Automatic Recognition of FEC Code and Interleaver Parameters in a Robust Environment

Swaminathan R*, ***A. S. Madhukumar*, Wang Guohua^, and Ting Shang Kee^***
**School of Computer Science and Engineering*
^Temasek Laboratories
Nanyang Technological University Singapore

Email : sramabadran@ntu.edu.sg

Outline of the Presentation

- Classification of Error Correcting Codes and Estimation of Interleaver Parameters
  - Introduction
  - Parameter estimation : Non-erroneous scenario
  - Code classification
  - Parameter estimation : Erroneous scenario
  - Simulation Results

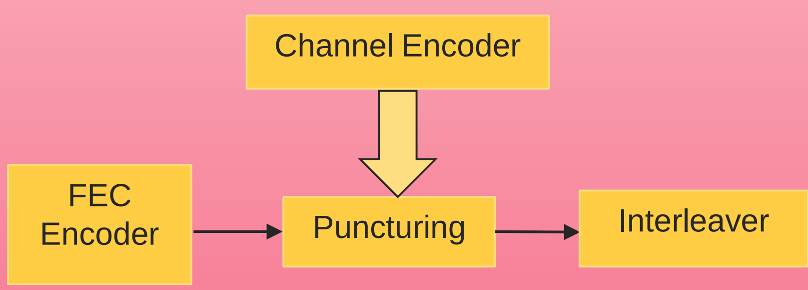
- Blind Reconstruction of Reed-Solomon Encoder and Interleavers Over Noisy Environment
  - Introduction
  - RS Code Parameter Estimation Algorithms
  - Joint RS code and Interleaver Parameter Estimation Algorithms
  - Simulation Results

Part 1: Classification of Error Correcting Codes and Estimation of Interleaver Parameters

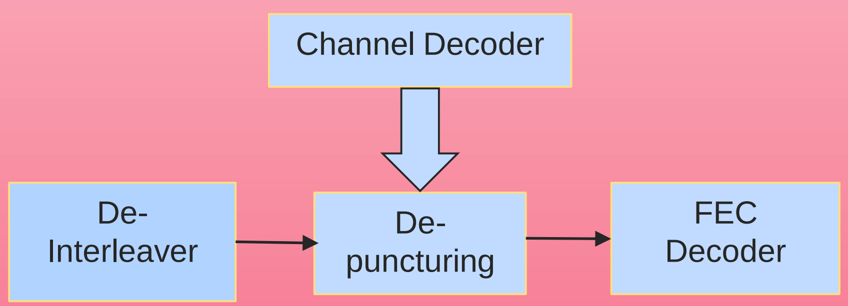
Swaminathan R and A.S.Madhukumar, ``Classication of error correction codes and estimation of interleaver parameters in a robust environment'', IEEE Transactions on Broadcasting, vol. 63, no. 3, pp. 463 - 478, Sept. 2017.

Introduction

- Channel encoding/decoding have become an integral part of modern digital communication systems
- Efficient encoding and decoding methods have been proposed to control and correct the errors introduced by the noisy channel
- Interleaver plays a vital role in communication and storage systems to distribute the burst errors



Channel Encoder



Channel Decoder

NANYANG TECHNOLOGICAL UNIVERSITY

Introduction

- Reconstructing an unknown code from the observation of noisy codewords problem is related to cryptanalysis
- This is called the code reconstruction problem in the literature
- An observer wants to extract information from a noisy data stream where the error correcting code used is unknown
- This problem arises in a non-cooperative context where observing a binary sequence originating from an unknown source
- Accurate information about the parameters of encoding scheme is required at the receiver to decode FEC codes
- Non-cooperative scenario: Parameters are either not known or only partially known at the receiver
- Applications:
  - Military and spectrum surveillance system,
  - Signal intelligence (SIGINT) (intelligence gathered by interception of signals)
  - Adaptive modulation and coding (AMC)
  - Cognitive radio

NANYANG TECHNOLOGICAL UNIVERSITY

Introduction

- Military surveillance may involve decoding an adversary's received data when the underlying channel code is not known
- AMC communication systems: Control channel will signal the AMC parameters to the receiver
- Blind recognition lead to conservation of channel resources
- AMC Wireless sensor networks (WSNs) : Reduces transmission overheads and total energy consumption of WSNs
- Designing separate decoder for every application is a costly and a tedious process
- It is essential to design an intelligent receiver system which adapts itself to any applications

Motivations

The main motivations are given as follows:

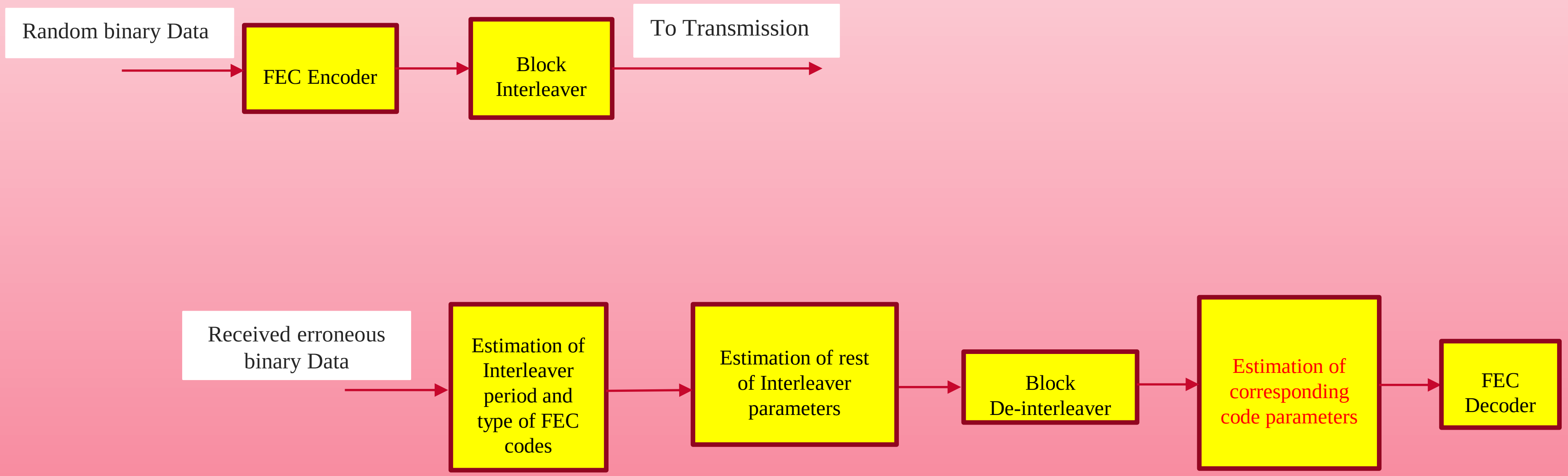
- It is essential to blindly reconstruct channel encoder using the intercepted sequences acquired from remote sensing through aircraft and satellite
- Code classification techniques were proposed only for non-erroneous scenario
- Code classification algorithm to classify among block, convolutional coded and uncoded has not been proposed
- Previously proposed block interleaver parameter estimation algorithms were restricted only to estimation of interleaver period

Contributions

The main contributions are as follows:

