Blind reconstruction of Reed-Solomon encoder and interleavers over noisy environment

Swaminathan, Ramabadran; Madhukumar, A. S.; Wang, Guohua; Ting, Shang Kee

2018

Swaminathan, R., Madhukumar, A. S., Wang, G., & Ting, S. K. (2018). Blind reconstruction of Reed-Solomon encoder and interleavers over noisy environment. IEEE Transactions on Broadcasting, 64(4), 830-845. doi:10.1109/TBC.2018.2795461

https://hdl.handle.net/10356/144731

https://doi.org/10.1109/TBC.2018.2795461

Blind Reconstruction of Reed-Solomon Encoder and Interleavers over Noisy Environment

Swaminathan R, A. S. Madhukumar, *Senior member, IEEE*, Guohua Wang, and Ting Shang Kee

***Abstract*—Blind estimation of code and interleaver parameters is useful in smart storage systems and ubiquitous communication applications such as adaptive modulation and coding, reconfigurable radio systems, non-cooperative radio systems, etc. In this paper, we analyze Reed-Solomon (RS) encoded data stream and propose blind estimation algorithms to identify RS code parameters. We also provide algorithms to estimate block interleaver parameters from RS coded and block interleaved data stream. In addition, synchronization compensation through appropriate bit/symbol positioning is integrated with the proposed code and interleaver parameter estimation algorithms. Simulation results validating the proposed algorithms are given for various test cases involving both erroneous and non-erroneous scenarios. Moreover, the accuracy of estimation of RS code and block interleaver parameters are also given with detailed inferences for different modulation schemes, codeword length, and code dimension values. It has been inferred that the accuracy of parameter estimation improves with decrease in code dimension and codeword length values of RS codes. Further, the accuracy of estimation of lower modulation order schemes is better when compared to higher modulation order schemes as expected. It has also been noted that the proposed code and interleaver parameter estimation algorithms for noisy environment consistently outperform the algorithms proposed in the prior works.**

***Index Terms*—Adaptive modulation and coding, blind reconstruction, block interleaver, data storage systems, non-cooperative systems, and Reed-Solomon (RS) codes**

I. Introduction

Forward error correcting (FEC) codes and interleavers are primarily used to counteract random and burst errors, respectively, in digital storage and communication systems. Blind reconstruction of code and interleaver parameters plays a vital role in non-cooperative scenarios [1] and [2], which exist particularly in military, spectrum surveillance, signals intelligence (SIGINT), and communications intelligence (COMINT) systems. Further, it will also provide additional advantages in applications such as adaptive modulation and coding, satellite communication systems, data storage systems, cognitive radio or reconfigurable receiver systems, etc. It is mandatory to reconstruct/estimate the FEC code parameters at the receiver in the case of non-cooperative systems. This is because, complete information about the code parameters used in the transmitter may not be available at the receiver. In the case of adaptive modulation and coding (AMC) systems, modulation and coding parameters are usually communicated to the receiver through control channel. Blind recognition of related parameters will lead to conservation of channel resources in such cases as mentioned in [3]-[5]. It is to be noted that wireless sensor networks (WSNs) also adopt AMC and the usage of blind parameter estimation algorithms help to reduce transmission overheads and total energy consumption of WSNs [3]. In most of the broadcast/communication applications, the code and interleaver parameters are known at the receiver. With the evolution of modern digital communication systems, designing separate decoding system for every broadcast/communication application is a costly and a tedious process. Therefore, it is essential to design an intelligent broadcast/communication receiver system which adapts itself to any specific broadcast/communication applications as suggested in [6] and [7]. In addition, it is also mandatory to blindly estimate the code and interleaver parameters for the intelligent receiver system or reconfigurable cognitive-radio-based broadcast/communication receiver system in order to adapt to the variations in the channel coding schemes for extracting the original data symbols [1]. Apart from the above applications, the parameter estimation techniques is also useful in the study of DNA sequences to identify possible error correcting codes in the genetic code [8] and [9].

Various methods for the blind estimation of coding and interleaver parameters are available in the recent literature. In [6]-[10], the blind recognition of convolutional code parameters was reported. In addition, interesting dual code properties were proposed in [11] for blind parameter estimation of convolutional codes. It is to be noted that the parameter estimation of convolutional codes was restricted to binary field (i.e. Galois Field GF(2)) in [6]-[11] and was extended to $GF(2^m)$ case in [12] assuming noiseless environment. The blind recognition of binary cyclic codes was carried out in [13]. In [14], the blind recognition algorithms were proposed for estimating punctured convolutional code parameters. In [15], an algebraic method for identification of puncturing pattern over noisy transmission was proposed. Recently, in [16], code classification algorithms were proposed to classify the incoming FEC coded symbols among block coded, convolutionally coded, and uncoded symbols. Further, in [17], the blind recognition of codeword length for various non-binary error correcting codes was extensively studied for noisy environment. In [18], the blind estimation of Reed-Solomon (RS) encoder was reported for noisy scenario. The algorithm in [18] was based on Barbier's dual code method [19]. The blind encoder identification technique based on the average log-likelihood ratio (LLR) of syndrome a posteriori probability

Swaminathan R & A.S.Madhukumar are with the School of Computer Science and Engineering, Nanyang Technological University, Singapore-639798, (e-mail: sramabadran@ntu.edu.sg, asmadhukumar@ntu.edu.sg).

Guohua Wang & Ting Shang Kee are with Temasek Laboratories, Nanyang Technological University, Singapore-639798, (e-mail: guowang@ntu.edu.sg, skting@ntu.edu.sg).

(SPP) was proposed for low-density parity-check (LDPC), RS, and convolutional codes in [3], [4], and [5], respectively.

Interleaver, which follows FEC encoder, plays a vital role in communication and storage systems to distribute the burst errors. In general, the systematic interleavers can be classified into block and convolutional interleavers. Algorithms for parameter estimation of block interleaver were proposed and analyzed in [19] and [20]. Here, the received data matrix is converted into row or column echelon form using Gauss-Jordan elimination through pivoting (GJETP) process [21]. The algorithm in [19] estimates the interleaver period based on the number of ones in row echelon form. The interleaver period along with the number of rows and columns of block interleaver matrix were estimated in [20] for convolutional encoded data based on the number of zeros in column echelon form. It is to be noted that the methodologies in [19] and [20] were valid only for binary coded data. The interleaver period estimation algorithm for block interleaver was extended to non-binary (RS coded) data in [22]. In [23]-[25], the algorithms for blind estimation of convolutional interleaver parameters were reported assuming linear block encoded, convolutional coded, and RS coded data symbols, respectively. However, the algorithms in [23] and [24] for noisy environment were restricted to binary field and the algorithm was restricted to noiseless environment in [25]. Finally, the code classification and code parameter estimation techniques for various FEC codes over non-erroneous scenario were studied in [1] with greater details.

RS codes, which is a special class of non-binary Bose-Chaudhuri-Hocquenghem (BCH) codes [26], are widely used in data storage, deep space, Digital video broadcasting (DVB), and satellite communication systems. Further, block interleavers play a vital role in error control systems compared to other interleavers. In this manuscript, we propose algorithms for estimating the parameters of block interleavers and associated RS codes. RS outer code followed by interleaver plays a vital role in concatenated codes, which are more prominently used in DVB-Terrestrial (DVB-T) systems [27] and compact disk (CD). Two levels of coding (i.e. inner and outer code) are usually applied to achieve desired error performance in case of serial concatenated codes. The input data is first encoded using outer code and then sent to interleaver. The interleaved data is further encoded using inner code. RS outer code followed by interleaver and convolutional inner code are widely used in applications such as space communication, DVB [27], and worldwide interoperability for microwave access (WiMAX) systems.

The following sections discuss the limitations of the existing approaches within the context of current research and major contributions of the proposed work.

A. Motivations

The main motivations behind the proposed work are given as follows:

- In a non-cooperative system, it is always mandatory to recognize the code and interleaver parameters at the receiver for decoding and de-interleaving, respectively.
- To propose an intelligent broadcast or communication receiver system which adapts itself to any specific broadcast or communication applications by estimating the code and interleaver parameters.
- Previously proposed algorithm in [17] for blind reconstruction of RS encoder can recognize only codeword length. However, generator polynomial and code dimension are mandatory for decoding RS coded symbols.
- The LLR-based technique proposed for RS codes in [4] assumes a predefined candidate set of RS encoders at the transmitter and receiver. Further, the bit position adjustment parameter to achieve time synchronization is not recognized.
- In the prior works, the block interleaver parameter estimation algorithms were restricted to convolutional encoded data. Furthermore, only interleaver period of block interleaver was estimated for non-binary RS codes and the same is not sufficient to de-interleave the coded symbols. Therefore, to the best of our knowledge, algorithms or methodologies have not been proposed for estimating all block interleaver parameters considering non-binary codes along with symbol position adjustment parameter to achieve time synchronization.
- It is also mandatory to propose algorithms for blind estimation of interleaver and RS outer code parameters to complete the parameter estimation process of serial concatenated codes.
- Finally, the accuracy of estimation of RS code and interleaver parameters and its inferences are not extensively reported in the literature.

B. Contributions

The major contributions of this manuscript are given as follows:

- Algorithms for the blind recognition of RS code parameters such as codeword length n, code dimension k, number of bits per symbol m, primitive polynomial p, and generator polynomial $g(x)$ are given for non-erroneous (noiseless) and erroneous (noisy) scenarios.
- Algorithms are proposed for the joint recognition of RS code and block interleaver parameters for erroneous (noisy) scenario. Matrix and helical scan interleavers are the types of block interleavers taken into consideration in the present work. Moreover, interleaver period β, number of rows N_r and columns N_c of interleaver matrix, and helical array step size d are the block interleaver parameters estimated from the incoming erroneous, non-synchronized, and non-binary coded data symbols.
- Bit/symbol position adjustment to achieve frame synchronization is also integrated with the proposed code and interleaver parameter estimation algorithms.
- Accuracy of parameter estimation of RS codes and block interleavers for various test cases considering different modulation schemes, codeword length, and code dimension values is demonstrated to prove the robustness of the algorithms. $M-$ary quadrature amplitude modulation ($M-$QAM) and $M-$ary phase-shift keying ($M-$PSK) schemes are considered in our simulation studies.

- Finally, performance of the proposed algorithms is also compared with the prior works reported in the literature.

The proposed algorithms can be integrated with convolutional inner code parameter estimation algorithms proposed in [6]-[10] to complete the parameter estimation process of serial concatenated codes. However, in this manuscript, we have restricted our work to the estimation of RS code and block interleaver parameters alone. It is also to be noted that together with the blind channel estimation techniques given in [28] and [29], the proposed code and interleaver parameter estimation techniques with blind frame synchronization will pave the way for designing a blind/intelligent/reconfigurable receiver system.

C. Organization of the manuscript

The manuscript is organized as follows. In Section II, the blind reconstruction of RS encoder over non-erroneous and erroneous scenarios is discussed with greater details. Further, in Section III, the parameter estimation algorithms for block interleavers over RS codes are given. In Section IV, simulation results and related discussions are given for various case studies. Finally, concluding remarks are given in Section V.

II. Parameter estimation of RS codes without interleaver

Here, in this section, we discuss the parameter estimation of RS codes without interleaver. Firstly, a brief introduction about RS codes is given. After that the parameter estimation process is explained with the help of a block diagram. Further, methodologies for parameter estimation over erroneous and non-erroneous scenarios are discussed.

