to 2. For t-error-correcting ($t > 1$) RS codes, correct recognition only requires the existence of an error-free codeword. Accordingly, the following two methods are adopted in PS-GFFT algorithm. Firstly, the guesses of n and $p(x)$ are abandoned when $N_{gn} < N_g$ and all the entries in the matrix N_z is equal to 2 in order to excluding random segments' interference. Secondly, 2 is excluded in N_z when not all the entries in the matrix N_z is equal to 2 for improving the correct parameter recognition rate of t-error-correcting ($t > 1$) RS codes.

B. RECOGNITION OF k AND g(x)

If there is a non-erroneous codeword, its GFFT spectrums must exist $2t$ continuous zero spectrums. All we need is to

find the correct codeword in order to identify the number of parity check symbols $2t$ and the code dimension k correctly.

Firstly, the mode of the continuous zero numbers is used to find the number of parity check symbols $(2t)$, i.e., $2t = mode(N_z)$. Secondly, the code dimension k is calculated by $k = n - 2t$. Thirdly, the generator polynomial $g(x)$ can be obtained according to the Equation (2).

The detailed steps for recognizing the Reed-Solomon codes parameters are given in **Algorithm 1**. Furthermore, in order to give readers a vivid impression of the process of the algorithm, we draw a flowchart about the specific procedure, which is shown in Fig. 6.

Algorithm 1 Parameter Identification of RS Codes Based on PS-GFFT

Input: the bitstream to be identified
Output: RS codes parameters $(n, k, p(x), g(x))$

Initialize: $m_{min} = 3$; $m_{max} = 8$; $N_g = 10$
for $m = m_{min} : m_{max}$ **do**
  $p = p_{min} = primpoly(m,' min')$
  $p_{max} = primpoly(m,' max')$
  Calculate N_{th} by Equation (10)
  while $p \leqslant p_{max}$ **do**
    Reshape the bitstream into h parts by $n = 2^m - 1$
    Get α by using primitive polynomial p
    Keep codewords with roots of α and α^2 in every segment among h parts and calculate the number of reserved codeword N_r
    if $N_r < N_{th}$ **then**
      Take the next primitive polynomial p and turn to label 6
    else
      $N_{gn} = min(N_r, N_g)$
      Apply GFFT calculation to N_{gn} codewords, find out the number of continuous zero spectrums and put **even numbers** among them into the matrix N_z
    end
    if *All of the entries in matrix* N_z *are* 2 **then**
      if $N_{gn} < N_g$ **then**
        Take next primitive polynomial p and turn to label 6
      else
        Turn to label 24
      end
    else
      Excluding 2 in N_z
      $n = 2^m - 1$
      $n - k = mode(N_z)$
      $p(x) = de2bi(p)$
      Use Equation (2) to find $g(x)$
    end
  end
end

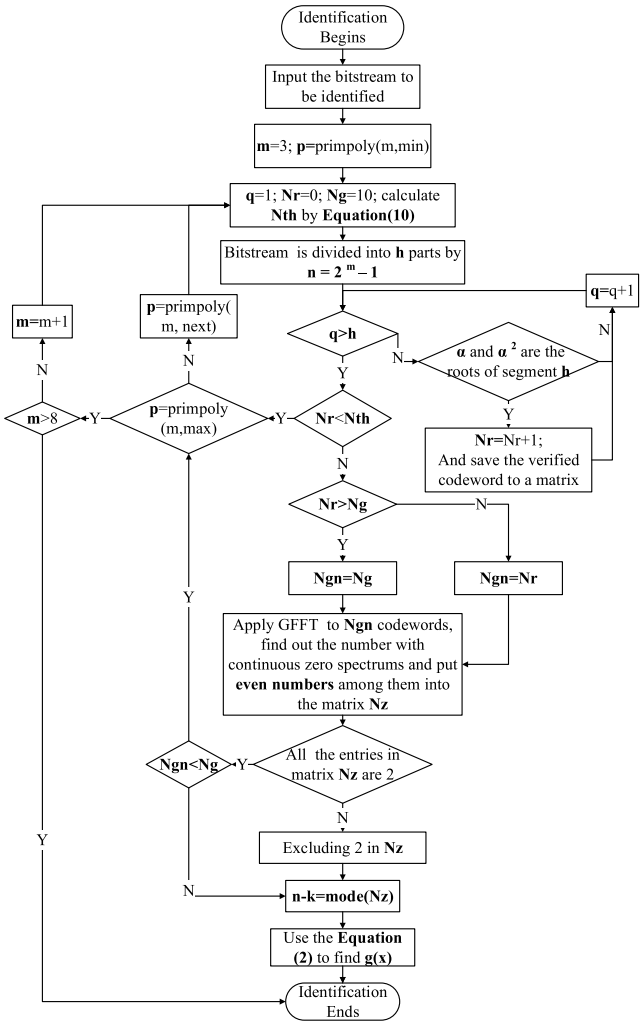


FIGURE 6. A detailed flowchart showing PS-GFFT algorithm.

C. THE UPPER BOUND ON CORRECT RECOGNITION RATE

It can be seen from the **Theorem 2** and **Theorem 4** that when a correct RS codeword passes through a noisy channel and produces an erroneous codeword, there is no difference between it and a random segment in terms of primitive α as its root. Whereas, one of the tasks of RS code parameter identification is to recognize the generator polynomial $g(x)$ that takes primitive α as a root. Accordingly, proper reconstruction of $g(x)$ requires an error-free codeword.