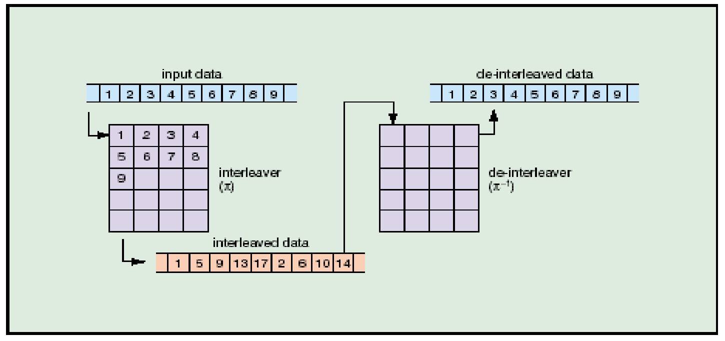
- Automatic recognition of type of FEC codes
- To differentiate among block coded, convolutionally coded, and uncoded data, algorithm is proposed for noisy scenario
- Algorithm is also given for estimating code and Interleaver parameters
- Code dimension k and Codeword length n are the estimated code parameters of block and convolutional codes
- Interleaver period β, Number of columns (N_c), and Number of rows (N_r) are the estimated matrix-based block interleaver parameters in the presence of bit errors
- Discussion is restricted to matrix-based block interleaver

Generic Block Diagram



Block Interleaver

- Error correcting codes provide protection against random errors and interleaver provides protection against error bursts
- A block interleaver receives a block of symbols rearranges them without removing any of the symbols
- Matrix-based block interleaver stores each block of data symbols row-wise and sends column-wise for transmission
- Interleaver period information alone is not sufficient to de-interleave the data stream
- The size of the interleaver matrix or interleaver period is given by $\beta = N_r \times N_c$, N_r - Number of rows and N_c - Number of Columns



Block Interleaver/de-interleaver

Parameter Estimation: Non-erroneous

Code classification (with interleaver) without the presence of bit errors:

- This can be done by using Rank-based methodology
- Reshape the column wise intercepted data stream into a matrix form of size $a \times b$, where a = $2 \times b$
- The rank of the data matrix S in GF (2) is computed by varying the number of columns b using Gauss elimination process

Convolutional Code:

- If $\beta = \gamma . n$ and while varying b, if $b = \alpha . \beta$, where α and γ are positive integers, then rank deficiency will be observed and Rank $\boldsymbol{\rho}$(S) = $\alpha . \gamma . k + m$ and rank ratio $p = \frac{\boldsymbol{\rho}(\mathrm{S})}{b} = r + \delta$, where $\delta \rightarrow 0$ as $b \rightarrow \infty$
- If $\beta \neq \gamma . n$ and while varying b, if $b = \alpha . lcm(n, \beta)$, then rank deficiency will be observed and $\boldsymbol{\rho}$(S) = $\alpha . \gamma . k + m$
- For the case when $b \neq \alpha . \beta$ and $b \neq \alpha . lcm(n, \beta)$, the data matrix will have full rank i.e. $\boldsymbol{\rho}$(S) = b and $p = 1$

Parameter Estimation: Non-erroneous

Block Code :

- If $\beta = \gamma.n$ and while varying b, if $b = \alpha.\beta$, then rank deficiency will be observed and $\boldsymbol{\rho}(S) = \alpha.\gamma.k$ and rank ratio $p = \frac{\boldsymbol{\rho}(S)}{b} = r$
- If $\beta \neq \gamma.n$ and while varying b , if $b = \alpha.lcm(n, \beta)$, then rank deficiency will be observed and $\boldsymbol{\rho}(S) = \alpha.\gamma.k$
- For the case when $b \neq \alpha.\beta$ and $b \neq \alpha.lcm(n, \beta)$, the data matrix will have full rank i.e. $\boldsymbol{\rho}(S) = b$ and $p = 1$.

Uncoded:

- Irrespective of the value of b, full rank will be obtained and rank ratio will be unity.

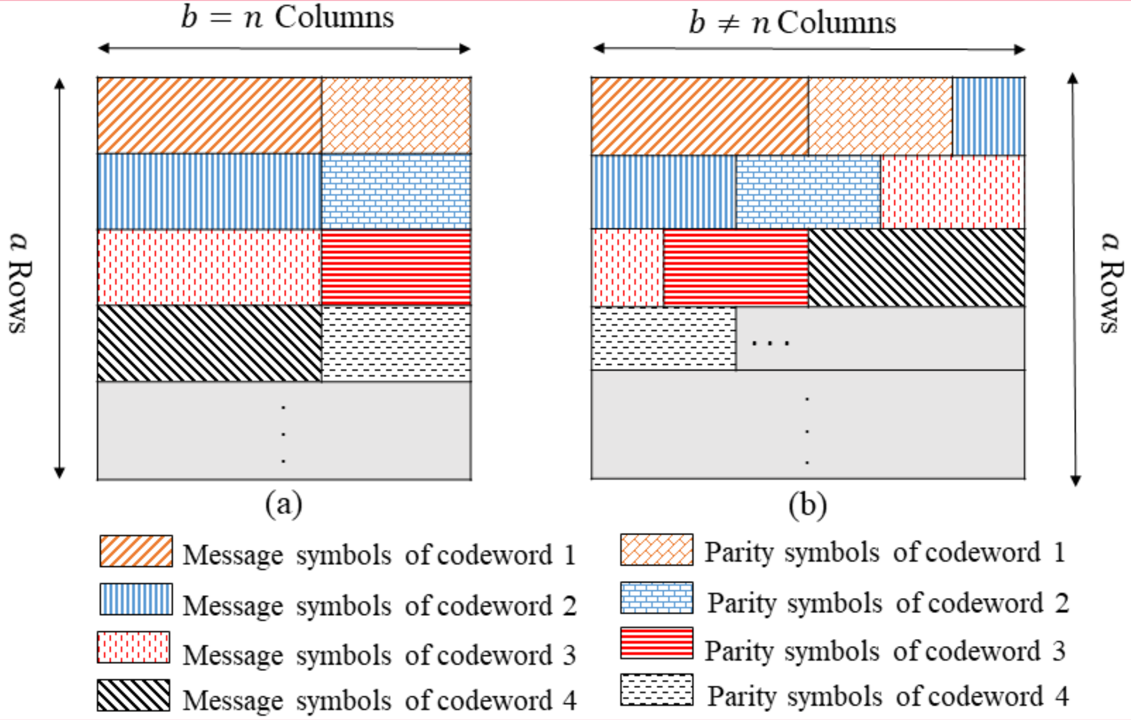
Parameter Estimation: Non-erroneous

Reason for rank deficiency:

- n output convolutionally coded data symbols depend on k present and m previous input uncoded data symbols
- $\alpha . n$ output coded data symbols depend on $\alpha . k$ present and m previous input uncoded symbols (i.e. $\alpha . k + m$ symbols)
- If convolutionally coded data is block interleaved and if $b = \alpha \times \beta$ with $\beta = \gamma \times n,$ then $\alpha . \gamma$ codewords in a particular row will depend on $\alpha . \gamma . k + m$ symbols
- It is also applicable to all other rows of *S*
- For block codes, it is to be noted that n output coded data symbols depend only on k input uncoded data symbols unlike convolutional codes, since $m = 0$
- The message and parity bits of $\alpha . \gamma$ codewords in all the rows will be properly aligned in the same column

Parameter Estimation: Non-erroneous

- After converting S into F through Gauss elimination process, when $b = \alpha \times \beta$, there will be only $\alpha.\gamma.k + m$ non-zero or independent columns out of b columns
- Hence, the deficient rank value is obtained