A. Reed-Solomon Codes

RS codes belong to a special class of non-binary BCH codes. The code symbols generated from RS codes belong to $GF(2^m)$, where m denotes the number of bits per symbol and $m \geq 3$. Let α be a primitive element of $GF(2^m)$ such that $\alpha^{2^m-1}=1$. In the case of t error correcting (n,k) RS codes, $\alpha, \alpha^2, \cdots, \alpha^{2t}$ are the roots of the generator polynomial $g(x)$ with degree $n-k$, which is given by

$$g(x) = \text{lcm}(\phi_1(x), \phi_2(x), ..., \phi_{2t}(x)), \tag{1}$$

where $\phi_i(x)$ is the minimal polynomial of α^i. Since α^i is an element of $GF(2^m)$, $\phi_i(x) = x - \alpha^i$. Hence, $g(x)$ can be written as

$$\begin{aligned} g(x) &= (x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{2t}) \\ &= g_0 + g_1\, x + g_2\, x^2 + \cdots + g_{2t-1}\, x^{2t-1} + x^{2t} \end{aligned} \tag{2}$$

From (2), it is observed that $g(x)$ has 2t+1 non-zero terms. Since $g(x)$ is $n-k$ degree polynomial, it can be written as $n-k=2t$. In a nutshell, RS code with symbols from $GF(2^m)$ has the following parameters [26]:

- Codeword length $n = 2^m - 1$
- Number of parity check symbols $n-k=2t$
- Code dimension $k = 2^m - 1 - 2t$
- Minimum hamming distance $d_{\text{min}} = 2t+1$

In this manuscript, we denote RS encoded data symbols as RS(n,k,m,p), where n, k, m, and p denote the codeword length, code dimension, number of bits per symbol, and integer representation of primitive polynomial $p(x)$, respectively.

B. Code parameter estimation process

The generic block diagram for the parameter estimation of RS codes is given in Fig. 1. The RS coded symbols are converted into binary data and then modulated using appropriate modulation schemes for storage or transmission. In the receiver side, after demodulation, the RS code and bit position adjustment parameters are estimated from binary coded data symbols by varying m, corresponding primitive polynomials $p(x)$, and bit position adjustment ϕ. We also discuss the parameter estimation when the receiver frames are not properly synchronized. In order to analyze such cases, we introduce bit offset at the receiver. The receiver only knows that the incoming data is RS coded without knowing the code parameters.

C. Parameter estimation over non-erroneous scenario

The parameter estimation of RS codes over non-erroneous scenario has been explained using Algorithm 1. The incoming binary symbols after demodulation are converted into non-binary RS coded symbols while simultaneously varying m, primitive polynomials $p(x)$ corresponding to m, and bit position adjustment parameter ϕ. Note that $p = \text{primpoly}(m, `all')$ returns all primitive polynomials $p(x)$ corresponding to m in an integer form, where $m \geq 3$. For instance, $p=37$ represents the polynomial $p(x) = x^5 + x^2 + 1$ due to the fact that 37_{10}=1 0 0 1 0 1_2. After converting the incoming binary data symbols into non-binary symbols between 0 and $2^m - 1$, a Galois field (GF) array is created. This array comprises of GF elements between 0 and $2^m - 1$ and it interprets the integers in the array with respect to a specific primitive polynomial for that field. The GF array, which comprises of RS coded symbols, is reshaped into a matrix S of size $a \times b$, where a and b denote the number of rows and columns of S, respectively. Since the matrix contains coded data symbols, it is called data matrix. The rank and rank ratio of S are calculated by performing finite-field Gauss elimination process [22]. The rank ratio refers to the ratio of the rank of a matrix to the number of columns. The rank of a matrix is the number of linearly independent rows/columns of a matrix. It can be obtained by transforming the given matrix into its row/column echelon form using Gauss elimination method. The number of non-zero rows/columns of row/column echelon form gives the rank. In this paper, column-wise operation is performed and the column echelon form of S is denoted by F. Please note that the similar operations can be performed row-wise as well. As RS coded symbols belong to finite-field or GF, finite-field Gauss elimination method has to be used instead of Gauss elimination to evaluate rank and rank ratio. From the rank ratio values, RS code parameters m, n, k, and $p(x)$ along with bit position adjustment parameter ϕ are estimated. Note that when rank of S is equal to $\min(a,b)$ or rank ratio is equal to unity or when all the columns and rows of S are

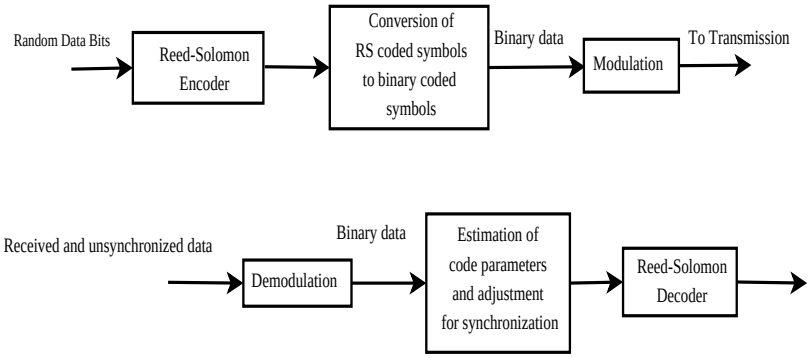


Fig. 1. Generic block diagram for parameter estimation of RS codes

Algorithm 1: Estimation of RS code parameters (non-erroneous scenario)

Notations: Let ϕ denotes the bit position adjustment to achieve synchronization. b and a indicate the number of columns and rows of data matrix S, respectively. The rank and rank ratio of S are denoted by $\rho(m,p,\phi)$ and $\rho'(m,p,\phi)$, respectively and F denotes the column echelon form of S. Finally, m_{est}, n_{est}, k_{est}, p_{est}, and ϕ_{est} denote the estimate of m, n, k, p, and ϕ, respectively

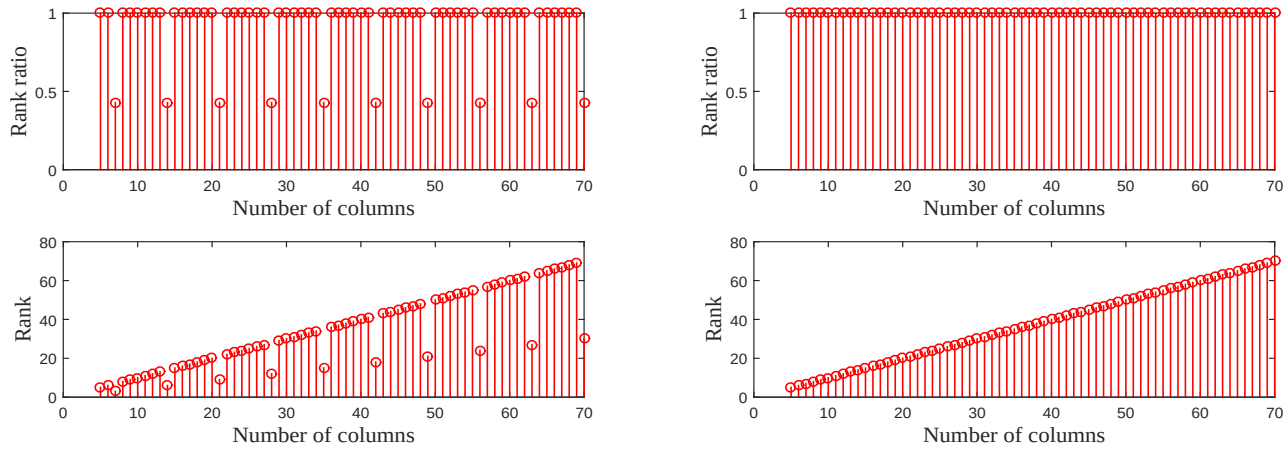
Assumptions: $a \geq 2b$, $m \in [m_{\text{min}}\ ,\ m_{\text{max}}]$, $\phi \in [0, ((2^m-1)m)-1]$ and the incoming bit stream is assumed to be RS encoded.

1: **for** $m = m_{min} : m_{max}$ **do**
  2: $p = primpoly(m, `all')$;
  3: **for** $\phi = 0 : ((2^m-1)m)-1$ **do**
    4: Shift ϕ bit positions and convert the binary data symbols into the respective elements of GF using p;
    5: Reshape the RS encoded GF elements into a data matrix S of size $a \times b$, where $b = 2^m - 1$;
    6: Use finite-field Gauss elimination process in $GF(2^m)$ to convert S into F;
    7: Compute $\rho(m,p,\phi)$ from the number of non-zero columns in F;
    8: Compute $\rho'(m,p,\phi) = \rho(m,p,\phi)/b$;
  end
end
9: Obtain $[m_{\text{est}}, p_{\text{est}}, \phi_{\text{est}}] = \underset{m,p,\phi}{\text{argmin}}(\rho'(m,p,\phi))$, $n_{\text{est}} = 2^{m_{\text{est}}} - 1$, and $k_{\text{est}} = \rho(m_{\text{est}}, p_{\text{est}}, \phi_{\text{est}})$;

linearly independent, then S is called full rank matrix. If the rank of S is less than $\min(a,b)$ or rank ratio is less than unity or when there is at least one column/row that is dependent on other columns/rows, then S is called rank deficient matrix.

While varying m in Algorithm 1, it is to be noted that b is also varied, since $b = 2^m - 1$. The correct combination of $[m,p,\phi]$, which minimizes rank ratio $\rho'(m,p,\phi)$, has been chosen as the estimated RS code and bit position adjustment parameters as mentioned in step 9 of Algorithm 1. The reason for rank deficiency is explained as follows: Firstly, we demonstrate the rank deficiency and full rank phenomena using RS$(7,3,3,11)$. In Fig. 2(a) and Fig. 2(b), the rank ratio and rank values of S are plotted against the number of columns b by assuming that the incoming data is synchronized for RS code RS$(7,3,3,11)$ considering non-erroneous and erroneous scenarios, respectively. From Fig. 2(a), it is inferred that when b is a multiple of n, rank deficiency is obtained. Further, for the case when b is not a multiple of n, full rank is obtained. From Fig. 2(b), it is observed that full rank is obtained irrespective of the number of columns for erroneous scenario (detailed explanation for Fig. 2(b) is given in Section II.D).

In the manuscript, we have used systematic encoding to explain the rank deficiency and full rank phenomena with better clarity. However, the proposed algorithms also work in the case of non-systematic encoding. Due to inherent property of systematic RS codes, n coded output data symbols depend on k uncoded input data symbols or each parity symbol is a linear combination of information symbols [22]. In the case of non-systematic RS codes, each of n data symbols will be a linear combination of k symbols [17]. Hence, $\alpha' \cdot n$ output symbols of S depend on $\alpha' \cdot k$ symbols, where α' is an integer and $\alpha' \geq 1$. As depicted in Fig. 3, it is observed that α' codewords in all the rows will be aligned properly in the same column only for the case when b is a multiple of n i.e. $b = \alpha' \cdot n$. Note that Fig. 3 is shown for the case when $\alpha' = 1$. If the data (i.e. independent) and parity (i.e. dependent) symbols in all the rows are aligned properly in the same column as shown in Fig. 3, the linear relation is satisfied in all the rows. Therefore, there will exist linear relations between columns in S. After converting S into F through finite field Gauss elimination process [22], all $\alpha' \cdot (n-k)$ dependent columns in S will be eliminated. There will be only $\alpha' \cdot k$ non-zero or independent columns out of b columns and hence, rank deficiency will be obtained. The deficient rank value for the case when $b = \alpha' \cdot n$ is given by $\alpha' \cdot k$. The finite field Gauss elimination process converts a given matrix, whose elements belong to a finite field, into a row or column echelon form by eliminating all the dependent rows or columns. In Algorithm 1, for the correct combination of $[m,p,\phi]$, the data and parity symbols of $\alpha' = 1$ codeword in all the rows of S will be aligned properly in the same column, which in turn will lead to deficient rank. The reason for rank deficiency in the case of RS codes is also explained in Appendix A using case study 1.