Considering a scenario that the code sequence to be recognized is obtained by means of hard decision (the values in the bitstream is bit 1 or bit 0), at least one correct RS codeword is needed to recognize RS code parameters. RS code is a kind of non-binary code. For example, the RS code (255, 223) actually has $255 * 8$ bits. Based on the description mentioned above, we present the following theorem about the upper bound of RS codes recognition and then prove it in the Appendix.

Theorem 5: For RS codes whose symbols are taken from $GF(2^m)$*, if the number of codewords with bit-error-rate* (P_e)

is N_l, the maximum recognition probability (P_r) of the RS codes is:

$$P_r = 1 - (1 - (1 - P_e)^{(2^m-1)*m})^{N_l} \quad (12)$$

Since the bit-error-rate (P_e) of the codeword is determined by the modulation and channel noise, i.e., signal-to-noise-ratio (SNR), we can derive the P_r under certain SNR and modulation type. Taking MQAM modulation for example, the relationship between the symbol-error-rate and SNR under ML demodulation is given by

$$P_s = 1 - (1 - (1 - \frac{1}{\sqrt{M}})erfc(\sqrt{\frac{3SNR}{2(M-1)}}))^2. \quad (13)$$

In general, the bit-error-rate can be expressed as

$$P_e = P_s/\log_2 M. \quad (14)$$

Then, the upper bound of recognition accuracy can also be obtained under different SNR conditions adopting MQAM modulation schemes.

IV. SIMULATION RESULTS AND ANALYSIS

In this section, we provide some simulation results for the performance of our proposed PS-GFFT algorithm. Firstly, RS(7,5) code and RS(31,15) code are used as examples to be identified by using PS-GFFT algorithm. Then, we simulate the presented upper bound with different values of m and the number of received codewords N_l. After that, we compare the correct recognition rate of our proposed PS-GFFT algorithm with the derived upper bound under the different bit-error-rate. Finally, we compare the recognition accuracy and computational complexity of PS-GFFT with other conventional algorithms under different values of SNR by setting 16QAM modulation over AWGN channel.

A. SIMULATION EXAMPLES OF OUR ALGORITHM

In this subsection, RS(7,5) code with primitive polynomial $p = 13$, which is the decimal representation of $p(x) = x^3 + x^2 + 1$ and RS(31,15) code with primitive polynomial $p = 41$, which is the decimal representation of $p(x) = x^5 + x^3 + 1$, are used as examples to be recognized. We suppose the frame synchronization is already realized before we take code recognition. If not, we need to shift the received data stream by ϕ ($0 \leqslant \phi < m*(2^m-1)$) bits to achieve frame synchronization, i.e., add (**for** $\phi = 0 : m*(2^m-1)-1$ **do**) and (shift the bitstream by ϕ bits) after label 6 in the **Algorithm** 1.

We set the number of received codewords (N_l) as 1000 and the number of codewords required for GFFT computation (N_g) is preset to 10. And the bit-error-rate of the codewords (P_e) is set as 0.2 for RS(7, 5) code and 0.04 for RS(31, 15) code. According to the process of our algorithm, the code length n and the primitive polynomial $p(x)$ will be recognized in the first place. Let us take $m = 3$, $p(x) = x^3 + x + 1$, which is the first primitive polynomial over $GF(2^3)$. The value of P_r is taken as 90%, and thus t_{P_r} is 1.29. Table 2 presents the difference between N_r and N_{th} for different p in the identification process of RS(7,5) code while Table 3 displays the gap between N_r and N_{th} for different m and p in the simulation process of RS(31,15) code recognition. Besides, Fig. 7 displays the details in the simulation process of RS(7,5) code recognition while the specific identification process for RS(31,15) code is shown in Fig. 8.

TABLE 2. The comparison between N_r and N_{th} for different p in the simulation process of RS(7,5) code recognition.

m	3	
p	11	13
N_r	18	32
N_{th}	20.7	

TABLE 3. The comparison between N_r and N_{th} for different m and p in the simulation process of RS(31,15) code recognition.

m	3		4		5	
p	11	13	19	25	37	41
N_r	108	113	13	9	3	6
N_{th}	129.15		14.21		2.3	

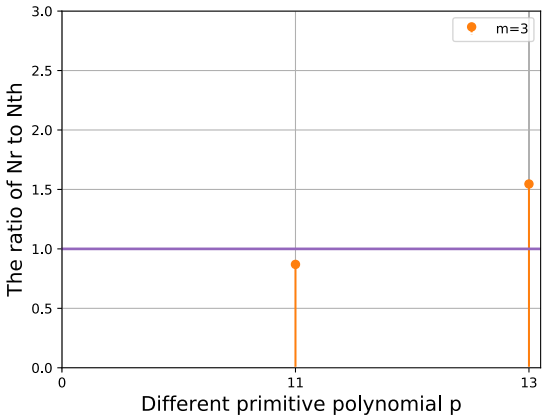


FIGURE 7. The process of comparing the number of reserved codewords N_r and N_{th} for RS(7, 5) code recognition.