Parameter Estimation: Non-erroneous

Convolutional Code

- The inequality $\alpha.\gamma.k + m < b$ holds true or the rank deficiency can be obtained only when $\alpha \geq \alpha_{\text{min}}$ or $b \geq b_{\text{min}}$
- The expressions for α_{min} and b_{min} are derived as follows: After substituting $b = \alpha.\gamma.n$, the inequality can be written as

$$\alpha.\gamma.k + m < \alpha.\gamma.n$$

After rearranging,

$$\alpha.\gamma.n.\left(1 - \frac{k}{n}\right) > m$$

$$\alpha.\gamma.n > \frac{n}{n-k} m$$

$$\alpha > \frac{m}{\gamma.(n-k)}$$

The minimum value of α, denoted by α_{min}, is given by

$$\alpha_{\text{min}} = \text{floor}\left(\frac{m}{\gamma.(n-k)}\right) + 1$$

b_{min} is given by

$$b_{\text{min}} = \alpha_{\text{min}}.\beta$$

Block codes:

- The inequality $\alpha.\gamma.k < b$, where $b = \alpha.\gamma.n$, remains true irrespective of α, since $k < n$
- Hence, $\alpha_{\text{min}} = 1$ and $b_{\text{min}} = \beta$ for block codes

Parameter Estimation: Non-erroneous

Estimation of code rate r and interleaver period β:

- Interleaver period β (i.e. for the case when β is a multiple of n) or $\mathrm{lcm}(n, \beta)$ (i.e. for the case when β is not a multiple of n) can be identified by observing the difference between the successive number of columns with rank deficiency

- Let $b = \alpha.\gamma.n$ and $b' = (\alpha+1).\gamma.n$ indicate the two rank deficient columns and their difference is given by

$$\begin{aligned} b' - b &= (\alpha+1).\gamma.n - \alpha.\gamma.n \\ &= \gamma.n \\ &= \beta \text{ or } \mathrm{lcm}(n, \beta) \end{aligned}$$

- The difference between two successive rank deficient values $\rho(S)$ and $\rho'(S)$ is given by

$$\begin{aligned} \rho'(S) - \rho(S) &= ((\alpha+1).\gamma.k + m) - (\alpha.\gamma.k + m) \\ &= \gamma.k \end{aligned}$$

- The code rate r can be estimated as follows:

$$\frac{\rho'(S) - \rho(S)}{b' - b} = r$$

- For block codes, the above steps are applicable for estimating r by assuming $m = 0$.

NANYANG TECHNOLOGICAL UNIVERSITY

Parameter Estimation: Non-erroneous

Convolutional Code (without interleaver):

- While varying b, if $b = \alpha.n$ and $b > b_{min}$, then rank deficiency will be observed and Rank $\boldsymbol{\rho}$(S) = $\alpha.k + m$ and rank ratio $p = \frac{\boldsymbol{\rho}(S)}{b} = r + \delta$
- If $b \neq \alpha.n$ or $b < b_{min}$, the data matrix will have full rank i.e. $\boldsymbol{\rho}$(S) = b and $p = 1$

Block Code (without interleaver)

- If $b = \alpha.n$, then $\boldsymbol{\rho}$(S) = $\alpha.k$ and rank ratio $p = \frac{\boldsymbol{\rho}(S)}{b} = r$
- If $b \neq \alpha.n$, then $\boldsymbol{\rho}$(S) = b and $p = 1$

- $b = \alpha \times n$ and $b' = (\alpha + 1) \times n$ indicate the two rank deficient columns and the difference $b' - b$ gives the value of codeword length n.
- The difference between rank values corresponding to rank deficient columns gives the estimate of code dimension k.

Uncoded

- While varying b, full rank will be obtained irrespective of b, as the incoming uncoded symbols are independent of each other

Parameter Estimation: Non-erroneous

TABLE I
MINIMUM NUMBER OF COLUMNS REQUIRED TO OBTAIN THE FIRST RANK DEFICIENT MATRIX FOR DIFFERENT CONVOLUTIONAL CODES

No.	Code rate (r)	n	k	Y	$b_{\min}$	g_i^j
1	1/2	2	1	3	6	[5,7]
2				4	8	[15,17]
3				5	10	[23,35]
4				6	12	[65,57]
5				6	12	[75,53]
6				7	14	[133,171]
7				8	16	[345,237]
8				9	18	[561,753]
9				10	20	[1167,1545]
10				11	22	[2335,3661]
11	1/3	3	1	4	6	[13,15,17]
12				7	12	[133,165,171]
13				10	15	[1117,1365,1633]
14	1/4	4	1	7	12	[133,171,117,165]

NANYANG TECHNOLOGICAL UNIVERSITY

Code Classification

- The incoming data symbols with or without interleaver can be classified easily from the rank ratio equations

Convolutional Code:

- The deficient rank ratio will be much greater than r for lower values of b.
- As b increases, deficient rank ratio will tend to remain constant slightly above r
- Deficient rank ratio will decay rapidly for smaller values of b
- For larger values of b, it will approximately remain constant slightly above r

Block Code:

- Deficient rank ratio will remain constant at r

Uncoded:

- Rank ratio will remain constant at unity for all values of b

Parameter Estimation: Erroneous

- The all-zero-column-based rank evaluation is limited to non-erroneous scenario
- Due to erroneous bits, dependent columns will not get converted into all-zero-columns
- This would result in full rank for both convolutional and block codes and code classification cannot be performed
- Erroneous scenario: Rank calculation will be performed based on the number of zeros in each columns
- Dependent and independent columns (rank) can be segregated
- Reason: If c^{th}column is dependent, then the number of zeros in that particular column will be smaller compared to the independent columns.

Parameter Estimation: Erroneous

- **Notations:** Let us denote the column echelon form of data matrix S_j as F_j, j denotes the iteration number, N denotes the number of iterations, $\omega_j(c)$ denotes the zero-ratio in c^{th} column of F_j, $\gamma(c)$ denotes the average of $\omega_j(c)$ over N iterations, and $data(\cdot)$ refers to an array of binary data symbols.
- $R_j = data(1 + (j-1)b \, : \, ba + (j-1)b)$
- Reshape R_j into a matrix S_j of size $a \times b$
- Convert S_j into F_j using Gauss elimination process
- Compute $\omega_j(c)$ in each column of F_j, where $c \in \{1, 2, ..., b\}$
- Form a row vector $A_j = [\omega_j(1) \, : \, \omega_j(b)]$
- Repeat the above steps for N iterations
- Accumulate all the row matrices into a single matrix A of size $N \times b$, where $A = [A_1 \, ; \, A_2 \, ; \, A_3 \, ; \cdots A_N]$
- Compute $B = mean(A)$, where $B = [\gamma(1) \, : \, \gamma(b)]$ and $\gamma(c) = \frac{\sum_{j=1}^{N} \omega_j(c)}{N}$
- Evaluate $\rho(b)$ as follows: $\rho(b) = \textbf{card}\left(c \in \{1, 2, ..., b\} \mid \gamma(c) < \Gamma^{\text{th}}\right)$ and $p(b) = \frac{\rho(b)}{b}$

Parameter Estimation: Erroneous

Matrix Size Estimation:

Step 1: ***Requires*** $\partial = lcm(n, \beta)$ or β and ***assumes*** $N_r{}'$ and $N_c{}' > 1$