(a) (b)

Fig. 2. (a) Variation of rank ratio and rank versus number of columns for RS$(7, 3, 3, 11)$ considering non-erroneous case (b) Variation of rank ratio and rank versus number of columns for RS$(7, 3, 3, 11)$ considering SER=3×10^{-2}

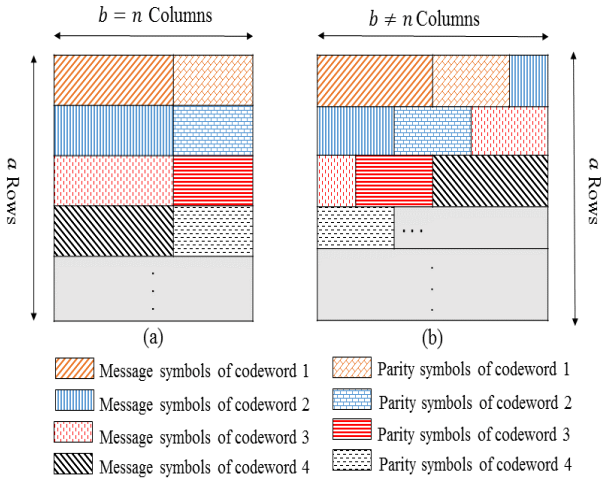


Fig. 3. Structure of data matrix for the case when (a) $b=n$ and (b) $b\neq n$

As depicted in Fig. 3, it is noticed that the data and parity symbols of α' codewords in all the rows are not aligned properly in the same column for the case when b is not a multiple of n i.e. $b \neq \alpha' \cdot n$. If data and parity symbols of a same code word are segregated in different rows and are not aligned properly in the same column, then certain parity symbols of a particular codeword cannot be represented as a linear combination of message symbols. Hence, the linear relation in a particular row will be affected, which in turn will lead to disappearance of linear relations between columns in S. Therefore, S will behave like a random matrix and will not have any dependent columns. After converting S into F, no dependent columns will be eliminated and full rank will be obtained. In Algorithm 1, the data and parity symbols of $\alpha'=1$ codeword in all the rows of S with b columns will not be aligned properly in the same column for incorrect combination of $[m, p, \phi]$, which in turn will lead to full rank. The reason for full rank is also explained in Appendix A using case study 1.

Refer to [6], [7], [16], and [17] for further details regarding the rank deficiency and full rank phenomena in block and convolutional codes.

In a nutshell, assuming $[m_{\text{est}}, p_{\text{est}}, \phi_{\text{est}}]$ are correct values of estimated parameters from Algorithm 1, if $b = n_{\text{est}} = 2^{m_{\text{est}}} - 1$, then the rank deficiency will be obtained. The rank and rank ratio for $b=n_{\text{est}}$ are, respectively, given by

$$\begin{aligned} \rho(m_{\text{est}}, p_{\text{est}}, \phi_{\text{est}}) &= k_{\text{est}}, \\ \rho'(m_{\text{est}}, p_{\text{est}}, \phi_{\text{est}}) &= \frac{k_{\text{est}}}{b} = r\,, \end{aligned} \tag{3}$$

where r is the code rate of RS codes. Similarly, if b is a multiple of n_{est} (i.e. $b = \alpha' \cdot n_{\text{est}}$), then $\rho(m_{\text{est}}, p_{\text{est}}, \phi_{\text{est}}) = \alpha' \cdot k_{\text{est}}$ and $\rho'(m_{\text{est}}, p_{\text{est}}, \phi_{\text{est}}) = r$.

However, if $b \neq \alpha' \cdot n_{\text{est}}$, then full rank will be obtained i.e. $\rho(m_{\text{est}}, p_{\text{est}}, \phi_{\text{est}}) = b$ and hence, $\rho'(m_{\text{est}}, p_{\text{est}}, \phi_{\text{est}}) = 1$. Since only correct combination of $[m, p, \phi]$ gives deficient rank, we obtain the RS code parameters and bit position adjustment parameter which minimize $\rho'(m, p, \phi)$.

D. Parameter estimation over erroneous scenario

Since all the dependent columns in S will be eliminated using finite-field Gauss elimination process, the number of non-zero columns gives the deficient rank value in the case of non-erroneous scenario. The proposed rank deficiency based algorithm considering non-erroneous scenario fails for noisy scenario [16], [19], and [22]. As stated before, full rank of a matrix corresponds to the fact that all rows and columns of the matrix are linearly independent. In addition, a matrix would have deficient rank only when there is at least one column/row that is dependent on other columns/rows. The presence of transmission errors or white noise increases the linear independence among rows/columns of a deficient rank matrix [17]. It is because of this reason, the data matrix S exhibits full rank feature irrespective of the number of columns b in an erroneous environment. However, it is to be noted that this linear independence increases with the noise level. When the noise level exceeds a threshold value, the resulting received data matrix S will not have any dependent columns and will behave like a random matrix. Hence, full rank will be obtained irrespective of b. For example, in Fig. 2(b), the variation of rank ratio and rank values with respect to the number of columns is shown for RS$(7, 3, 3, 11)$ considering the case when SER $= 3 \times 10^{-2}$. It is observed that full rank is obtained irrespective of b. However, it is noticed that the dependent columns in S will have less number of non-zero elements in F compared to independent columns. Hence, it is intuitive that the column echelon form of deficient rank matrix over erroneous channel conditions will have less number of non-zero elements compared to the full rank matrix. In the case of full rank matrix, each element in the finite field will occur with equally likely probability [22]. Thus, the rank deficient matrix over erroneous channel conditions can be identified based on the number of non-zero elements in F instead of number of non-zero columns. Therefore, we modify Algorithm 1 for erroneous scenario and RS code parameters are estimated based on normalized non-zero-mean-ratio of F using Algorithm 2. The normalized non-zero-mean-ratio, which is denoted by $\mu'(m, p, \phi)$ in Algorithm 2, is the ratio of the sum of normalized mean value of the number of non-zero elements in each column to the total number of columns of F. Note that the normalization is done with respect to maximum value.

Most of the steps (i.e. step 1 to 6) in Algorithm 2 are similar to Algorithm 1. The only difference is the correct combination of $[m, p, \phi]$, which minimizes normalized non-zero-mean-ratio $\mu'(m, p, \phi)$, has been chosen as the estimated RS code and bit position adjustment parameters instead of identifying the parameters based on rank ratio. It is to be noted that the code polynomials share the roots of generator polynomial. Hence, we evaluate the number of roots of more than 100 code polynomials. It has been observed that in most of the cases, the number of roots for code polynomials and generator polynomial are the same though there exists few cases with different number of roots. Hence, we adopt a maximum likelihood approach to evaluate the number of roots of the generator polynomial. Therefore, by identifying the number of roots, $2t$ is estimated and for RS codes $n - k = 2t$. As n_{est} is already known from Algorithm 2, k_{est} is recognized from $n - k$. After estimating the number of roots of code polynomial, the generator polynomial $g(x)$ is obtained from (2).

Algorithm 2: Estimation of RS code parameters (erroneous scenario)

Notations: Let us denote the mean value and normalized mean value of number of non-zero elements in c^{th} column of F as $\sigma(c, m, p, \phi)$ and $\sigma'(c, m, p, \phi)$, respectively. Further, the normalized non-zero-mean-ratio is denoted as $\mu'(m, p, \phi)$.
Assumptions: $a \geq t\, b$, where t is a constant and the erroneous incoming bit stream is assumed to be RS encoded.
1: **for** $m = m_{min} : m_{max}$ **do**
  2: $p = \text{primpoly}(m, 'all')$;
  3: **for** $\phi = 0 : ((2^m - 1)m) - 1$ **do**
    4: Shift the erroneous incoming binary data symbols by ϕ bit positions and convert it into the respective elements of GF using p;
    5: Reshape the RS encoded GF elements into a data matrix S of size $a \times b$, where $b = 2^m - 1$;
    6: Convert S into F using finite-field Gauss elimination process;
    7: Evaluate $\sigma(c, m, p, \phi)$, where $c \in \{1, 2, ..., b\}$, and normalize the obtained values with respect to the maximum value;
    8: Calculate $\mu'(m, p, \phi)$, where $\mu'(m, p, \phi) = \frac{\sum_{c=1}^{b} \sigma'(c, m, p, \phi)}{b}$;
  end
end
9: Obtain $[m_{\text{est}}, p_{\text{est}}, \phi_{\text{est}}] = \underset{m,p,\phi}{\text{argmin}}(\mu'(m, p, \phi))$ and $n_{\text{est}} = 2^m\text{est} - 1$;
10: Identify the number of roots of generator polynomial and estimate $n - k$;
11: Obtain k_{est} from $n - k$;
12: Obtain the generator polynomial $g(x)$ from (2);

III. Parameter estimation of block interleavers over RS codes

In this section, the parameter estimation of block interleavers, which include matrix and helical scan interleavers, over RS codes is discussed. A brief introduction about the

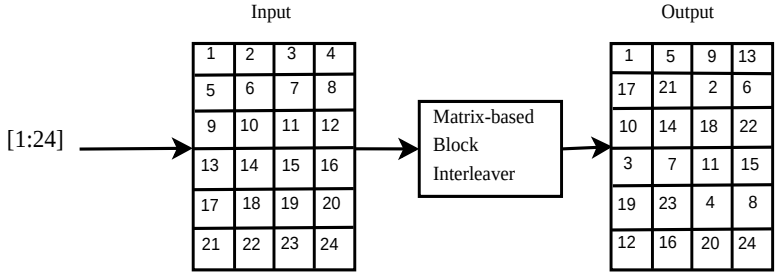


Fig. 4. Matrix-based block interleaver operation assuming $N_r = 6$ and $N_c = 4$ considering input values $[1 : 24]$

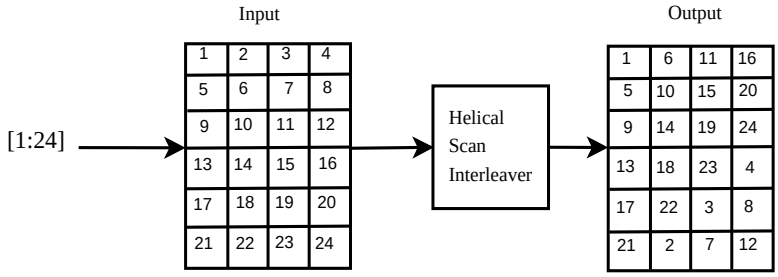


Fig. 5. Helical scan interleaver operation assuming $N_r = 6$, $N_c = 4$, and $d = 1$ considering input values $[1 : 24]$

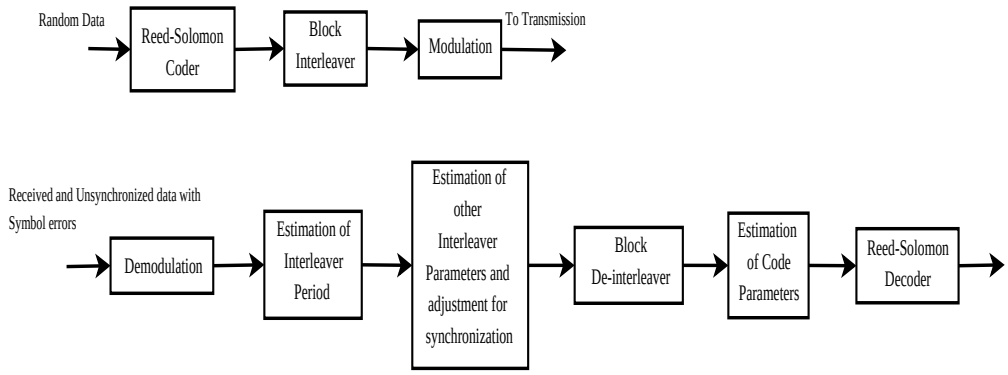


Fig. 6. Generic block diagram for interleaver parameter estimation process over RS codes considering block interleavers

interleavers is given. After that the parameter estimation methodologies for both the interleavers are reported.

A. Block interleavers

Since block interleavers are being used in most of the communication and storage systems, we have taken the same into consideration. The operation of a matrix-based block interleaver is simple and straight forward. For neighboring symbols to encounter independent fading, a matrix-based block interleaver stores the data symbols row-wise in a matrix of size $N_r \times N_c$ and reads column-wise, where N_r and N_c denote the number of rows and columns of the matrix, respectively. An example for matrix-based block interleaver with $N_r = 6$ and $N_c = 4$ is shown in Fig. 4. Similarly, the helical scan interleaver stores the data symbols row-wise in a matrix of size $N_r \times N_c$. However, the data symbols will be interleaved in a helical fashion according to helical array step size d unlike matrix-based block interleaver and $d < N_r$. It is to be noted that the interleaver period for block interleavers is given by $\beta = N_r \times N_c$. In Fig. 5, the helical scan interleaver operation with $N_r = 6$, $N_c = 4$, and $d = 1$ is shown.