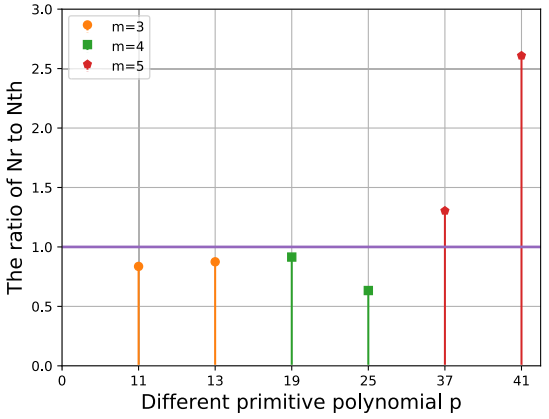


FIGURE 8. The process of comparing the number of reserved codewords N_r and N_{th} for RS(31, 15) code recognition.

In the identification process of RS(7,5) code, the primitive polynomials (11) in decimal was blocked by the threshold because N_r (18) is smaller than N_{th} (20.7). According to labels 10 and 11 in **Algorithm 1**, the algorithm begins with the verification of the next primitive polynomial (13). At this time, N_r (32) is bigger than N_{th} (20.7) and thus $N_{gn} = min(N_r, N_g) = min(32, 10) = 10$ codewords are taken for GFFT calculation. And this example reflects the role of N_g in reducing the computational complexity of GFFT calculation. After taking GFFT calculation, the even numbers (2, 2, 2, 2, 2, 2, 2, 2, 2, 2) of continuous zeros spectrums are put into a matrix N_z. Due to the reason that all the entries in matrix N_z are 2 and $N_{gn} = N_g = 10$, labels 16, 17, 20 and 24 in **Algorithm 1** will be executed. Then $n-k$ is estimated from the mode operation in matrix N_z by $n - k = mode(N_z)$ and the code parameters are correctly identified as

- Codeword length $n = 7$;
- Primitive polynomial $p = 13$, $p(x) = x^3 + x^2 + 1$;
- Information dimension $k = 5$;
- Generator polynomial $g(x) = x^2 + 6x + 5$.

When it comes to the simulation process of RS(31,15) code recognition, it is clearly demonstrated in the Fig. 8 that all the primitive polynomials (11, 13, 19, 25) in decimal was blocked by the threshold when $m = 3$ and $m = 4$. However, the random segment passed the threshold when $m = 5$, $p = 37$. The number of the reserved codewords is three ($N_r = 3$), and thus $N_{gn} = min(N_r, N_g) = min(3, 10) = 3$ codewords are taken for GFFT calculation. Each of the three codewords has two consecutive zero spectrums. According to labels 17 and 18 in **Algorithm 1**, the guesses of n and $p(x)$ need to be discarded because N_{gn} is less than N_g (10). Consequently, the algorithm begins with the verification of the next primitive polynomial (41). And this example reflects the advantage of GFFT in avoiding wrong estimated parameters in the PS-GFFT algorithm. When $p = 41$, the threshold is passed because N_r (6) is bigger than N_{th} (2.3). After taking GFFT calculation, the even number (2, 2, 16, 16, 16) of continuous zeros spectrums (2, 2, 3, 16, 16, 16) is put into a matrix N_z including three correct codewords. According to labels 16 and 22 in **Algorithm 1**, the mode in the matrix is used to identify k by $n - k = mode(N_z)$ after excluding 2 in N_z and the code parameters are correctly identified as

- Codeword length $n = 31$;
- Primitive polynomial $p = 41$, $p(x) = x^5 + x^3 + 1$;
- Information dimension $k = 15$;
- Generator polynomial $g(x) = x^{16} + 17x^{15} + 23x^{14} + 31x^{13} + 10x^{12} + 31x^{11} + 26x^{10} + 9x^9 + 25x^8 + 7x^7 + 15x^6 + 29x^5 + 16x^4 + 30x^3 + 20x^2 + 31x + 30$.

B. THE UPPER BOUND SIMULATION

In this subsection, we simulate the upper bound $P_r = 1 - (1 - (1 - P_e)^{(2^m-1)*m})^{N_l})$ in our proposed **Theorem 5**. The formula quantifies the influence of the number of received codeword (N_l), the bit error rate of the codewords (P_e), and the number of bits per symbol (m) on the accuracy of parameters estimation (P_r).

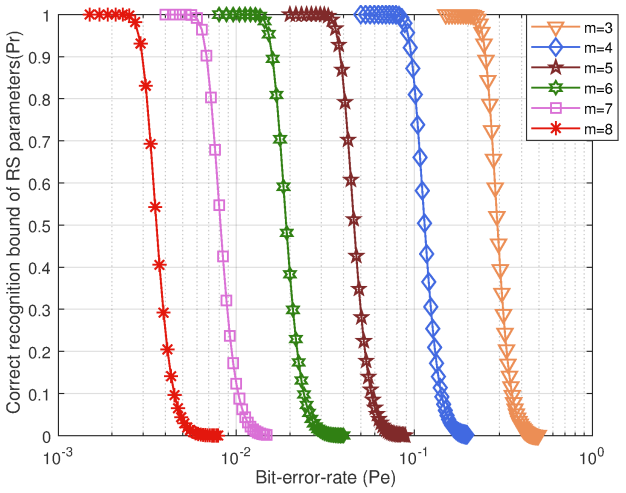


FIGURE 9. Accuracy upper bound of RS codes estimation from $m = 3$ to $m = 8$ with the variation of bit-error-rate (P_e) When $N_l = 1000$.