Step 2: $for\ i = 1{:}\,n\_max$

$Get\ possible\ combinations\ of$
$two\ factors\ N_r{}'\text{and}\ N_c'$
$that\ satisfy\ N_r{}' \times N_c' = \frac{\partial}{i}$

end

Step 3: ***Fix Number of columns as a multiple of interleaver period (i.e.*** $\boldsymbol{Ncol = \alpha \times \partial, where\ \alpha > 1}$***)***

Step 4: ***De-interleave and evaluate mean of γ(c) for all possible values of*** $[N_r{}'\ N_c']$

Step 5: $[N_r^{est}, N_c^{est}] = \underset{N_r', N_c'}{argmax}(\mu'(b)), \text{ where } \mu'(b) = \frac{\sum_{c=1}^{b} \gamma(c)}{b}$

NANYANG TECHNOLOGICAL UNIVERSITY

Fixing Threshold: Analytical approach

- Data matrix S is converted into a column echelon form F using modified GJETP as follows: $S \cdot \chi = F$, where χ is a permutation matrix
- Columns in χ corresponding to all-zero columns in F is known as kernel of S i.e. $S.d = 0$, where $d = [d_1 d_2 \cdots d_b]^T$
- XOR of the column elements in S with column index i corresponding to $d_i = 1$ is equal to 0
- Otherwise, there should be even number of ones in the column positions of S corresponding to $d_i = 1$, such that $S.d = 0$
- **Erroneous scenario**: XOR of the column elements in S with index i corresponding to $d_i = 1$ will not be equal to zero due to odd number of ones
- The number of ones $\phi_j(c)$ in c^{th} dependent column of F_j is a RV denoted by B_c^j
- $\phi_j(c)$ follows a binomial distribution with parameters a and P_c^j (i.e. $B_c^j \sim \mathcal{B}(a, P_c^j)$), where P_c^j denotes the probability of getting ones in c^{th} dependent column of F_j

Fixing Threshold: Analytical approach

- The probability of getting ones in c^{th} dependent column of F_j is given by

$$
\begin{aligned}
P_c^j &= 1 - \sum_{l=0}^{floor\left(\frac{z_j^c}{2}\right)} \binom{z_j^c}{2l} p_e^{2l}\,(1-p_e)^{z_j^c-2l} \\
&= \frac{1-(1-2\,p_e)^{z_j^c}}{2},
\end{aligned}
$$

  where z_j^c denotes the hamming weight of c^{th} column in column permutation matrix χ_j and p_e denotes the BER value

- Binary symmetric channel (BSC) model is assumed for calculating the threshold value
- The number of ones $\phi_j(k)$ in k^{th} independent column of F_j is also a RV denoted by D_k^j and it follows $\mathcal{B}(a, P_k^{''})$
- $P_k^{''} = 0.5$. **Reason:** Probability of ones and zeros appearing in an independent column is equally likely
- For larger values of a, binomial RVs B_c^j and D_k^j can be approximated as normal RVs
- $B_c^j \sim \mathcal{N}(a.P_c^j, a.P_c^j.(1-P_c^j))$ and $D_k^j \sim \mathcal{N}(\frac{a}{2}, \frac{a}{4})$, where $\mathcal{N}(\mu, \sigma^2)$ denotes the normal distribution with mean μ and variance σ^2.
- The mean value of N different normal RVs B_c^j is also a RV denoted by μ_c
- μ_c also follows normal distribution with mean and variance $\frac{a\,q}{N}$ and $\frac{a\,r}{N^2}$, where $q = \sum_{j=1}^{N} P_c^j$ and $r = \sum_{j=1}^{N} P_c^j.(1-P_c^j)$
- Mean value of N different normal RVs D_k^j is denoted by μ_k' also follows normal distribution with mean and variance $\frac{a}{2}$ and $\frac{a}{4N}$

NANYANG TECHNOLOGICAL UNIVERSITY

Fixing Threshold: Analytical approach

- The probability of mis-detection of either dependent or independent column is given by

$$P_{\text{md}} = Pr\left(\frac{\mu_c}{a} > \Gamma^{\text{th}} \mid c^{\text{th}}\text{column is dependent}\right) + Pr\left(\frac{\mu'_k}{a} < \Gamma^{\text{th}} \mid k^{\text{th}}\text{column is independent}\right)$$

- By substituting the normal PDF

$$P_{\text{md}} = \int_{a\Gamma^{\text{th}}}^{\infty} \frac{N}{\sqrt{2\,\pi\,a\,r}} \exp\left(-\frac{N^2(\mu_c - \frac{a\,q}{N})^2}{2\,a\,r}\right) d\,\mu_c + \int_{-\infty}^{a\Gamma^{\text{th}}} \frac{\sqrt{2\,N}}{\sqrt{\pi\,a}} \exp\left(-\frac{2\,N(\mu'_k - \frac{a}{2})^2}{a}\right) d\,\mu'_k$$

- The expression for $\Gamma^{\text{th}}_{\text{opt}}$, which minimizes P_{md}, can be derived by differentiating P_{md} and equating it to zero
- After simplification, Γ^{th} is given by

$$\Gamma^{\text{th}}_{\text{opt}} = \frac{-\gamma - \sqrt{\gamma^2 - (\alpha\,\Delta)}}{\alpha}$$

where $\alpha = Na(4r - N)$, $\gamma = Na(q - 2r)$, and $\Delta = raN - aq^2 - r\ln\left(\frac{4r}{N}\right)$

- Exact BER value p_e need not be known to evaluate $\Gamma^{\text{th}}_{\text{opt}}$
- We can fix a maximum value for BER $p_e^{\max}$ depending upon the environment and calculate $\Gamma^{\text{th}}_{\text{opt}}$ $\rho(S)$
- The same optimal threshold values work well for the case when $p_e \le p_e^{\max}$.