B. Interleaver parameter estimation process

A generic block diagram is given in Fig. 6, which shows the interleaver parameter estimation process over RS codes. Here, the interleaver block follows the RS encoder to counteract the burst errors. The RS encoded and interleaved data stream is transmitted using suitable modulation scheme. After demodulation at the receiver, interleaver period β along with RS code parameters (i.e. m, $p(x)$, and n) and symbol position adjustment parameter ϕ' will be estimated. The interleaver period is an intermediate parameter which is to be estimated in order to identify N_r, N_c, and d. Subsequently, individual block interleaver parameters and symbol adjustment parameter will be estimated by de-interleaving with limited possible combinations of interleaver parameters. The code dimension k and generator polynomial $g(x)$ will be estimated after de-interleaving using the estimated interleaver parameters. The receiver only knows that the incoming data is RS coded and block interleaved without knowing the code and interleaver parameters.

Algorithm 3: Estimation of interleaver period (non-erroneous scenario)

Notations: The rank and rank ratio of S are denoted by $\rho(m,p,b)$ and $\rho'(m,p,b)$, respectively.
Assumptions: $a \geq 2b$, $b \in [b_{\min}\ ,\ b_{\max}]$ and the incoming bit stream is assumed to be RS encoded and block interleaved.
1: **for** $m = m_{min} : m_{max}$ **do**
  2: p=primpoly(m,$'all'$);
  3: **for** $b = b_{min} : b_{max}$ **do**
    4: Convert the incoming RS coded and block interleaved binary data symbols into the respective elements of GF using p;
    5: Reshape the RS encoded GF elements into a data matrix S of size $a \times b$;
    6: Convert S into F using finite-field Gauss elimination process;
    7: Compute $\rho(m,p,b)$ from the number of non-zero columns in F;
    8: Compute $\rho'(m,p,b) = \rho(m,p,b)/b$;
  end
end
9: Obtain $[m_{\text{est}}, p_{\text{est}}, b_{\text{est}}] = \underset{m,p,b}{\text{argmin}}(\rho'(m,p,b))$ and $n_{\text{est}} = 2^{m_{\text{est}}} - 1$;

C. Parameter estimation over non-erroneous scenario

In this section, innovative algorithms are proposed for estimating the block interleaver parameters from the RS encoded data stream. Firstly, the algorithm for estimating interleaver period (i.e. $\beta = N_r \times N_c$) over non-erroneous scenario is proposed (refer to Algorithm 3).

Unlike Algorithm 1, b is varied from $b_{\min}$ to $b_{\max}$ in Algorithm 3. The correct combination of $[m,p,b]$, which minimizes the rank ratio $\rho'(m,p,b)$, has been chosen as the estimated parameters as mentioned in step 9 of Algorithm 3.

We already know that the output n data symbols depend only on k input symbols in the case of RS codes. Hence, $\alpha' \cdot \gamma \cdot n$ output symbols of S in a particular row depend on $\alpha' \cdot \gamma \cdot k$ input symbols, where γ and α' are integers, $\alpha' \geq 1$ and $\gamma \geq 1$. The message and parity symbols of $\alpha' \cdot \gamma$ codewords in all the rows will be aligned properly in the same column only for the case when b is a multiple of β i.e. $b = \alpha' \cdot \beta$ and β is a multiple of n i.e. $\beta = \gamma \cdot n$. Because of the proper alignment similar to Fig. 3(a), there will exist linear relations between the columns of S. Hence, after converting S into F, there will be only $\alpha' \cdot \gamma \cdot k$ independent columns out of b columns and the rank deficiency will be observed for the case when b is a multiple of β. The deficient rank value is given by $\alpha' \cdot \gamma \cdot k$. Similarly, if β is not a multiple of n, then it is expected that the rank deficiency will be observed for the case when b is a multiple of $\text{lcm}(n,\beta)$ i.e. $b = \alpha' \cdot \text{lcm}(n,\beta)$ assuming $\text{lcm}(n,\beta) = \Gamma \cdot n$, where Γ is an integer and $\Gamma \geq 1$. In Algorithm 3, the data and parity symbols of $\alpha' \cdot \gamma$ or $\alpha' \cdot \Gamma$codewords in all the rows of S with b columns will be aligned properly in the same column for the correct combination of $[m,p,b]$, which in turn will lead to deficient rank.

If $b \neq \alpha' \cdot \beta$ or $b \neq \alpha' \cdot \text{lcm}(n,\beta)$, then data and parity symbols of $\alpha' \cdot \gamma$ or $\alpha' \cdot \Gamma$ codewords in all the rows will not be aligned properly in the same column similar to Fig. 3(b). Because of this the linear relations between the columns in S will be affected and S will behave like a random matrix. Since no dependent columns will be eliminated using finite field Gauss elimination process, full rank will be obtained. In Algorithm 3, the data and parity symbols of $\alpha' \cdot \gamma$ or $\alpha' \cdot \Gamma$ codewords in all the rows of S with b columns will not be aligned properly in the same column for the incorrect combination of $[m,p,b]$, which in turn will lead to full rank. As only correct combination of $[m,p,b]$ gives deficient rank, we obtain interleaver period and RS code parameters which minimize $\rho'(m,p,b)$.

The rank deficiency and full rank phenomena of RS code with block interleaver for the case when β is a multiple of n is also explained using another case study given in Appendix B.

It is also inferred from Algorithm 3 that $\beta_{\text{est}} = b_{\text{est}}$ for the case when β is a multiple of n, where β_{est} is the estimate of interleaver period β. For the case when β is not a multiple of n, $\text{lcm}(n_{\text{est}}, \beta_{\text{est}}) = b_{\text{est}}$. Note that β_{est} or $\text{lcm}(n_{\text{est}}, \beta_{\text{est}}) = b_{\text{est}}$ is applicable when $\rho'(m_{\text{est}}, p_{\text{est}}, b_{\text{est}})$ is the only minimum value in the search space. If there are multiple values of b for which $\rho'(m,p,b)$ is minimum, then the difference between successive number of columns with rank deficiency gives the estimate of β_{est} or $\text{lcm}(n_{\text{est}}, \beta_{\text{est}})$. Let $b = \alpha' \cdot \beta$ and $b' = (\alpha'+1) \cdot \beta$ denote two successive columns with deficient rank values for the case when $\beta = \gamma \cdot n$. From $b' - b$, the interleaver period β is identified. Similarly, $\text{lcm}(n,\beta)$ is identified from $b' - b$ for the case when $\beta \neq \gamma \cdot n$ and $\text{lcm}(n,\beta) = \Gamma \cdot n$.

For further details regarding the rank deficiency and full rank phenomena in case of FEC codes with interleaver, [16], [19], [20], [22], and [24] can be referred.

In a nutshell, let the RS coded and block interleaved symbols are reshaped into a data matrix S with b columns. Assuming $[m_{\text{est}}, p_{\text{est}}, b_{\text{est}}]$ are estimated correctly using Algorithm 3, **if β is a multiple of** n i.e. $\beta = \gamma \cdot n$ and $b = \alpha' \cdot \beta$, where γ and α' are integers, then the rank deficiency will be obtained. The deficient rank and rank ratio are, respectively, given by

$$\begin{aligned} \rho(m_{\text{est}}, p_{\text{est}}, b_{\text{est}}) &= \alpha' \cdot \gamma \cdot k_{\text{est}}, \\ \rho'(m_{\text{est}}, p_{\text{est}}, b_{\text{est}}) &= \frac{\rho(m_{\text{est}}, p_{\text{est}}, b_{\text{est}})}{b} = r\,. \end{aligned} \quad (4)$$

However, if $b \neq \alpha' \cdot \beta$, then full rank will be obtained.

Moreover, **If β is not a multiple of** n, then rank deficiency will be obtained for the case when b is a multiple of $\text{lcm}(n,\beta)$ i.e. $b = \alpha' \cdot \text{lcm}(n,\beta)$. Assuming $\text{lcm}(n,\beta) = \Gamma \cdot n$, where Γ is an integer, the deficient rank and rank ratio values are, respectively, given by

$$\begin{aligned} \rho(m_{\text{est}}, p_{\text{est}}, b_{\text{est}}) &= \alpha' \cdot \Gamma \cdot k_{\text{est}}, \\ \rho'(m_{\text{est}}, p_{\text{est}}, b_{\text{est}}) &= \frac{\rho(m_{\text{est}}, p_{\text{est}}, b_{\text{est}})}{b} = r\,. \end{aligned} \quad (5)$$

However, if $b \neq \alpha' \cdot \text{lcm}(n,\beta)$, then full rank will be obtained.

Algorithm 4: Estimation of interleaver period (erroneous scenario)

Notations: Let us denote the mean value and normalized mean value of number of non-zero elements in c^{th} column of F as $\sigma(c,m,p)$ and $\sigma'(c,m,p)$, respectively. Further, the normalized non-zero-mean-ratio is denoted as $\mu'(m,p,b)$.

Assumptions: $a \geq t\,b$, where t is a constant, and the erroneous incoming bit stream is assumed to be RS encoded and block interleaved.

1: **for** $m = m_{min} : m_{max}$ **do**
  2: p=primpoly(m,' all');
  3: **for** $b = b_{min} : b_{max}$ **do**
    4: Convert the incoming RS coded and block interleaved binary data symbols into the respective elements of GF using p;
    5: Reshape the RS encoded GF array elements into a data matrix S of size $a \times b$;
    6: Convert S into F using finite-field Gauss elimination process;
    7: Evaluate $\sigma(c,m,p)$, where $c \in \{1,2,...,b\}$, and normalize the obtained values with respect to the maximum value;
    8: Calculate normalized non-zero-mean-ratio $\mu'(m,p,b)$, where $\mu'(m,p,b) = \frac{\sum_{c=1}^{b} \sigma'(c,m,p)}{b}$;
  end
end
9:Obtain $[m_{\text{est}}, p_{\text{est}}, b_{\text{est}}] = \underset{m,p,b}{\text{argmin}}(\mu'(m,p,b))$ and $n_{\text{est}} = 2^{m_{\text{est}}} - 1$;

D. Parameter estimation over erroneous scenario

The methodology proposed for non-erroneous scenario when applied to erroneous scenario will result in full rank irrespective of the number of columns due to erroneous symbols. Hence, Algorithm 3 is modified for erroneous scenario and β or lcm(n,β) is estimated based on normalized non-zero-mean-ratio of F i.e. $\mu'(m,p,b)$ using Algorithm 4.

It is observed from Algorithm 4 that $\beta_{\text{est}} = b_{\text{est}}$ for the case when β is a multiple of n. For the case when β is not a multiple of n, lcm$(n_{\text{est}}, \beta_{\text{est}}) = b_{\text{est}}$. Alternatively, β_{est} or lcm$(n_{\text{est}}, \beta_{\text{est}})$ can be estimated by observing the difference between successive number of columns with lower values of $\mu'(m,p,b)$. After estimating β_{est} or lcm$(n_{\text{est}}, \beta_{\text{est}})$, n_{est}, m_{est}, and p_{est}, it is mandatory to estimate the number of rows and columns of block interleaver i.e. N_r and N_c (for both matrix-based and helical scan block interleavers), step size for helical scan interleaver d, symbol position adjustment parameter ϕ', and code dimension k of RS codes. Algorithm 5 is proposed for estimating N_r, N_c, d, ϕ', and k. Firstly, the incoming binary data symbols are converted into respective elements of $GF(2^m)$, where $m = m_{\text{est}}$, using the estimated primitive polynomial p_{est}. After that the coded symbols are shifted by ϕ' symbol positions, where ϕ' is the symbol adjustment parameter, and de-interleaved with limited possible combinations of interleaver parameters i.e.

Algorithm 5: Estimation of N_r, N_c, ϕ', d, and k (erroneous scenario)

Notations : Let us denote $\zeta_{\text{est}} = \text{lcm}(n_{\text{est}}, \beta_{\text{est}})$, ϕ' as the symbol position adjustment to achieve synchronization. d denotes the helical array step size. Further, the normalized non-zero-mean-ratio of F for matrix-based and helical scan interleavers are denoted as $\mu'(N_r', N_c', \phi')$ and $\mu'(N_r', N_c', d, \phi')$, respectively. Finally, N_r^{est}, N_c^{est}, d^{est}, ϕ_1^{est} denote the estimate of N_r, N_c, d, and ϕ'.