In Fig.9, we simulate the accuracy upper bound of RS codes recognition under different coding parameters from $m = 3$ to $m = 8$ when the received codeword's length N_l is 1000. As can be seen from the figure, the accuracy upper bound of codeword recognition is lower as bit-error-rate rises. Besides, through the comparison of different curves, it is found that the recognition bound decreases with the growth of the codeword length n under the same bit-error-rate.

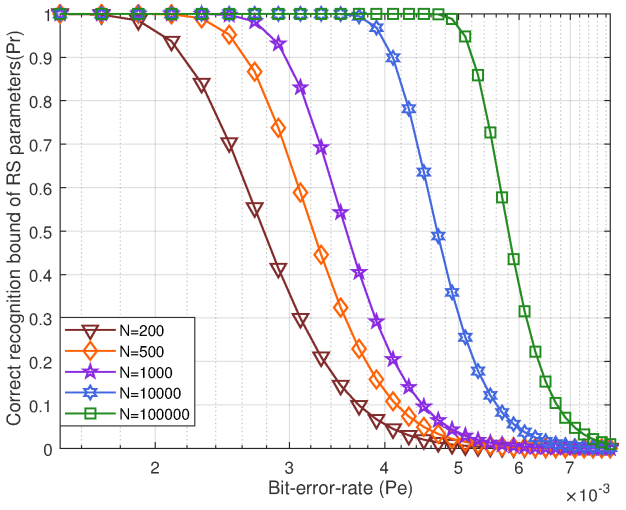


FIGURE 10. Accuracy upper bound of RS codes estimation over $GF(2^8)$ with the variation of bit-error-rate (P_e) When $N_l = 200, 500, 1000, 10000, 100000$.

Then in Fig. 10, we change the number of the received codeword, which is encoded over $GF(2^8)$, and set it for 200, 500, 1000, 10000, 100000, respectively. It is obvious that the correct recognition bound increases with the number of codewords received. Theoretically, as long as the number of received codewords increases, the upper bound on correct recognition rate can reach a relatively high probability at

a certain bit-error-rate. This illustrates that increasing the number of received codewords can improve the recognition accuracy under severe channel conditions. However, the computational complexity is also increased as the growth of N_l.

C. PERFORMANCE COMPARISON

In order to use the accuracy upper bound to evaluate the performance of our algorithm, errors are added directly to the RS codes with different bit-error-rate. The performance of PS-GFFT algorithm is evaluated by Monte Carlo simulations in terms of the correct identification probability. The number of received codewords N_l is taken as 1000. RS(7,3), RS(15,9), RS(31,15), RS(63,57), RS(127,111), RS(255,223) are adopted here because they are commonly used in data storage as well as deep-space communications.

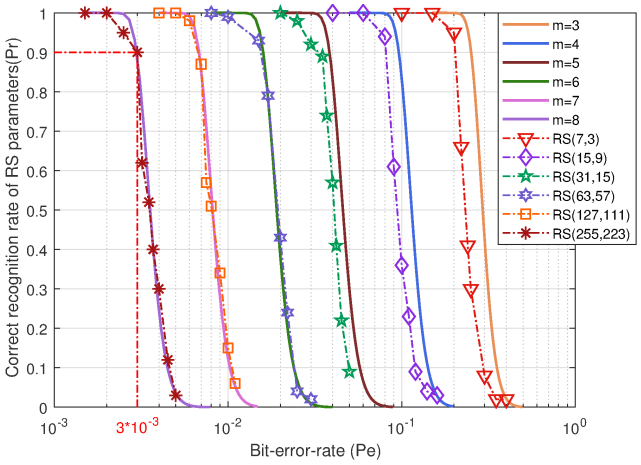


FIGURE 11. Performance comparison of the proposed PS-GFFT algorithm and the upper bound.

The correct recognition rate versus the upper bound with the bit-error-rate of RS codewords is illustrated in Fig. 11. The results indicate that the proposed algorithm is close to the upper bound when the code length is larger than 2^6–1 ($m \geqslant 6$) and the correct recognition probability of RS codewords whose length is no more than 255 will be over 90% when the error rate is below $3 * 10^{-3}$. In the case of short code length, there is a little gap between our algorithm and the upper bound. The explanation is that $p_1 = 1/2^{2m}$ will be larger when the code length is shorter, i.e., m gets smaller. It will lead to more wrong codewords taking the primitive element α as a root and then affect the recognition performance of the algorithm.