NANYANG TECHNOLOGICAL UNIVERSITY

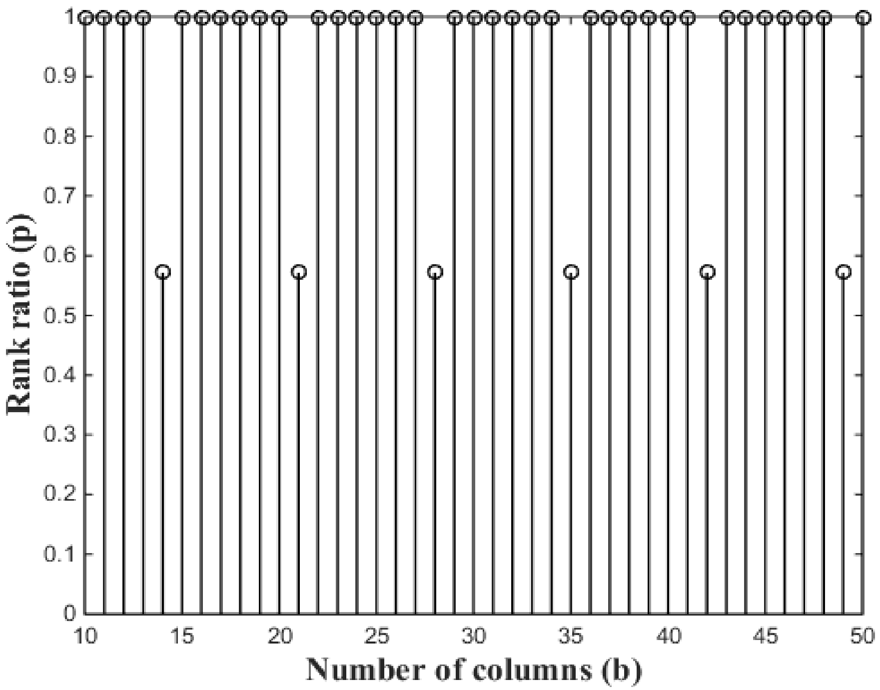
Fixing Threshold: Histogram approach

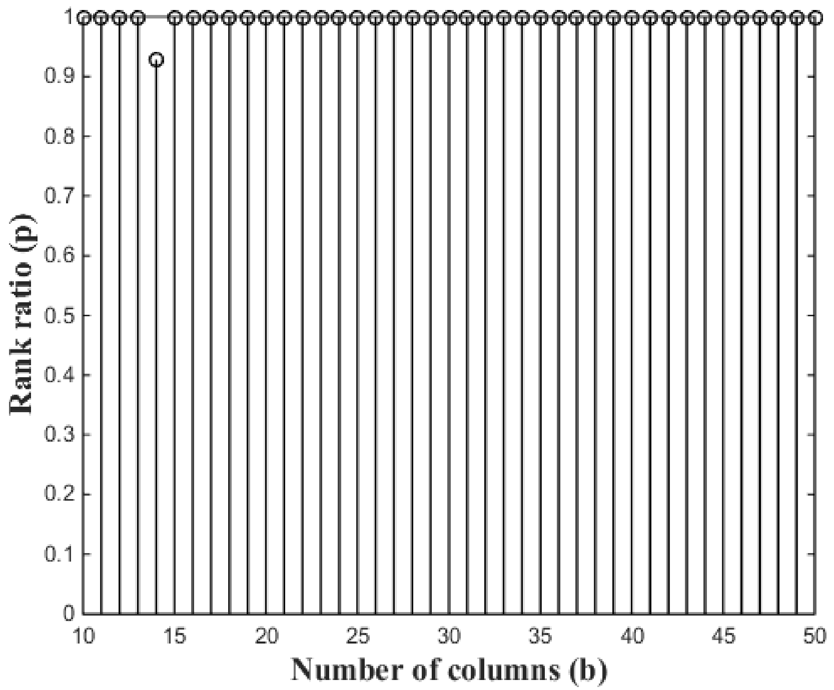
- The optimal threshold value can also be fixed by plotting the histogram for zero-ratio or non-zero-ratio
- A range of possible threshold values, which segregate the dependent and independent columns, is obtained
- From the range of possible values, a safe optimal threshold value is fixed
- The same optimal threshold value is applicable for all the other values of b to classify the dependent and independent columns

Simulation Results

- Various transmission standards specify the allowable BER for a given quality of service (QOS)
- For example, the post-FEC BER requirement for desirable operation of DVB receiver is 2×10^{-4}
- Considering the BER values together with the allowances of coding gain, the pre-FEC BER values for acceptable performance will be usually greater than 10^{-3}
- Considering these factors, we have taken a safe value of 10^{-2} as the BER threshold to account the worst case scenario
- The overall performance of the algorithm is extensively tested within the range of 5×10^{-3} to 6×10^{-2}

Simulation Results



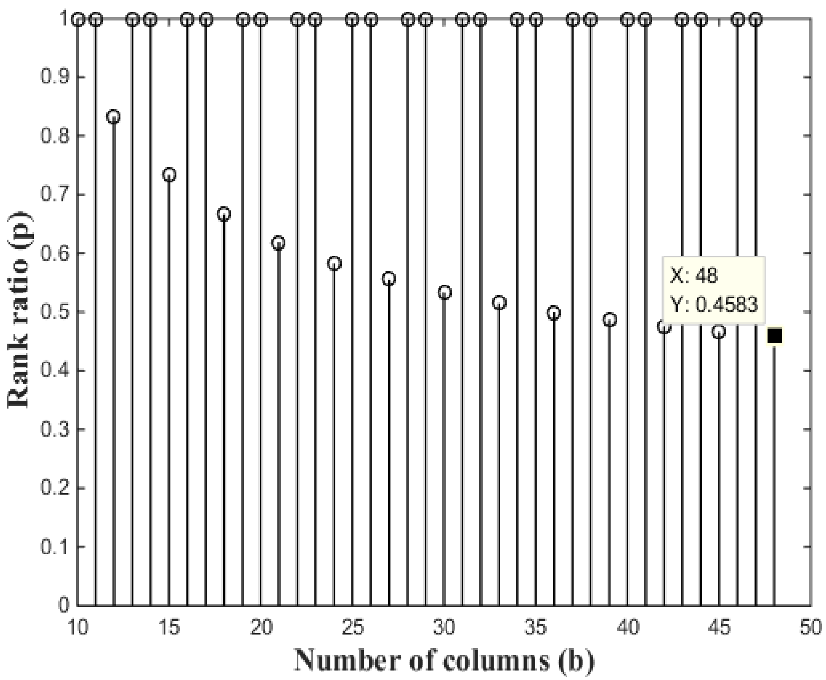


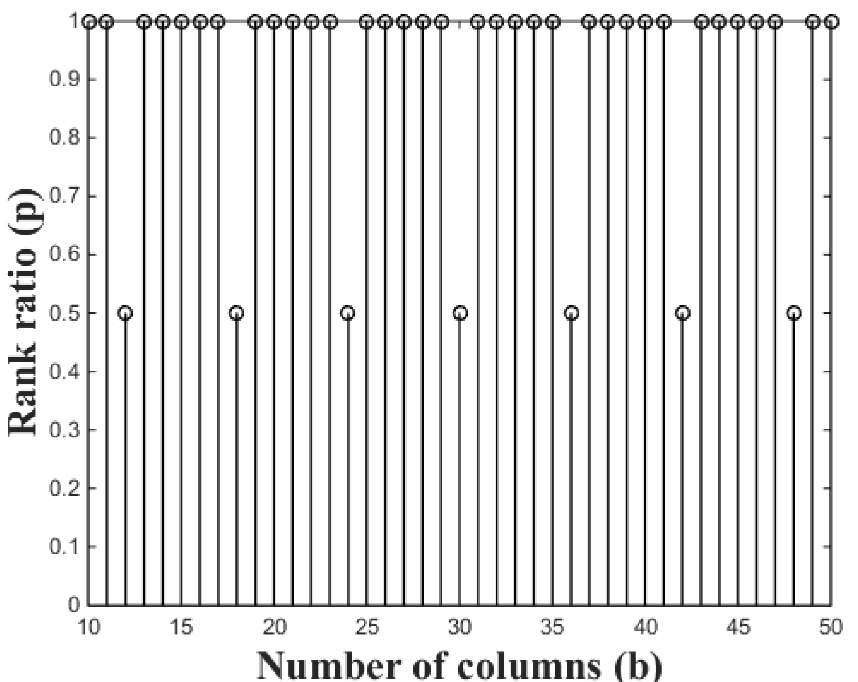
- Variation of rank ratio p with b for $B(7,4)$ assuming BER $= 0$
- Variation of rank ratio p with b for $B(7,4)$ assuming BER $= 5 \times 10^{-3}$