Assumptions : $a \geq t\,b$, $\phi' \in [0\,,\,\zeta_{\text{est}} - 1]$, $d \in [1\,,\,N_r' - 1]$. It is assumed that lcm(n, β_{est}) or β_{est}, m_{est}, n_{est}, and p_{est} are estimated correctly using Algorithm 4.

1: **for** $\phi' = 0 : \zeta_{est} - 1$ **do**
  2: Convert the incoming RS coded and block interleaved binary data symbols into the respective elements of GF using p_{est};
  3: Get all possible values of δ' that satisfy lcm$(n_{\text{est}}, \delta') = \zeta_{\text{est}}$;
  4: Get all possible combinations of two factors N_r' and N_c' that satisfy $N_r'\,N_c' = \delta'$;
  5: Shift the coded and interleaved non-binary symbols by ϕ' symbol positions;
  6: De-interleave using N_r' and N_c' in the case of matrix-based block interleaver;
  7 De-interleave using N_r', N_c', and d in the case of helical scan interleaver;
  8: Fix b as a multiple of n_{est};
  9: Reshape the RS encoded GF elements into a data matrix S of size $a \times b$;
  10: Convert S into F using finite-field Gauss elimination process;
  11: Evaluate $\mu'(N_r', N_c', \phi')$ for all possible values of N_r' and N_c' in the case of matrix interleaver;
  12: Evaluate $\mu'(N_r', N_c', d, \phi')$ for all possible values of N_r', N_c', and d in the case of helical scan interleaver;
end
13: **Matrix-based block interleaver:** Obtain $[N_r^{\text{est}}, N_c^{\text{est}}, \phi_1^{\text{est}}] = \underset{N_r', N_c', \phi'}{\text{argmin}}\,(\mu'(N_r', N_c', \phi'))$;
14: **Helical scan interleaver:** Obtain $[N_r^{\text{est}}, N_c^{\text{est}}, d^{\text{est}}, \phi_1^{\text{est}}] = \underset{N_r', N_c', d, \phi'}{\text{argmin}}\,(\mu'(N_r', N_c', d, \phi'))$;
15: **Matrix-based block interleaver:** Shift ϕ_1^{est} symbol positions and de-interleave using N_r^{est} and N_c^{est};
16: **Helical scan interleaver:** Shift ϕ_1^{est} symbol positions and de-interleave using N_r^{est}, N_c^{est}, and d^{est};
17: Identify the number of roots of generator polynomial and estimate $n - k$;
18: Obtain k_{est} from $n - k$;
19: Obtain the generator polynomial $g(x)$ from (2);

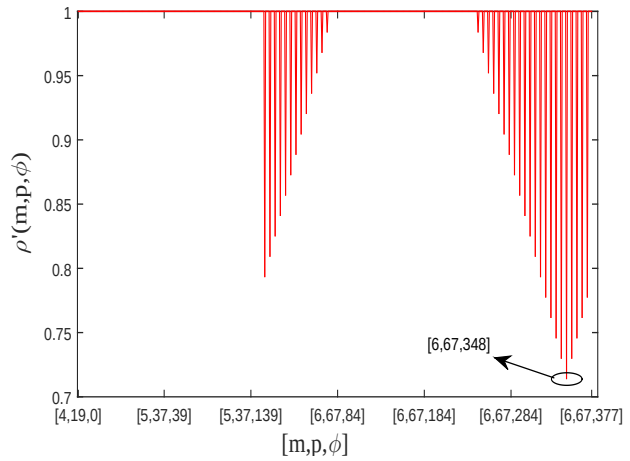


Fig. 7. Variation of $\rho'(m,p,\phi)$ with respect to $[m,p,\phi]$ for RS$(63,45,6,67)$ assuming 64-QAM scheme, $\Delta = 6$, and non-erroneous scenario

TABLE I
SIMULATION PARAMETERS

Modulation schemes	BPSK, QPSK, 8-PSK, 8-QAM 16-PSK, 16-QAM, 32-QAM, 64-QAM, 256-QAM
Symbol error rate (SER)	0.001 to 0.1
Signal-to-noise ratio (SNR)	$\geq$5 dB
Number of rows	a=2b (for non-erroneous case) and $a > 2b$ (for erroneous case)
RS Codes tested	RS$(7,3,3,11)$, RS$(15,7,4,19)$, RS$(15,9,4,19)$, RS$(15,11,4,19)$, RS$(31,15,5,37)$, RS$(31,19,5,37)$, RS$(31,23,5,37)$, RS$(63,45,6,67)$, RS$(255,127,8,285)$
Block interleaver parameters	(a) $N_r = 15$ and $N_c = 7$ (b) $N_r = 5$, $N_c = 2$, and $d = 4$ (c) $N_r = 5$ and $N_c = 6$

$[N'_r, N'_c]$ or $[N'_r, N'_c, d]$ as mentioned in steps 6 and 7 of Algorithm 5. The de-interleaved symbols are reshaped into a data matrix of size $a \times b$, where b is fixed as a multiple of n_{est}. Using finite-field Gauss elimination process, the data matrix is converted into its column echelon form F and the normalized non-zero-mean-ratio of F is calculated for limited possible combinations of interleaver and synchronization parameters $[N'_r, N'_c, \phi']$ or $[N'_r, N'_c, d, \phi']$ as given in steps 11 and 12. The corresponding interleaver and synchronization parameters for which the normalized non-zero-mean-ratio reaches global minimum gives the estimate of N_r, N_c, d, and ϕ' as shown in steps 13 and 14. Finally, the code dimension is estimated from the number of roots of generator polynomial similar to Algorithm 2.

In Algorithm 5, by fixing b as a multiple of n_{est}, the block interleaver parameters are estimated successfully by searching the correct combination of $[N'_r, N'_c, \phi']$ or $[N'_r, N'_c, d, \phi']$, which minimizes the normalized non-zero-mean-ratio $\mu'(N'_r, N'_c, \phi')$ or $\mu'(N'_r, N'_c, d, \phi')$, respectively. The reason for fixing b as a multiple of n_{est} is given as follows: After de-interleaving using the correct block interleaver parameters, the data symbols will be RS encoded. If b is fixed as a multiple of n_{est}, then the rank deficiency will be obtained for RS coded data symbols. Equivalently, the normalized non-zero-mean-ratio $\mu'(N'_r, N'_c, \phi')$ or $\mu'(N'_r, N'_c, d, \phi')$ will be lower for rank deficient matrix in erroneous scenario. However, if RS encoded data symbols are de-interleaved using incorrect block interleaver parameters, it is highly impossible to obtain deficient rank value by fixing b as a multiple of n_{est} due to misalignment of data and parity bits. Therefore, $\mu'(N'_r, N'_c, \phi')$ or $\mu'(N'_r, N'_c, d, \phi')$ will be higher for incorrect combinations of block interleaver parameters. Thus, the correct combination of $[N'_r, N'_c, \phi']$ or $[N'_r, N'_c, d, \phi']$, which minimizes $\mu'(N'_r, N'_c, \phi')$ or $\mu'(N'_r, N'_c, d, \phi')$, respectively, is chosen as the estimated block interleaver parameters as mentioned in steps 13 and 14 of Algorithm 5. It is also to be noted that $b \neq \zeta_{\text{est}}$ in Algorithm 5. This is because, if $b = \zeta_{\text{est}}$, then the rank deficiency will be observed for all possible combinations of N'_r and N'_c. Hence, the normalized non-zero mean ratio value will be approximately same for all possible combinations, which will lead to wrong estimation of N_r and N_c.

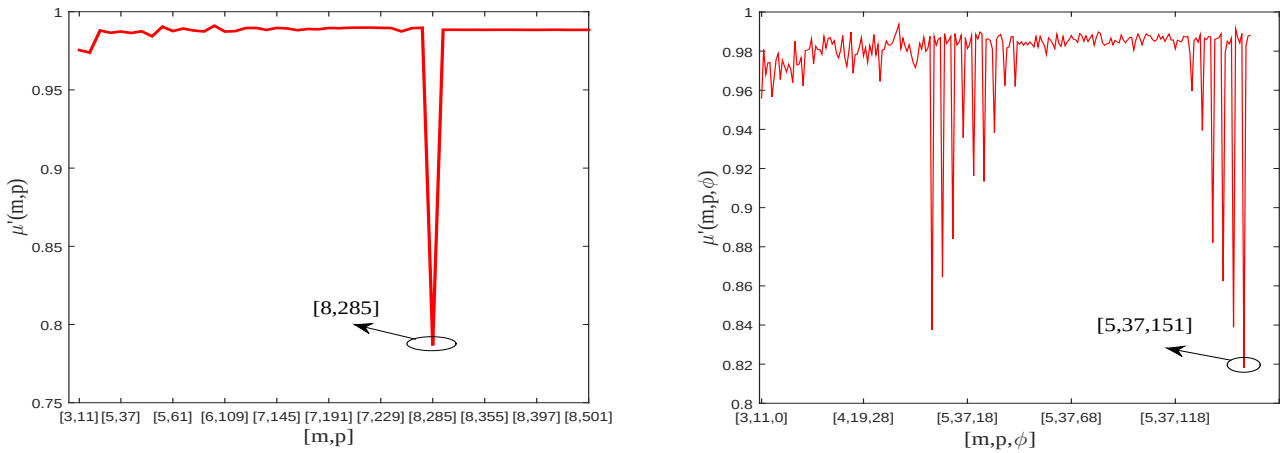
IV. Simulation Results and Discussions

Firstly, various simulation parameters assumed in this section are listed in Table I. For instance, if the receiver starts receiving the modulated data symbols at Δ^{th} symbol position of χ^{th} RS code word, then time synchronization is achieved after demodulation by shifting $\phi = (\chi\ m\ (q-1)+1) - (\Delta\ M_1 - M_1 + 1)$ bit positions, where $M_1 = \log_2 M$ and $q = 2^m$, for a system without interleaver. Further, if the receiver starts receiving the modulated data symbols at Δ^{th} symbol position of χ'^{th} interleaver block, then time synchronization is achieved after shifting $\phi' = (\chi' \zeta_{\text{est}} + 1) - \Delta$ symbol positions. It is to be noted that as the number of rows or t increases, the accuracy of estimation improves for erroneous case.

A. Simulation results for estimation of RS code parameters

In Fig. 7, the variation of rank ratio $\rho'(m,p,\phi)$ is shown with respect to $[m,p,\phi]$ for non-erroneous scenario, where m denotes the number of bits per symbol, $m \in [4\ ,\ 6]$, p denotes the integer representation of primitive polynomial, assuming RS$(63,45,6,67)$, 64-QAM scheme (i.e. $M = 64$ and $M_1 = 6$), $\Delta = 6$, and $\chi = 1$. From the curves, it is inferred that for $[m,p,\phi] = [6,67,348]$, $\rho'(m,p,\phi)$ is minimum and $\rho'(m,p,\phi) = r = 0.714$, which validates (3). Hence, RS code parameters $m_{\text{est}} = 6$, $n_{\text{est}} = 63$, $p_{\text{est}} = 67$, and $k_{\text{est}} = \rho(m,p,\phi) = 45$ are recognized correctly using Algorithm 1 for non-erroneous scenario. Moreover, the bit position adjustment to achieve time synchronization (i.e. $\phi_{\text{est}} = 348$) is also identified successfully using Algorithm 1.

In Fig. 8(a), the variation of normalized non-zero-mean-ratio $\mu'(m,p)$ is shown with respect to $[m,p]$, where $m \in [3\ ,\ 8]$, for RS$(255,127,8,285)$ considering synchronized scenario assuming 256-QAM scheme and SER=2×10^{-3}. Since the coded data is synchronized, we vary m and p alone in Algorithm 2 to



(a) (b)

Fig. 8. (a) Variation of normalized non-zero-mean-ratio $\mu'(m,p)$ with $[m,p]$ for RS$(255,127,8,285)$ coded data symbols assuming 256-QAM scheme and SER=2×10^{-3} (b) Variation of normalized non-zero-mean-ratio $\mu'(m,p,\phi)$ with $[m,p,\phi]$ for RS$(31,15,5,37)$ coded data symbols assuming 16-QAM scheme, $\Delta=2$, and SER=10^{-2}

evaluate normalized non-zero-mean-ratio. From the figure, it is inferred that for $[m,p]=[8,285]$, $\mu'(m,p)$ reaches minimum compared to other possible combinations. Hence, m_{est} and p_{est} are identified successfully. From $m_{\text{est}}=8$, codeword length $n_{\text{est}}=255$ is recognized correctly. Further, from the number of roots of generator polynomial, $n_{\text{est}}-k_{\text{est}}$ has been estimated. From $n_{\text{est}}-k_{\text{est}}$, the code dimension $k_{\text{est}}=127$ has been recognized correctly.