The performance comparison about RS(255,223) between our algorithm and the algorithms proposed in articles [12] and [17] is shown in Fig. 12. It is obvious that the performance of our PS-GFFT algorithm is much better than that of [12] based on primitive element check and [17] based on GFFT. Specifically, the algorithm proposed in [12] works with 90% and 10% accuracy when $P_e = 2 * 10^{-3}$ and $P_e = 2.8 * 10^{-3}$, respectively. Besides, the other algorithm proposed [17] operates with 90% and 3% accuracy for when

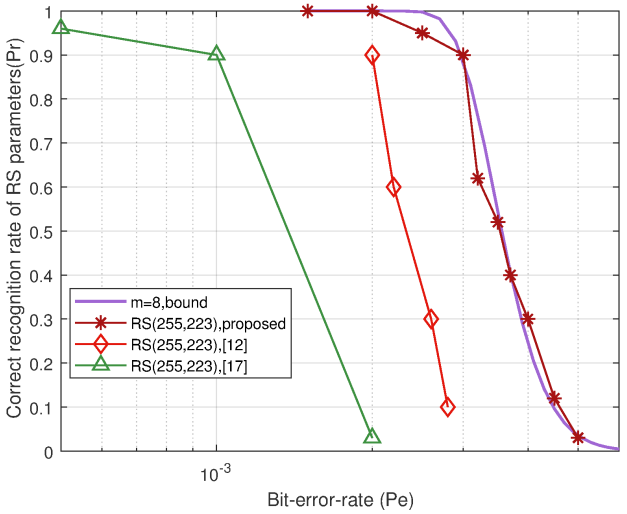


FIGURE 12. Performance comparison about RS(255,223) of the proposed algorithm and the algorithms proposed in [12] and [17].

$P_e = 10^{-3}$ and $P_e = 2 * 10^{-3}$. However, our algorithm can achieve 90% accuracy for $P_e \leqslant 3 * 10^{-3}$.

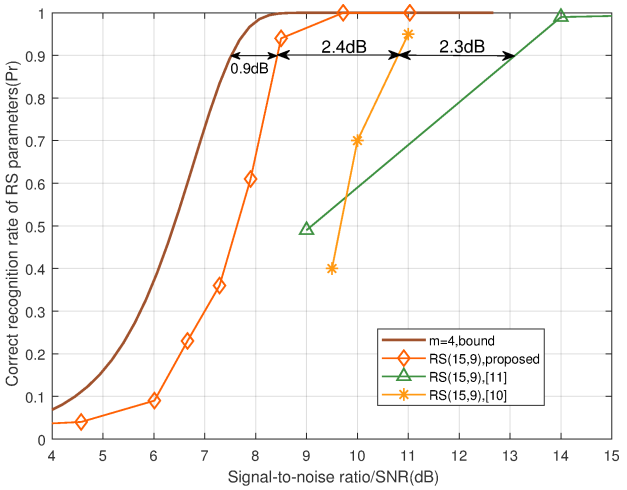


FIGURE 13. Performance comparison about RS(15,9) of the proposed algorithm and the algorithms proposed in [10] and [11].

Fig. 13 shows the performance comparison about RS(15,9) between proposed method and the algorithms in [10] and [11]. The codewords are modulated by 16QAM (adopted in both [10] and [11]). Then, the modulated signal is transmitted through an additive white Gaussian noise channel with different SNR. From the performance curves, it is evident that the proposed PS-GFFT algorithm outperforms the algorithm based on rank deficiency and normalized non-zero-mean-ratio values in [10] and the LLR-based methodology in [11]. To be more specific, the algorithm proposed in [10] operates with 40% and 95% accuracy for when SNR equals 9.5dB and 11dB. Additionally, the correct recognition rate of the other algorithm proposed in [11] achieves 50% and 99% when SNR equals 9dB and 14dB, respectively. Nevertheless, our algorithm can identify RS(15,9) with over 90% accuracy

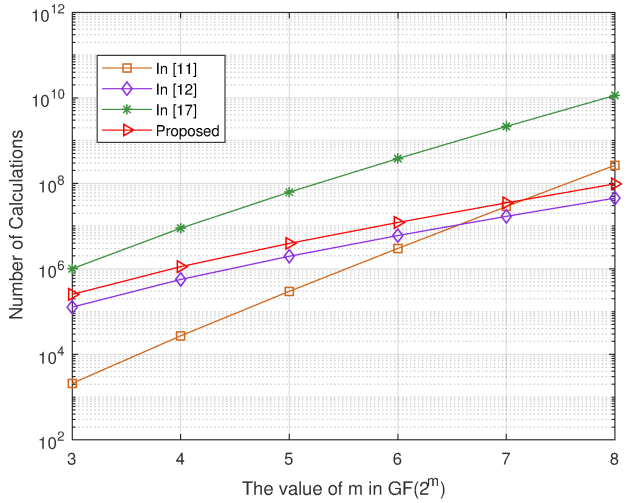


FIGURE 14. Comparison about computational complexity of the proposed GFFT algorithm and the algorithms proposed in [11], [12], and [17].

when SNR is larger than 8.42dB, which is only 0.9dB away from the accuracy upper bound and there is a gain of 2.4dB over reference [10] and 4.7dB over reference [11].