Rank values are obtained using algorithm proposed for non-erroneous scenario

NANYANG TECHNOLOGICAL UNIVERSITY

Simulation Results



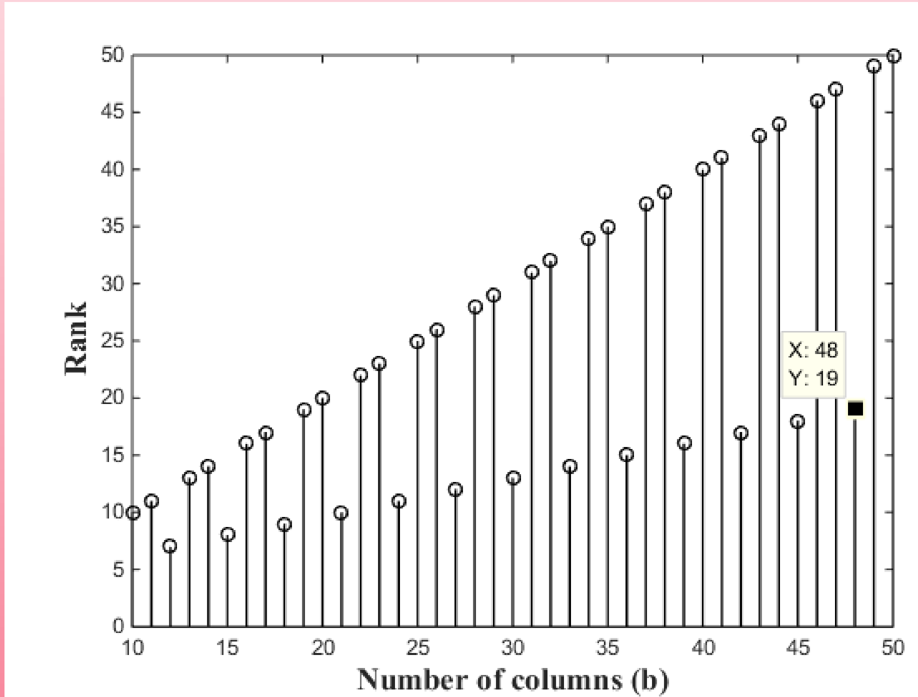


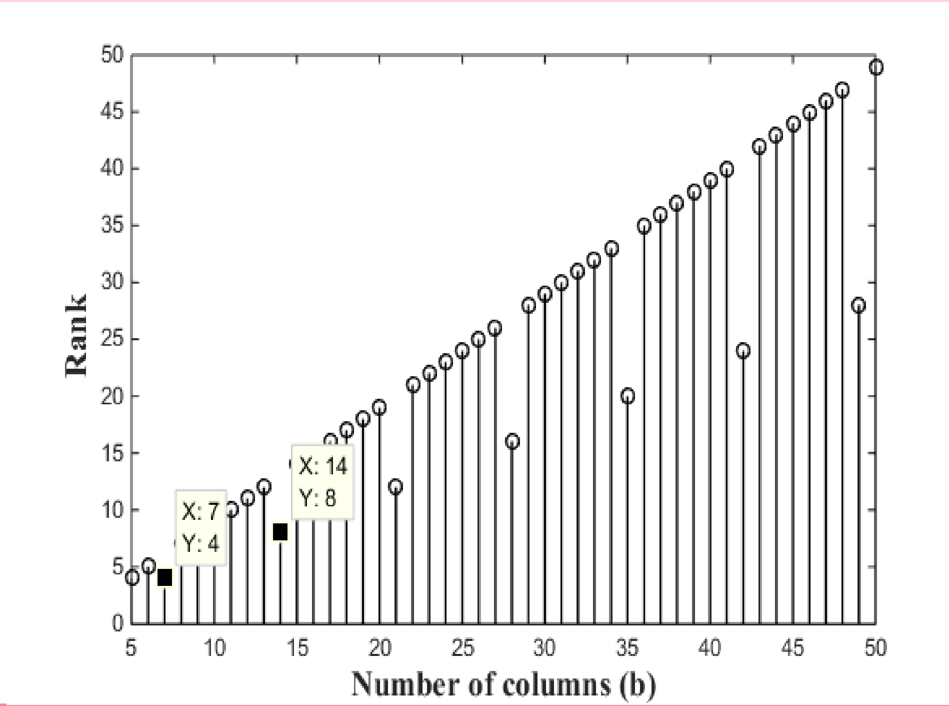
- Rank ratio p versus number of columns b for $C(3,1,7)[133,165,171]$ with $\mathrm{BER} = 2\times10^{-2}$.
- Rank ratio p versus number of columns b for $B(6,3)$ with $\mathrm{BER} = 10^{-2}$

Rank values are obtained using algorithm proposed for erroneous scenario: Histogram approach

NANYANG TECHNOLOGICAL UNIVERSITY

Simulation Results

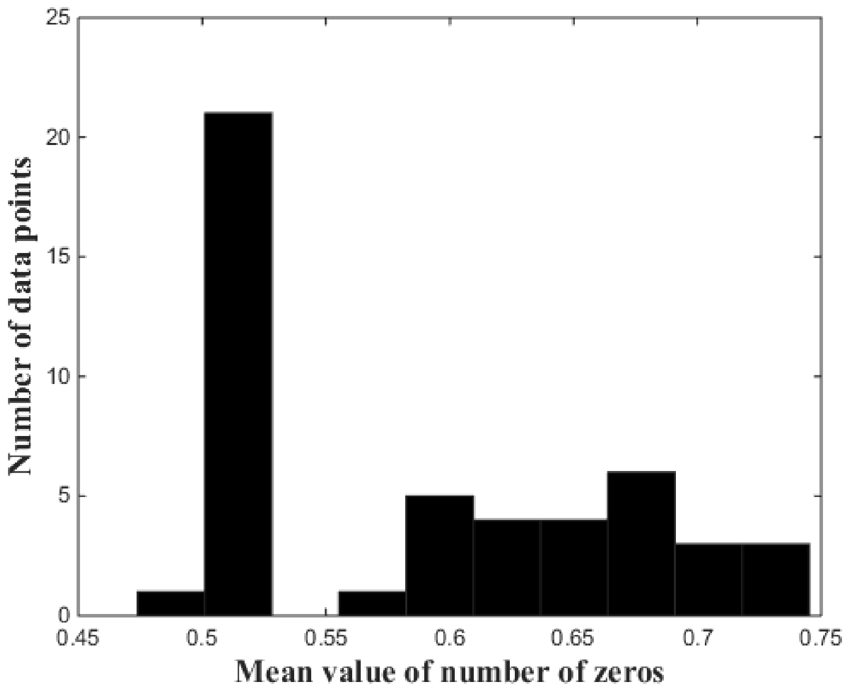


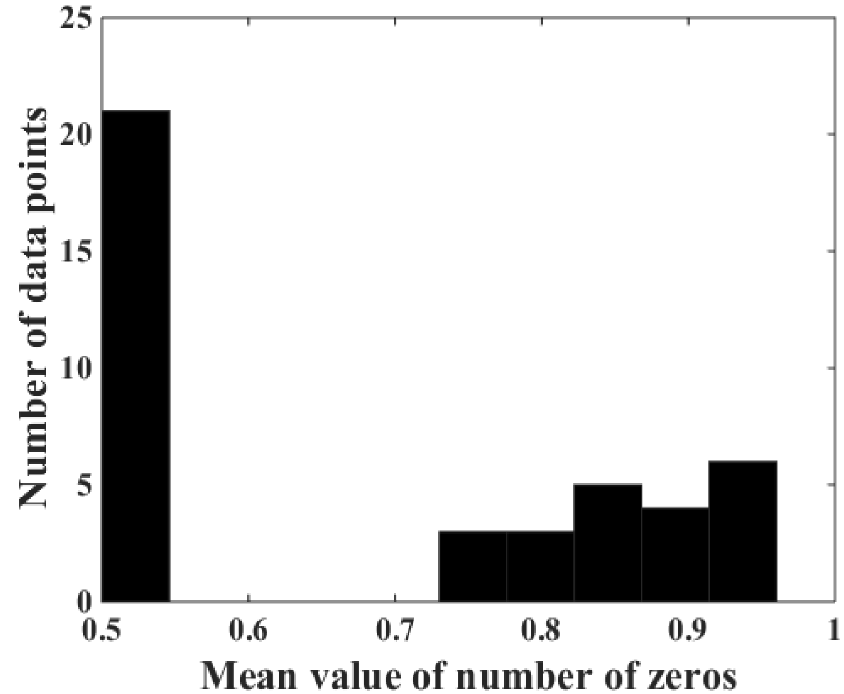


- Rank $\rho(S)$ versus number of columns b for $C(3,1,4)[13,15,17]$ with BER $= 2\times10^{-2}$.
- Rank $\rho(S)$ versus number of columns b for $B(7,4)$ with BER $= 10^{-2}$