Similarly, the variation of $\mu'(m,p,\phi)$ with respect to $[m,p,\phi]$, where $m\in[3\ ,\ 5]$ and ϕ denotes the bit position adjustment parameter, is shown in Fig. 8(b) assuming RS$(31,15,5,37)$, 16-QAM scheme (i.e. $M=16$ and $M_1=4$), $\Delta=2$, $\chi=1$, and SER = 10^{-2}. From the plot, it is inferred that $\mu'(m,p,\phi)$ reaches minimum at $[m,p,\phi]=[5,37,151]$. Therefore, the RS code parameters $m_{\text{est}}=5$, $n_{\text{est}}=31$, and $p_{\text{est}}=37$ are estimated successfully using Algorithm 2. Further, the number of roots of generator polynomial is also estimated and is given by $n_{\text{est}}-k_{\text{est}}=16$. The code dimension $k_{\text{est}}=15$ is recognized correctly from $n_{\text{est}}-k_{\text{est}}$. Finally, the adjustment of bit position to achieve synchronization (i.e. $\phi_{\text{est}}=151$) is also identified correctly using Algorithm 2.

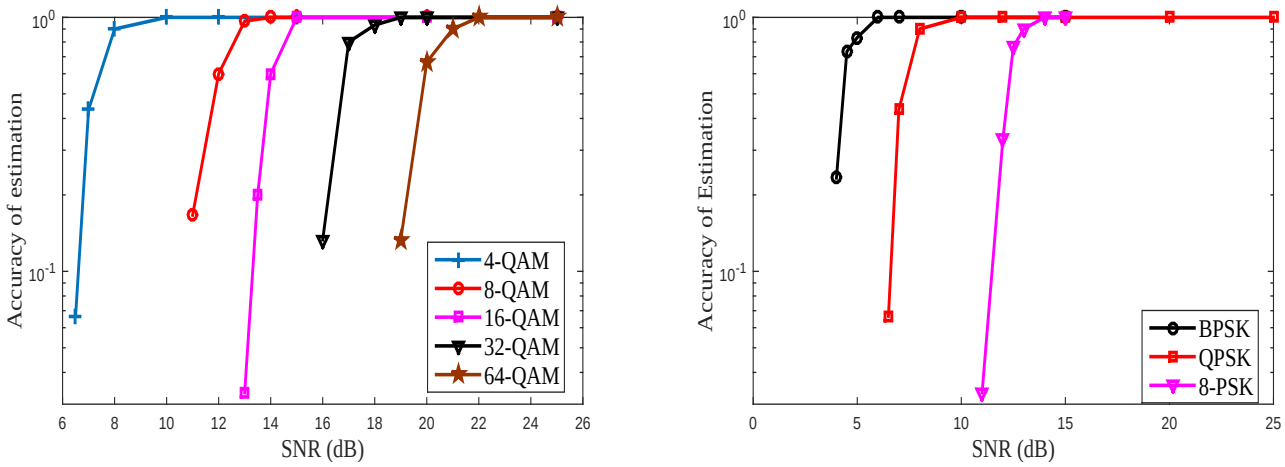
In Fig. 9(a) and 9(b), the accuracy of estimation of RS codes considering RS$(15,9,4,19)$ is given for various M-QAM and M-PSK schemes by varying the SNR value. It is to be noted that additive white Gaussian noise (AWGN) is considered. Here, it can be observed that as the modulation order decreases, improvement in the accuracy of estimation is observed, as expected.

In Fig. 10(a), the accuracy of estimation of RS codes assuming $n=15$, $m=4$, and $p=19$ with 16-QAM scheme is given for different code dimension values by varying the SER value. From the plots, it can be observed that the accuracy of estimation of RS code parameters deteriorates with increase in the value of k or r. As r increases, it is always difficult to classify rank-deficient and full-rank data matrices based on $\mu'(m,p,\phi)$ due to less number of dependent columns (i.e. $n-k$). In Fig. 10(b), the accuracy of estimation plot by varying the SER value is given for different RS codes such as RS$(63,45,6,67)$, RS$(31,23,5,37)$, and RS$(15,11,4,19)$ for 16-QAM scheme assuming code rate $r\approx0.7$. From the plots, it is inferred that the accuracy of estimation deteriorates as n increases.

B. Simulation results for estimation of interleaver parameters

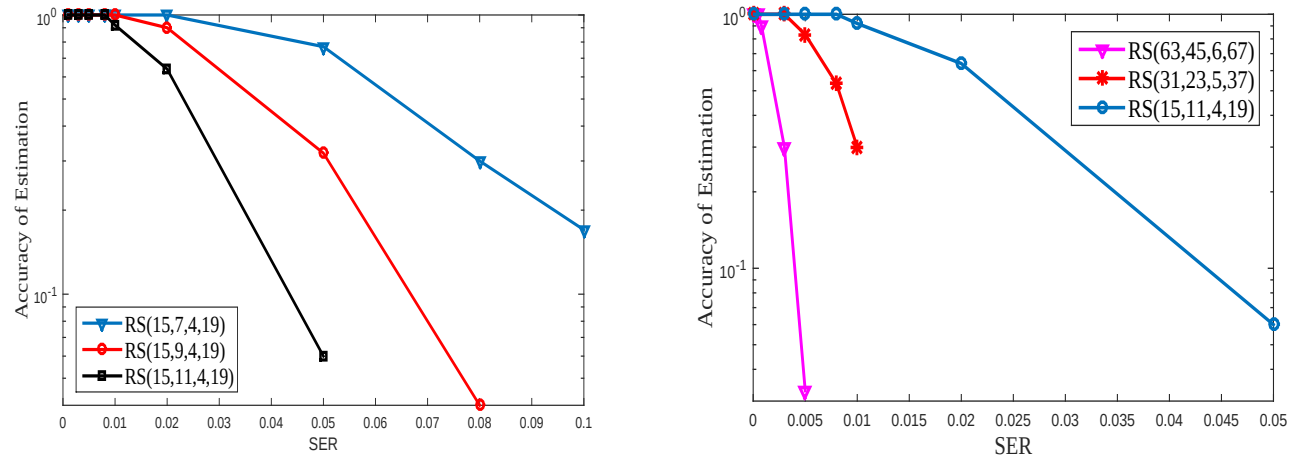
According to Algorithm 4, the variation of normalized non-zero-mean-ratio $\mu'(m,p,b)$ with respect to $[m,p,b]$, where b denotes the number of columns of data matrix S, is shown in Fig. 11(a) for RS$(7,3,3,11)$ considering matrix-based block interleaver assuming interleaver period $\beta=105$, $N_r=15$, $N_c=7$, 8-PSK constellation, $\Delta=4$, and SER=8×10^{-3}. Firstly, from the plot it is inferred that at $[m,p,b]=[3,11,105]$, $\mu'(m,p,b)$ reaches global minimum and hence, interleaver period $\beta_{\text{est}}=105$ (i.e. $b_{\text{est}}=105$) is estimated correctly. Moreover, the RS code parameters $m_{\text{est}}=3$, $n_{\text{est}}=2^3-1=7$, and $p_{\text{est}}=11$ are also recognized successfully. Since β is a multiple of n, $\zeta_{\text{est}}=\beta$ is estimated using Algorithm 4. In Fig. 11(b), the variation of normalized non-zero-mean-ratio by fixing $b=n_{\text{est}}$ is given for the same case as assumed in Fig. 11(a). According to Algorithm 5, the normalized non-zero-mean-ratio $\mu'(N_r',N_c',\phi')$ is evaluated for all possible values of $[N_r',N_c',\phi']$. From the figure, it is observed that at $[N_r',N_c',\phi']=[15,7,102]$, $\mu'(N_r',N_c',\phi')$ achieves minimum. Therefore, by shifting 102 symbol positions (i.e. $(\chi'\zeta_{\text{est}}+1)-\Delta$ positions, where $\chi'=1$), time synchronization is achieved and with $N_r^{\text{est}}=15$ and $N_c^{\text{est}}=7$, the block interleaved data symbols can be successfully de-interleaved. Hence, from Fig. 11(a) and Fig. 11(b), the matrix-based block interleaver and synchronization parameters are estimated correctly.

In Fig. 12(a), the variation of $\mu'(m,p,b)$ with respect to $[m,p,b]$ is shown for RS$(15,7,4,19)$ with helical scan interleaver assuming $N_r=5$, $N_c=2$, $d=4$, 16-PSK constellation, and SER=10^{-2}. From the figure, it can be observed that $\mu'(m,p,b)$ reaches global minimum for the case



(a) (b)

Fig. 9. (a) Accuracy of estimation of RS codes RS$(15, 9, 4, 19)$ for different M-QAM schemes by varying the average SNR value (b) Accuracy of estimation of RS codes RS$(15, 9, 4, 19)$ for different M-PSK schemes by varying the average SNR value



(a) (b)

Fig. 10. (a) Accuracy of estimation of RS codes considering $n = 15$, $m = 4$, and $p = 19$ with 16-QAM scheme for different values of code dimension k. (b) Accuracy of estimation of RS codes with 16-QAM scheme for different values of codeword length n

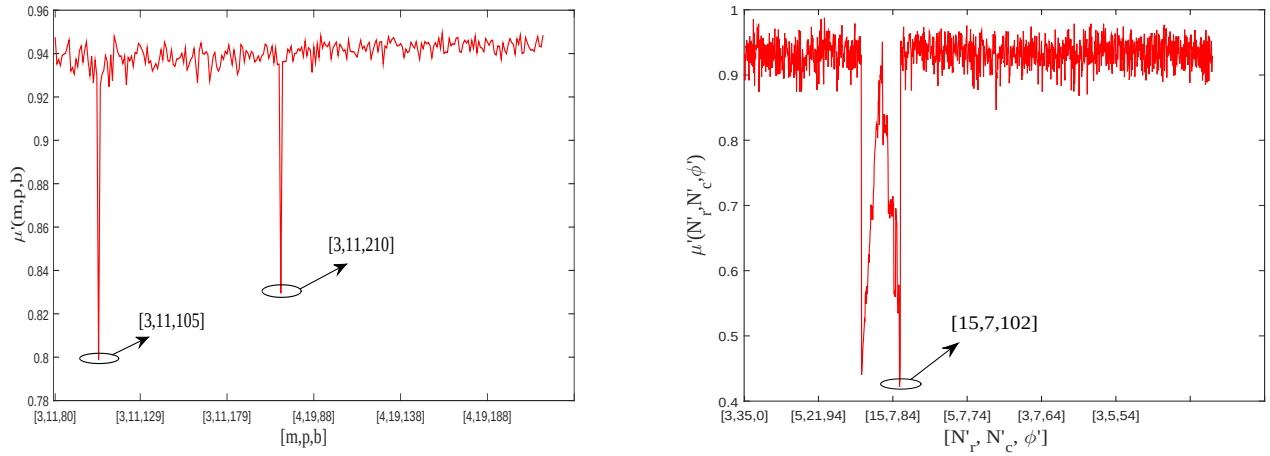
when $[m, p, b] = [4, 19, 30]$. Hence, $\zeta_{\text{est}} = \text{lcm}(n, \beta) = 30$, $m_{\text{est}} = 4$, $p_{\text{est}} = 19$, and $n_{\text{est}} = 2^4 - 1 = 15$ are estimated successfully using Algorithm 4. Since $\beta = 10$ is not a multiple of $n = 15$, $\zeta_{\text{est}} = \text{lcm}(n, \beta)$ is recognized using Algorithm 4. Moreover, in Fig. 12(b), the variation of $\mu'(N_r', N_c', d, \phi')$ with respect to $[N_r', N_c', d, \phi']$ is shown for the same case. From the figure, it is observed that for $[N_r', N_c', d, \phi'] = [5, 2, 4, 14]$, $\mu'(N_r', N_c', d, \phi')$ achieves minimum and hence, all the helical scan interleaver and synchronization parameters are successfully estimated using Algorithm 4 and 5.