D. COMPLEXITY ANALYSIS

In this part, the computational complexity of proposed PS-GFFT algorithm is compared with that of [10]–[12] and [17]. The complexity of our algorithm is introduced as follows. It requires $n-1$ times multiplications and additions over $GF(2^m)$ to verify whether an element is the root of the codeword polynomial. The computational complexity is $(n-1)*(3m(m-1)+m)$ additions over $GF(2)$. Besides, a codeword for the complexity of the GFFT calculation needs n^2 multiplications and $n(n-1)$ additions over $GF(2^m)$, resulting $n^2*(3m(m-1))+n(n-1)*m$ additions over $GF(2)$. A primitive polynomial search procedure in PS-GFFT needs to verify whether α and α^2 are the roots of N_l codeword polynomials. Furthermore, there is a 10% chance when $np \leqslant 5$ codeword is used for GFFT because the threshold value is 90% in our simulation. Meanwhile, ten times GFFT is required when the real primitive is encountered ($p = 1/50$, 50 primitive polynomials from $m = 3$ to $m = 8$). Therefore, the complexity of our algorithm is written as $N_l*2*(n-1)*(3m(m-1)+m)+(0.1*5+1/50*10)*n^2*(3m(m-1))+n(n-1)*m$. When N_l is large enough like 1000, the complexity of GFFT in our algorithm is far less than the complexity of verifying a root. Consequently, the rough complexity of the proposed method is $\mathcal{O}(m^2n)$.

Then, the complexity in other articles is presented. Finite-field Gauss elimination process is adopted in [10] with approximate complexity as $\mathcal{O}(\frac{rank(G)^3}{mk}) = \mathcal{O}(\frac{m^3n^3}{mk})$, i.e., $\mathcal{O}(m^2n^2)$ roughly. In [11], the LLR-based methodology is used to search for a posteriori probabilities of a certain check with the complexity of $2*(q-1)^3$ real-valued additions over $GF(q)$. As a result, $2*n^3*m$ additions is needed over $GF(2)$, i.e., $\mathcal{O}(mn^3)$ roughly. Reference [12] verifies the primitive element and another element with the probability of 0.01. The computational complexity is $(N_l+N_l*0.01)*(n-1)*(3m(m-1)+m)$, i.e., $\mathcal{O}(m^2n)$ roughly. Liu *et al.* [17] carry out GFFT for all received codewords, with the complexity $N_l*n^2*(3m(m-1))+n(n-1)*m$, i.e., $\mathcal{O}(m^2n^2)$ roughly.

Comparison about specific computational complexity of the PS-GFFT algorithm and the algorithms proposed in [11], [12], and [17] is shown in Fig. 14 where $N_l = 1000$. The figure shows that the complexity of our algorithm is not as complicated as that of the algorithm proposed in [17]. Though it's a little more complicated than [12], the performance of our algorithm is much better. Since it takes much less time to identify short code length than long code length in the recognition process, we think it makes more sense to reduce complexity in long code length comparing with [11]. In short, the computational complexity of the proposed algorithm is acceptable by comparison.

V. CONCLUSIONS

In this paper, we proposed a PS-GFFT algorithm of the blind parameter recognition of RS codes and an upper bound of RS codes recognition accuracy is derived. Through numerous simulation experiments, it is observed that the proposed algorithm can approach the upper bound effectively, especially for long code length. Besides, the recognition performance of the proposed algorithm is much better than the algorithms proposed by others to the best of our knowledge while the complexity of our algorithm is acceptable. Specifically, the correct recognition probability of RS codewords whose length is no more than 255 can be over 90% when the codeword bit-error-rate is below $3*10^{-3}$, while the conventional algorithms have the best correct recognition probability of 10%. Conclusively, the PS-GFFT algorithm is particularly promising for the adaptive modulation and coding systems, cognitive radio technology and non-cooperative communication while the upper bound on correct recognition rate of RS codes is of great significance in evaluating recognition performance of algorithms.

APPENDIX

A. PROOF OF THEOREM 2

Proof of Theorem 2: Since α is the primitive element of Galois field $GF(2^m)$, all elements in $GF(2^m)$ are

$$(0, 1, \alpha, \alpha^2, \cdots, \alpha^{2^m-2}).$$

Any codeword $(c_0, c_1, \cdots, c_{2^m-2})$ whose length is n over $GF(2^m)$ can be written in the form of the polynomial as

$$c(x) = c_0 + c_1x + \cdots + c_{2^m-2}x^{2^m-2}. \tag{15}$$

If we substitute α^j in the polynomial (15), we can get

$$c(\alpha^j) = c_0 + c_1\alpha^j + \cdots + c_{2^m-2}\alpha^{j(2^m-2)}. \tag{16}$$

Every element in codeword vector $(c_0, c_1, \cdots, c_{2^m-2})$ is a random element (α^b) from $GF(2^m)$ and α^{ij} is also a random element in $GF(2^m)$. Let $p_i = c_i * \alpha^{ij} = \alpha^b * \alpha^{ij} = \alpha^{(b+ij)mod(2^m-1)}$, then p_i is a random element in $GF(2^m)$. Thus, Equation (16) can be restated as

$$c(\alpha^j) = p_0 + p_1 + \cdots + p_{2^m-2}, \tag{17}$$

where p_i is a random element in $GF(2^m)$. Thanks to the closure of set, $c(\alpha^j)$ is a random element in $GF(2^m)$, i.e., it obeys the uniform distribution in $(0, 1, \alpha, \alpha^2, \cdots, \alpha^{2^m-2})$. Therefore, the probability that $c(\alpha^j) = 0$ is $1/2^m$. □