By plotting rank ratio versus number of columns, code classification can be performed and by plotting rank versus number of columns, n and k can be identified

Simulation Results



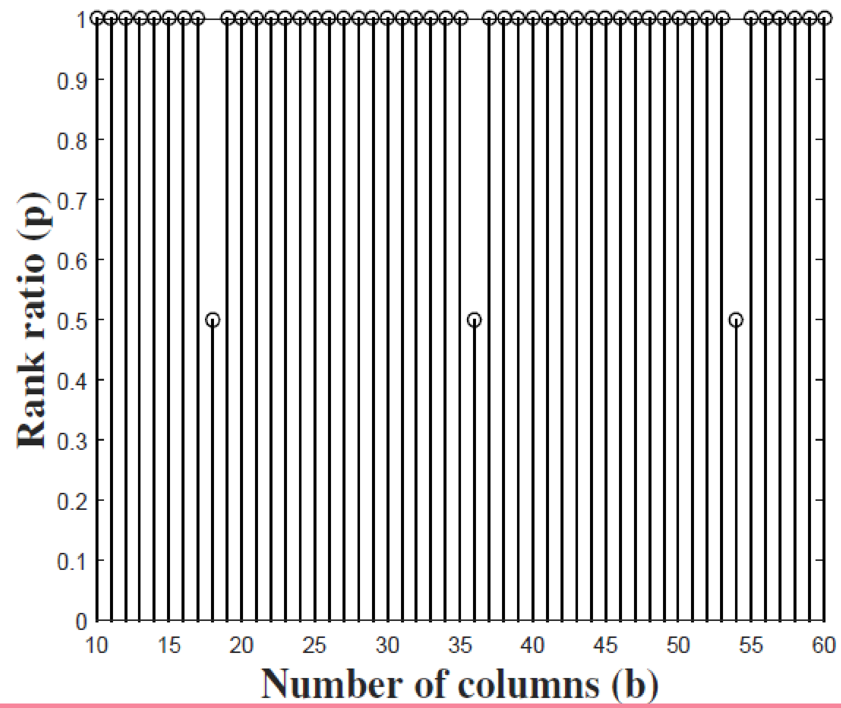


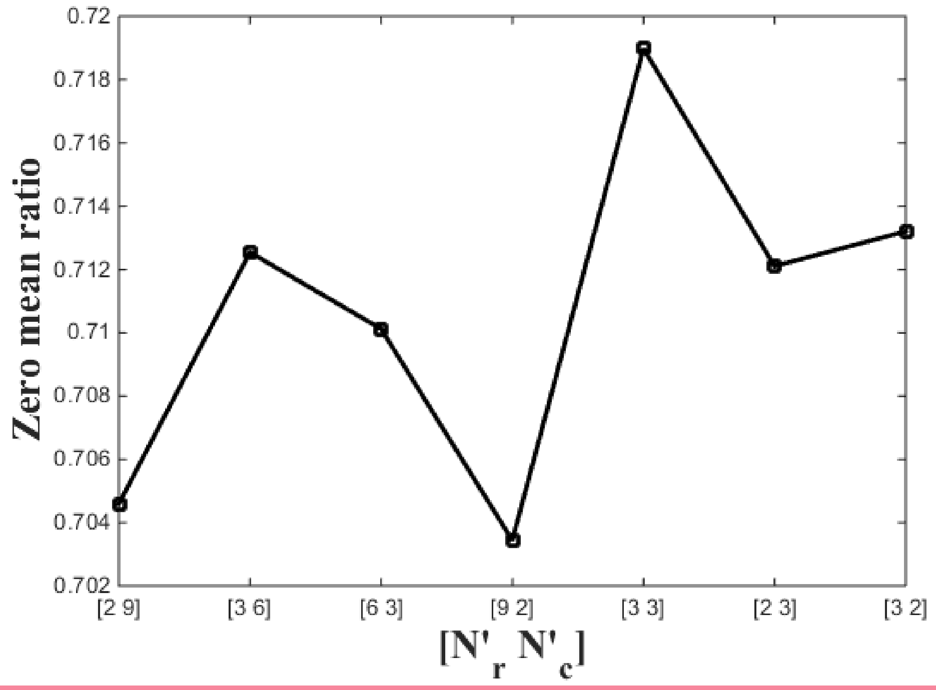
- Histogram plot for $mean(A)$ considering $b = 48$, $C(3,1,7)[133,165,171]$, and BER $= 2\times10^{-2}$.
- Histogram plot for $mean(A)$ considering $b = 42$, $B(6,3)$, and BER $= 10^{-2}$