In Fig. 11(a) and Fig. 12(a), the corresponding $[m, p, b]$ values for which $\mu'(m, p, b)$ reaches global minimum gives the actual RS code parameters and block interleaver period. However, in some cases, we observe local minimum points due to deficient rank values. For example, a local minimum point is observed when $b = 210$ in Fig. 11(a) and few local minimum points are observed in Fig. 12(a) when $b = 60, 90,$ and 120. This observation is useful in validating the interleaver period. This is because, the interleaver period can also be estimated by observing the difference between successive number of columns with lower values of $\mu'(m, p, b)$. For example, β_{est} in Fig. 11(a) can also be identified by observing the difference between successive number of columns with lower values of $\mu'(m, p, b)$.

In Fig. 13, the accuracy of estimation of block interleaver parameters over RS codes is shown by varying the SNR value considering $N_r = 5$ and $N_c = 6$ for different $M-$QAM schemes. It has been noticed from the figure that as M increases, the estimation accuracy deteriorates, as expected.

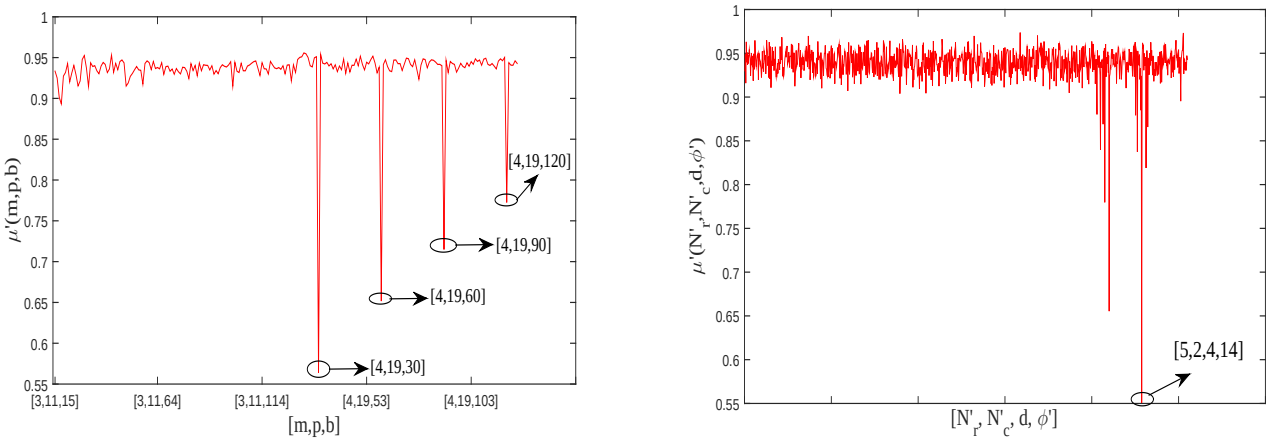
C. Performance comparison of proposed algorithms with prior works

The performance comparison of the proposed algorithm for RS codes over erroneous scenario (i.e. Algorithm 2) with the LLR-based methodology reported in [4] is shown in Fig. 14.



(a) (b)

Fig. 11. (a) Variation of $\mu'(m,p,b)$ with $[m,p,b]$ for RS$(7,3,3,11)$ and matrix-based block interleaver assuming $N_r=15$, $N_c=7$, 8-PSK scheme, $\Delta=4$, and SER=8×10^{-3}. (b) Variation of $\mu'(N'_r,N'_c,\phi')$ with $[N'_r,N'_c,\phi']$ for RS$(7,3,3,11)$ assuming $N_r=15$, $N_c=7$, 8-PSK scheme, $\Delta=4$, and SER=8×10^{-3}



(a) (b)

Fig. 12. (a) Variation of $\mu'(m,p,b)$ with $[m,p,b]$ for RS$(15,7,4,19)$ and helical scan interleaver assuming $N_r=5$, $N_c=2$, $d=4$, 16-PSK scheme, $\Delta=17$, and SER=10^{-2} (b) Variation of $\mu'(N'_r,N'_c,d,\phi)$ with $[N'_r,N'_c,d,\phi]$ for RS$(15,7,4,19)$ and helical scan interleaver assuming $N_r=5$, $N_c=2$, $d=4$, 16-PSK scheme, $\Delta=17$, and SER=10^{-2}

Here, the probability of correct detection of two RS codes namely RS$(15,7,4,19)$ and RS$(31,19,5,37)$ assuming 16-QAM and 32-QAM schemes, respectively, are compared. It is noticed from the performance curves that the proposed algorithm outperforms the LLR-based methodology. The LLR approach proposed in [4] estimates the true RS encoder with 100% and 40% accuracy for RS$(15,7,4,19)$ when SNR$\geq$20 dB and SNR $=15$ dB, respectively. On the other hand, our algorithm can successfully recognize RS code parameters with 100% accuracy when SNR≥15 dB.

The probability of correct detection of RS code RS$(15,7,4,19)$ using Algorithm 2 is also compared with the Barbier's method [18] for different SER values in Table II. The Barbier's method is based on recognizing potential dual-codewords and estimating the code parameters that maximize the rank of a matrix, whose rows are dual-codewords. In our algorithm, RS code parameters are identified based on deficient rank and normalized non-zero-mean-ratio values. It is inferred from the tabulated values that for SER $=0.075$ and SER$=0.1$, improvement in the accuracy of estimation of code parameters is obtained using Algorithm 2 compared to the algorithm proposed in [18]. In Table III, the probability of correct detection of interleaver period $\beta=21$ using Algorithm 4 is compared with the interleaver period estimation algorithm proposed in [22] for different bit error rate (BER) values. From the tabulated values, improvement in the probability of correct detection of interleaver period is noticed using Algorithm 4 for all the BER values compared to the algorithm proposed in [22]. Note that the algorithm in [22] is proposed to estimate only interleaver period based on evaluating the mean or variance of number of zero elements of column echelon form F crossing a particular threshold value $1/M_2$,

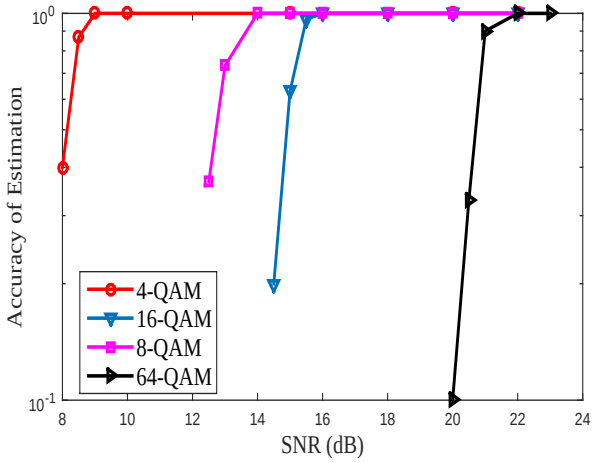


Fig. 13. Accuracy of estimation of block interleaver parameters over RS code RS$(15, 9, 4, 19)$ by varying the SNR value considering $N_r = 5$ and $N_c = 6$ for different $M-$QAM schemes

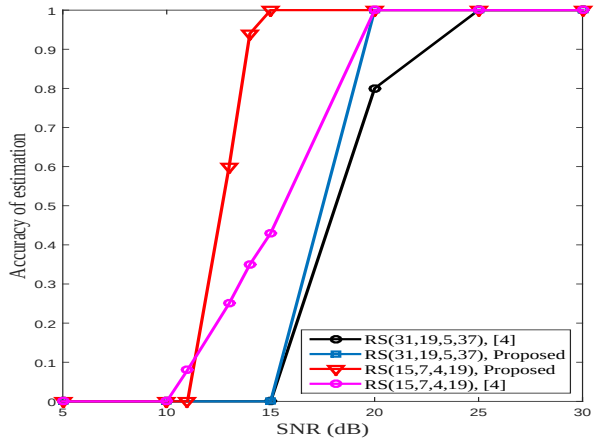


Fig. 14. Performance comparison of Algorithm 2 with the algorithm proposed in [4]

where M_2 denotes number of non-binary symbols.

Finally, the proposed algorithms after slight modification can also be extended to shortened RS codes. However, the simulation results are not provided due to space constraints.

V. Conclusions

In this paper, the blind estimation algorithms are proposed for estimating RS code and block interleaver parameters. The proposed algorithms are based on rank deficiency and normalized non-zero-mean-ratio values for noiseless and noisy environments, respectively. The bit/symbol positioning adjustment is also integrated with the proposed code and interleaver parameter estimation algorithms to achieve time synchronization. The simulation studies show that the proposed algorithms can successfully estimate RS code and block interleaver parameters for various test cases. Further, the accuracy of estimation plots are shown for different M-QAM and $M-$PSK schemes, code dimension, and codeword length values. It has been inferred that the accuracy of parameter estimation improves with decrease in code dimension and codeword length values.

TABLE II
Comparison of probability of correct detection of RS code RS$(15, 7, 4, 19)$

SER	Probability of correct detection ([18])	Probability of correct detection (proposed algorithm)
0.001	1	1
0.01	1	1
0.05	1	1
0.075	0.52	0.92
0.1	0	0.40

TABLE III
Comparison of probability of correct detection of interleaver period for RS code RS$(7, 3, 3, 11)$

BER	Probability of correct detection ([22])	Probability of correct detection (proposed algorithm)
0.006	0.85	1
0.009	0.37	1
0.015	0.1	1

Further, the lower modulation order schemes perform better then the higher modulation order schemes. It has also been noted that the proposed algorithm for noisy environment consistently outperforms the algorithms proposed in the prior works.

Appendix A
Case Study 1: RS code without interleaver

A case study explaining the rank deficiency and full rank phenomena considering RS code RS$(7, 3, 3, 11)$ without interleaver has been discussed for better understanding in this Appendix. Let us assume the non-binary input sequence $(t_1, t_2, t_3, t_4, \cdots)$ enters the systematic RS encoder RS$(7, 3, 3, 11)$ one symbol at a time. The RS codeword corresponding to the non-binary input sequence is given by $(t_1, t_2, t_3, g_1, g_2, g_3, g_4, \cdots)$, where g_1, g_2, g_3, and g_4 denote the parity symbols corresponding to the input sequence (t_1, t_2, t_3). Similarly, g_5, g_6, g_7, and g_8 denote the parity symbols corresponding to the input sequence (t_4, t_5, t_6). The RS encoded symbols are reshaped into a matrix S of size $a \times b$, where $b = 7, 10,$ and, 14 and $a = 3$ as shown in Table IV. From the reshaped coded data matrix, one complete codeword is noticed in all the three rows for the case when $b = 7$. Similarly, for the case when $b = 14$, two complete codewords are noticed. It is also observed that for both the cases, the data and parity symbols are aligned properly in the same column. For any linear block code including RS code, a codeword of length n bits/symbols depend only on k input message bits/symbols [17]. Therefore, $\alpha'.n$ output coded bits/symbols will depend on $\alpha' \cdot k$ input message bits/symbols. Hence, after converting S into F through finite field Gauss elimination process, only $\alpha' \cdot k = 3$ non-zero or independent columns will be observed for $b = 7$ and $\alpha' \cdot k = 6$ independent columns will be observed for $b = 14$. It is to be noted that $\alpha' = 1$ for $b = 7$ and $\alpha' = 2$ for $b = 14$. Since the number of independent columns gives the rank of a matrix, the corresponding rank values obtained for $b = 7$ and 14 well agree with (3) as well as Fig. 3(a).