B. PROOF OF THEOREM 3

Proof of Theorem 3: Let event A represent that the random segment takes α^j as root, and let event B denote that it is with root α^k. Event C means that the random segment takes roots of both α^j and α^k. Theorem 2 tells us that probability of A is equal to that of B, which can be written as

$$P(A) = P(B).$$

Let us substitute α^j and α^k in the polynomial (15) and do the derivation, then we get

$$c(\alpha^j) = p_0 + p_1 + \cdots + p_{2^m-2},$$

where $p_i = c_i * \alpha^{ij} = \alpha^b * \alpha^{ij} = \alpha^{(b+ij)mod(2^m-1)}$

$$c(\alpha^k) = q_0 + q_1 + \cdots + q_{2^m-2},$$

where $q_i = c_i * \alpha^{ik} = \alpha^b * \alpha^{ik} = \alpha^{(b+ik)mod(2^m-1)}$. Both p_i and q_i are random elements in $GF(2^m)$. Since α^j and α^k are given in advance, the probability of q_i under p_i can be written as $P(q_i|p_k) = P(q_i)$. Therefore, $c(\alpha^j)$ and $c(\alpha^k)$ are independent of each other, which can be denoted as

$$P(C) = P(c(\alpha^j) = 0) * P(c(\alpha^k) = 0) = P(A) * P(B).$$

□

C. PROOF OF THEOREM 4

Proof of Theorem 4: In (15), it is obvious that the codeword polynomial takes α^i $(0 < i \leqslant 2t)$ as a root, which can be expressed as

$$c(\alpha^i) = c_0 + c_1\alpha^i + \cdots + c_{2^m-2}\alpha^{i(2^m-2)} = 0. \quad (18)$$

Assuming that the error location is $k_1, \cdots, k_p$, the original codeword polynomial (15) can be written as

$$c(x) = c_0 + \cdots + c_{k_1}x^{k_1} + \cdots + c_{k_p}x^{k_p} + \cdots + c_{2^m-2}x^{2^m-2}. \quad (19)$$

Let us substitute α^i in (19), then we get

$$c(\alpha^i) = c_0 + \cdots + c_{k_1}\alpha^{ik_1} + \cdots + c_{k_p}\alpha^{ik_p} + \cdots + c_{2^m-2}\alpha^{i(2^m-2)}. \quad (20)$$

According to the addition property of the Galois field, when considering other values in (18) apart from the error location, the sum of them is equal to that of the original values in the error location (m_i, $1 \leqslant i \leqslant p$). Hence, the equation in (20) can be rewrited as

$$\begin{aligned} c(\alpha^i) &= c_0 + \cdots + c_{k_1}\alpha^{ik_1} + \cdots + c_{k_p}\alpha^{ik_p} + \cdots + c_{2^m-2}\alpha^{i(2^m-2)} \\ &= c_{k_1}\alpha^{ik_1} + \cdots + c_{k_p}\alpha^{ik_p} + \cdots + c_{m_1}\alpha^{ik_1} + \cdots + c_{m_p}\alpha^{ik_p} \\ &= (c_{k_1} + c_{m_1})\alpha^{ik_1} + \cdots + (c_{k_p} + c_{m_p})\alpha^{ik_p}. \end{aligned}$$

Since both c_{k_i} and c_{m_i} are random numbers from $GF(2^m)$ and can be denoted as α^j $(0 \leqslant j \leqslant 2^m - 2)$ or *zero*. Therefore, according to the closure property of the setïijŇ we get $c_{k_i} + c_{m_i} = \alpha^{q_i}$ and

$$\begin{aligned} c(\alpha^i) &= (c_{k_1} + c_{m_1})\alpha^{ik_1} + \cdots + (c_{k_p} + c_{m_p})\alpha^{ik_p} \\ &= \alpha^{q_1}\alpha^{ik_1} + \cdots + \alpha^{q_p}\alpha^{ik_p} \\ &= \alpha^l. \end{aligned} \quad (21)$$

From equation (21), we found that $c(\alpha^i)$ is a random number from $GF(2^m)$. As a result, the probability of $c(\alpha^i) = 0$ is $1/2^m$. □

D. PROOF OF THEOREM 5

Proof of Theorem 5: N_l RS codewords whose symbol is taken from $G(2^m)$ are transmitted in a noisy channel with bit-error-rate (P_e). Based on the knowledge of probability statistics, the probability of no error occurring in any bit of a codeword is

$$(1 - P_e)^{(2^m-1)*m}.$$

The probability of errors occurring in N_l codes is

$$(1 - (1 - P_e)^{(2^m-1)*m})^{N_l}.$$

Thus, the probability that at least one codeword is correct is

$$1 - (1 - (1 - P_e)^{(2^m-1)*m})^{N_l}.$$

When an algorithm is able to find the error-free codeword, RS code parameters can be recognized correctly. On the contrary, if the correct codeword is ignored or interfered by random segments, the real code parameters could not be identified and the recognition will fail. Hence, the maximum correct recognition probability (P_r) of the RS code is given by

$$P_r = 1 - (1 - (1 - P_e)^{(2^m-1)*m})^{N_l}.$$

□

REFERENCES

[1] G. Wu, B. Zhang, X. Wen, and D. Guo, "Blind recognition of BCH code based on Galois field Fourier transform," in *Proc. Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Oct. 2015, pp. 1–4.

[2] P. Yu, H. Peng, and J. Li, "On blind recognition of channel codes within a candidate set," *IEEE Commun. Lett.*, vol. 20, no. 4, pp. 736–739, Apr. 2016.