TABLE IV
RS CODE RS$(7,3,3,11)$ RESHAPED INTO A DATA MATRIX S OF SIZE $3\times b$

$b=7$	t_1	t_2	t_3	g_1	g_2	g_3	g_4							
	t_4	t_5	t_6	g_5	g_6	g_7	g_8							
	t_7	t_8	t_9	g_9	g_{10}	g_{11}	g_{12}							
$b=10$	t_1	t_2	t_3	g_1	g_2	g_3	g_4	t_4	t_5	t_6				
	g_5	g_6	g_7	g_8	t_7	t_8	t_9	g_9	g_{10}	g_{11}				
	g_{12}	t_{10}	t_{11}	t_{12}	g_{13}	g_{14}	g_{15}	g_{16}	t_{13}	t_{14}				
$b=14$	t_1	t_2	t_3	g_1	g_2	g_3	g_4	t_4	t_5	t_6	g_5	g_6	g_7	g_8
	t_7	t_8	t_9	g_9	g_{10}	g_{11}	g_{12}	t_{10}	t_{11}	t_{12}	g_{13}	g_{14}	g_{15}	g_{16}
	t_{13}	t_{14}	t_{15}	g_{17}	g_{18}	g_{19}	g_{20}	t_{16}	t_{17}	t_{18}	g_{21}	g_{22}	g_{23}	g_{24}

TABLE V
RS CODE RS$(7,3,3,11)$ WITH BLOCK INTERLEAVER $N_r=7$ AND $N_c=3$ RESHAPED INTO A DATA MATRIX S OF SIZE $3\times b$

$b=21$	t_1	g_1	g_4	t_6	g_7	t_8	g_{10}	t_2	g_2	t_4	g_5	g_8	t_9	g_{11}	t_3	g_3	t_5	g_6	t_7	g_9	g_{12}			
	t_{10}	g_{13}	g_{16}	t_{15}	g_{19}	t_{17}	g_{22}	t_{11}	g_{14}	t_{13}	g_{17}	g_{20}	t_{18}	g_{23}	t_{12}	g_{15}	t_{14}	g_{18}	t_{16}	t_{21}	g_{24}			
	t_{19}	g_{25}	g_{28}	t_{24}	g_{31}	t_{26}	g_{34}	t_{20}	g_{26}	t_{22}	g_{29}	g_{32}	t_{27}	g_{35}	t_{21}	g_{27}	t_{23}	g_{30}	t_{25}	g_{33}	g_{36}			
$b=24$	t_1	g_1	g_4	t_6	g_7	t_8	g_{10}	t_2	g_2	t_4	g_5	g_8	t_9	g_{11}	t_3	g_3	t_5	g_6	t_7	g_9	g_{12}	t_{10}	g_{13}	g_{16}
	t_{15}	g_{19}	t_{17}	g_{22}	t_{11}	g_{14}	t_{13}	g_{17}	g_{20}	t_{18}	g_{23}	t_{12}	g_{15}	t_{14}	g_{18}	t_{16}	t_{21}	g_{24}	t_{19}	g_{25}	g_{28}	t_{24}	g_{31}	t_{26}
	g_{34}	t_{20}	g_{26}	t_{22}	g_{29}	g_{32}	t_{27}	g_{35}	t_{21}	g_{27}	t_{23}	g_{30}	t_{25}	g_{33}	g_{36}	t_{28}	g_{37}	g_{40}	t_{33}	g_{43}	t_{35}	g_{46}	t_{29}	g_{38}

Further, it is also observed that the rank deficiency is obtained only when b is a multiple of codeword length n i.e. $b=\alpha' \cdot n$. This is mainly due to proper alignment of the data and parity symbols in the same column and existence of linear relations between the columns of S.

Suppose, if $b \neq \alpha' \cdot n$, then it is noticed from the case when $b=10$ that the data and parity symbols are not properly aligned in the same column. Due to improper alignment, certain parity symbols of a particular codeword cannot be represented as a linear combination of input message symbols. For example, g_5, g_6, g_7, and g_8 in second row for $b=10$ case cannot be represented as a linear combination of message symbols t_4, t_5, and t_6. Due to this improper alignment, it is also noticed from Table IV that there are no linear relations between columns in S in contrast to the case when $b=7$ and $b=14$. Hence, data matrix S behaves like a random matrix, which will lead to full rank.

APPENDIX B
CASE STUDY 2: RS CODE WITH BLOCK INTERLEAVER

In this appendix, a case study explaining the rank deficiency and full rank phenomena considering RS code RS$(7,3,3,11)$ with block interleaver assuming $N_r=7$ and $N_c=3$ has been discussed for better understanding. The systematic RS encoded data symbols are interleaved using matrix-based block interleaver. After block interleaving, the data symbols are reshaped into a matrix S of size $a \times b$ considering $b=21$ and 24 with $a=3$ as shown in Table V. It is to be noted that the matrix-based block interleaver operation is carried out as shown in Fig. 4. For simplicity without loss of generality only three rows of the block interleaved codewords are shown considering non-erroneous and synchronized case. From the interleaved data stream, three complete codewords are observed in all the three rows for the case when $b=21$. It is also observed that the data and parity symbols of three codewords in all the rows are aligned properly in the same column. We know that for RS code, a codeword of length n symbols depend on k information symbols. Hence, $\alpha' \cdot \gamma \cdot n$ output symbols should depend on $\alpha' \cdot \gamma \cdot k$ present input symbols. The case study in Table V is shown by considering interleaver period $\beta=\gamma \cdot n=21$. For the case when $b=\alpha' \cdot \beta=21$, we noted that $\alpha'=1$ and $\gamma=3$. Thus, $\alpha \cdot \gamma \cdot n=21$ output data symbols in a particular row will depend on $\alpha' \cdot \gamma \cdot k=9$ input symbols. Otherwise, $\alpha \cdot \gamma \cdot n$ data symbols will be a linear combination of $\alpha \cdot \gamma \cdot k$ data symbols Since the data and parity symbols in all the rows are aligned properly in the same column as shown in Table V, the linear relation will be satisfied in all the rows. Because of that there exist linear relations between columns of S. Thus, $b=21$ columns will be converted into $\alpha \cdot \gamma \cdot k=9$ non-zero or independent columns through finite field Gauss elimination process. As the number of independent columns in S or non-zero columns in F indicates the rank of the matrix, the corresponding rank value, which is equal to 9, obtained for $b=21$ well agree with (4).

However, for the case when $b=24$, it can be observed that the data and parity symbols are not aligned properly in the same column. Moreover, some parity symbols in the second row is moved to the first row. For example, the parity symbols g_{13} and g_{16}, which is generated as a linear combination of data symbols t_{10}, t_{11}, and t_{12}, are shifted to the first row. Similarly, g_{25} and g_{28}, which is generated as a linear combination of t_{19}, t_{20}, and t_{21}, are shifted to the second row unlike the case when $b=21$. Since the linear relations are not satisfied, the data matrix S behaves like a random matrix. Thus, after converting S into F, full rank will be observed.

REFERENCES

[1] J. F. Ziegler, "Automatic Recognition and Classification of Forward Error Correcting Codes," M.S. thesis, M.S. thesis, Dept. Elect. Comput. Eng., George Mason Univ., Fairfax, VA, USA, 2000.

[2] C. Choi and D. Yoon, "Enhanced blind interleaver parameters estimation algorithm for noisy environment," *IEEE Access*, vol. PP, no. 99, pp. 1-6, Early access.

[3] T. Xia and H.-C. Wu, "Novel blind identification of LDPC codes using average LLR of syndrome a posteriori probability," *IEEE Trans. Signal Process.*, vol. 62, no. 3, pp. 632–640, Feb. 2014.

[4] H. Zhang, H-C. Wu, and H. Jiang, "Novel blind encoder identification of Reed-Solomon codes with low computational complexity," *in Proc. IEEE GLOBECOM*, 2013, pp. 3294–3299.

[5] R. Moosavi and E. G. Larsson, "Fast blind recognition of channel codes," *IEEE Trans. Commun.*, vol. 62, no. 5, pp. 1393–1405, May 2014.

[6] M. Marazin, R. Gautier, and G. Burel, "Dual code method for blind recognition of convolutional encoder for cognitive radio receiver design," *in Proc. IEEE GLOBECOM*, 2009, pp. 1–6.

[7] M. Marazin, R. Gautier, and G. Burel, "Blind recovery of k/n rate convolutional encoders in a noisy environment," *EURASIP J. Wirel. Commun. and Netw.*, vol. 2011:168, pp. 1–9, 2011.

[8] G. L. Rosen, "Examining coding structure and redundancy in DNA," *IEEE Eng. Med. Biol. Mag.*, vol. 25, no. 1, pp. 62–68, Jan. 2006.

[9] J-P. Tillich, A. Tixier, N. Sendrier, "Recovering the interleaver of an unknown Turbo-Code," *in Proc. IEEE ISIT*, 2014, pp. 2784–2788.

[10] J. Dingel and J. Hagenauer, "Parameter estimation of a convolutional encoder from noisy observations," *in Proc. IEEE ISIT*, 2007, pp. 1776–1780.

[11] M. Marazin, R. Gautier, and G. Burel, "Some interesting dual-code properties of convolutional encoder for standards self-recognition," *IET Commun.*, vol. 6, no. 8, pp. 931–935, July 2012.

[12] Y. Zrelli, M. Marazin, R. Gautier, E. Rannou, and E. Radoi, "Blind identification of convolutional encoder parameters over GF(2m) in the noiseless case," *in Proc. IEEE ICCCN*, 2011, pp. 1–5.

[13] Z. Jing, H. Zhiping, S. Shaojing, and Y. Shaowu, "Blind recognition of binary cyclic codes," *EURASIP J. Wirel. Commun. Netw.*, vol. 2013:218, pp. 1–17, 2013.

[14] M. Cluzeau and M. Finiasz, "Reconstruction of punctured convolutional codes," *in Proc. IEEE ISIT*, 2009, pp. 75–79.

[15] M. Marazin, R. Gautier, and G. Burel, "Algebraic method for blind recovery of punctured convolutional encoders from an erroneous bit stream," *IET Signal Process.*, vol. 6, no. 2, pp. 122–131, April 2012.

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

[17] Y. Zrelli, M. Marazin, R. Gautier, E. Rannou, and E. Radoi, "Blind identification of code word length for non-binary error-correcting codes in noisy transmission," *EURASIP J. Wirel. Commun. Netw.*, vol. 2015:43, pp. 1–16, 2015.

[18] A. Zahedi and G-R. Mohammad-Khani, "Reconstruction of a non-binary block code from an intercepted sequence with application to Reed-Solomon codes," *IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences*, VOL.E95-A, no. 11, pp. 1873–1880, Nov. 2012.

[19] G. Sicot, S. Houcke, and J. Barbier, "Blind detection of interleaver parameters," *Signal Process.*, vol. 89, pp. 450–462, April 2009.

[20] Swaminathan R, A. S. Madhukumar, N. W. Teck, and S. C. M. Samson, "Parameter estimation of block and helical scan interleavers in the presence of bit errors," *Digital Signal Process.*, vol. 60, pp. 20–32, Jan. 2017.

[21] G. Golub and C. F. V. Loan, *Matrix computations*, 3rd ed. Baltimore, MD, USA: Johns Hopkins Univ. Press, 1996.

[22] L. Lu, K. H. Li, and Y. L. Guan, "Blind detection of interleaver parameters for non-binary coded data streams," *in Proc. IEEE ICC*, 2009, pp. 1–4.

[23] L. Lu, K. H. Li, and Y. L. Guan, "Blind identification of convolutional interleaver parameters," *in Proc. IEEE ICICS*, 2009, pp. 1–5.

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

[25] Y-Q. Jia, L-P. Li, Y-Z. Li, and L. Gan, "Blind estimation of convolutional interleaver parameters," *in Proc. IEEE WiCOM*, 2012, pp. 1–4.

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

[27] "Digital video broadcasting (DVB); Framing structure, channel coding and modulation for digital terrestrial television," ETSI, Sophia Antipolis, France, Tech. Rep. EN 300 744 V1.6.1 (2009-01), 2009.

[28] C. Shin, R. W. Heath, E. J. Powers, "Blind channel estimation for MIMO-OFDM systems," *IEEE Trans. Veh. Technol.*, vol. 56, no. 2, pp. 670-685, Mar. 2007.

[29] H. H. Zeng and L. Tong, "Blind channel estimation using the second-order statistics: algorithms," *IEEE Trans. Signal Process.*, vol. 45, no. 8, pp. 1919-1930, Aug. 1997.