[3] R. Swaminathan and A. S. Madhukumar, "Classification of error correcting codes and estimation of interleaver parameters in a noisy transmission environment," *IEEE Trans. Broadcast.*, vol. 63, no. 3, pp. 463–478, Sep. 2017.

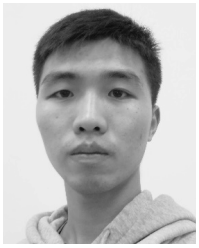
[4] S. Ramabadran, A. S. Madhukumar, W. Guohua, and T. S. Kee, "Blind recognition of LDPC code parameters over erroneous channel conditions," *IET Signal Process.*, vol. 13, no. 1, pp. 86–95, Feb. 2019.

[5] S. Ramabadran, A. S. Madhukumar, N. W. Teck, and C. M. S. See, "Parameter estimation of convolutional and helical interleavers in a noisy environment," *IEEE Access*, vol. 5, pp. 6151–6167, 2017.

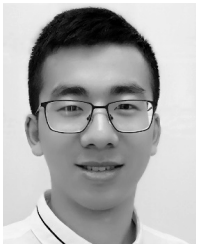
[6] Y. Zrelli, R. Gautier, E. Rannou, M. Marazin, and E. Radoi, "Blind identification of code word length for non-binary error-correcting codes in noisy transmission," *EURASIP J. Wireless Commun. Netw.*, vol. 43, no. 1, pp. 1–16, 2015.

[7] S. Lin and D. J. Costello, *Error Control Coding*, 2nd ed. Upper Saddle River, NJ, USA: Pearson Education, 2004.

[8] C. Li, T.-Q. Zhang, and Y. Liu, "Blind recognition of RS codes based on Galois field columns Gaussian elimination," in *Proc. 7th Int. Congr. Image Signal Process. (CISP)*, Oct. 2014, pp. 836–841.
[9] W. Li, J. Lei, L. Wen, and B. Chen, "An improved method of blind recognition of RS code based on matrix transformation," in *Proc. 15th IEEE Int. Conf. Commun. Technol. (ICCT)*, Nov. 2013, pp. 196–200.
[10] R. Swaminathan, A. S. MadhuKumar, W. Guohua, and T. S. Kee, "Parameter identification of Reed–Solomon codes over noisy environment," in *Proc. IEEE 86th Veh. Technol. Conf. (VTC-Fall)*, Sep. 2017, pp. 1–5.
[11] H. Zhang, H.-C. Wu, and H. Jiang, "Novel blind encoder identification of Reed–Solomon codes with low computational complexity," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2013, pp. 3294–3299.
[12] P. Wang, W. Zeng, and J. Chen, "Fast blind recognition algorithm for RS codes by primitive element," *J. Xidian Univ.*, vol. 40, no. 1, pp. 105–110, 2013.
[13] R. Moosavi and E. G. Larsson, "Fast blind recognition of channel codes," *IEEE Trans. Commun.*, vol. 62, no. 5, pp. 1393–1405, May 2014.
[14] A. Bonvard, S. Houcke, M. Marazin, and R. Gautier, "Order statistics on minimal Euclidean distance for blind linear block code identification," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–5.
[15] G. Wu, B. Zhang, D. Guo, and X. Liang, "Blind recognition of BCH codes in faster-than-Nyquist signalling system," *IET Electron. Lett.*, vol. 52, no. 9, pp. 716–718, Apr. 2016.
[16] V. Choqueuse, M. Marazin, L. Collin, K. C. Yao, and G. Burel, "Blind recognition of linear space–time block codes: A likelihood-based approach," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1290–1299, Mar. 2010.
[17] J. Liu, N. Xie, and X.-Y. Zhou, "Blind recognition method of RS coding," *J. Univ. Electron. Sci. Technol. China*, vol. 38, no. 3, pp. 363–367, 2009.
[18] R. V. Hogg and A. T. Craig, *Introduction to Mathematical Statistics*, 6th ed. Upper Saddle River, NJ, USA: Pearson Education, 2005.



PENGTAO LIU is currently pursuing the B.Sc. degree in communication engineering with the Department of Communication Engineering, School of Electronic Science, National University of Defense Technology (NUDT), Changsha, China. His research interests include channel coding and advanced wireless communication technology.



ZHIPENG PAN received the B.S. and M.S. degrees in information and communication engineering from the National University of Defense Technology (NUDT), Changsha, China, in 2014 and 2016, respectively, where he is currently pursuing the Ph.D. degree with the Department of Communication Engineering, School of Electronic Science. His research interests include advanced multiple access techniques, channel coding, and iterative decoding.

JING LEI received the B.Sc., M.Sc., and Ph.D. degrees from the National University of Defense Technology (NUDT), Changsha, China, in 1990, 1994, and 2009, respectively. She was a Visiting Scholar with the School of Electronics and Computer Science, University of Southampton, U.K. She is currently a Distinguished Professor with the Department of Communications Engineering, College of Electronic Science, NUDT, where she is also the Leader of the Communication Coding Group. She has published many papers in various journals and conference proceedings and five books. Her research interests include information theory, LDPC, space–time coding, advanced multiple access technology, physical layer security, and wireless communication technology.