(a) Fig. 1 : Γ_{opt}^{th} can be fixed between 0.53 to 0.56

(b) Fig. 2 : Γ_{opt}^{th} can be fixed between 0.55 to 0.57

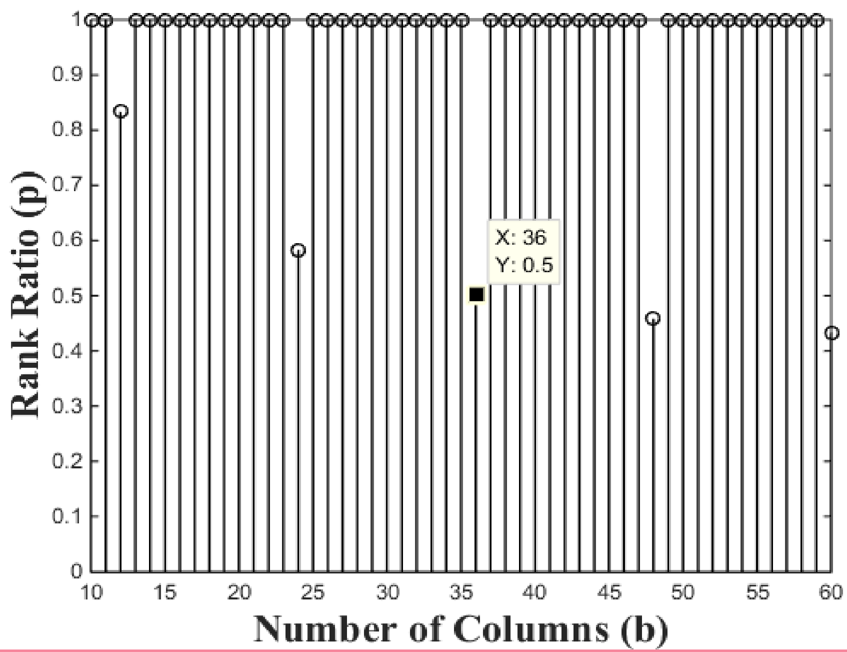
Simulation Results

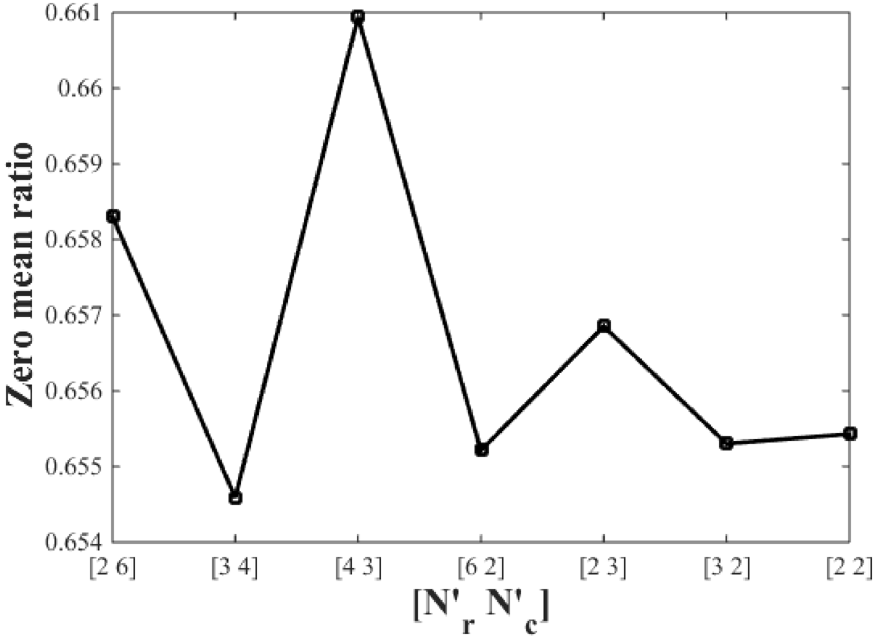




- Variation of rank ratio p with b for $B(6,3)$ considering block interleaver assuming $N_r = 3$, $N_c = 3$, and BER $= 10^{-2}$.
- Variation of zero mean ratio $\delta'(b)$ with all possible values of $[N_r' \; N_c']$ for $B(6,3)$ considering block interleaver assuming $N_r = 3$, $N_c = 3$, and BER $= 10^{-2}$

Simulation Results

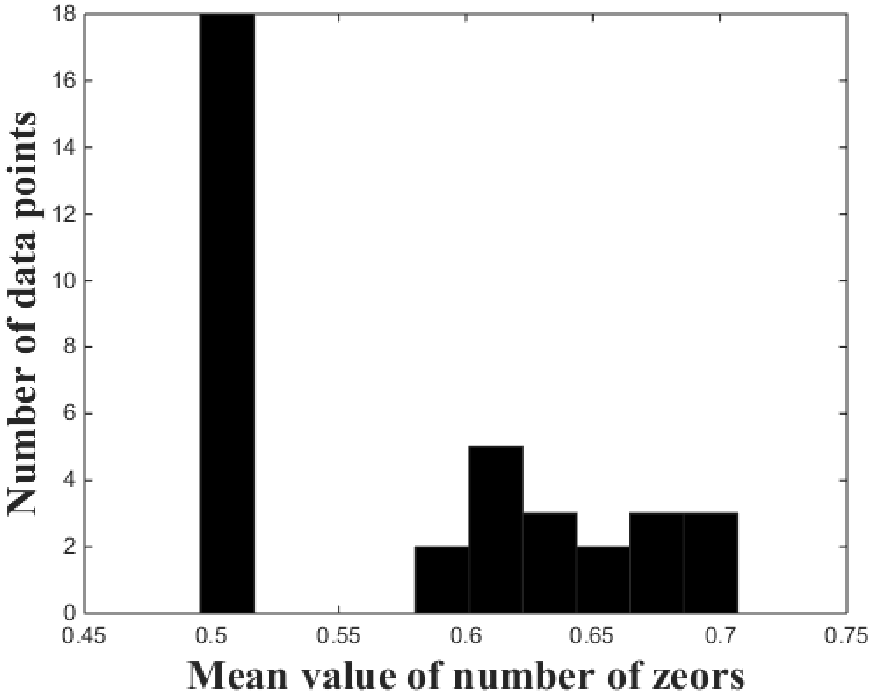


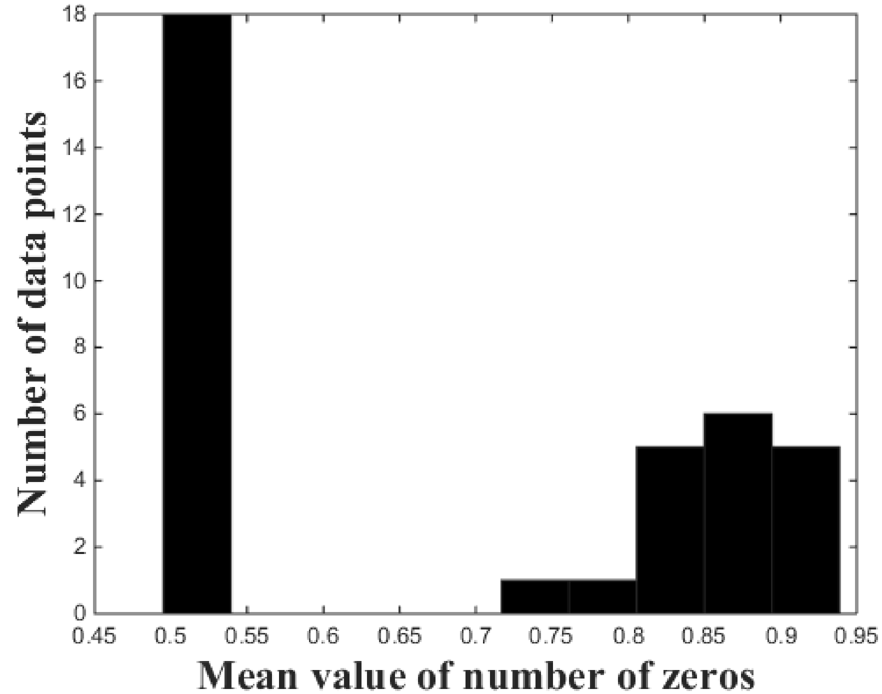


- Variation of rank ratio p with b for $C(3,1,7)[133,165,171]$ considering block interleaver assuming $N_r = 4$, $N_c = 3$, and BER $= 2\times10^{-2}$.
- Variation of zero mean ratio with all possible values of $[N'_r N'_c]$ for $C(3,1,7)[133,165,171]$ considering block interleaver assuming $N_r = 4$, $N_c = 3$, and BER $= 2\times10^{-2}$

NANYANG TECHNOLOGICAL UNIVERSITY

Simulation Results





- Histogram plot for $mean(A)$ assuming $b=36$, $N_r=4$, $N_c=3$, $C(3,1,7)[133,165,171]$, and $\text{BER} = 2\times10^{-2}$.
- Histogram plot for $mean(A)$ assuming $b=36$, $N_r=3$, $N_c=3$, $B(6,3)$, and $\text{BER} = 10^{-2}$

  - Fig. 1 : Γ_{opt}^{th} can be fixed between 0.52 to 0.59
  - Fig. 2 : Γ_{opt}^{th} can be fixed between 0.54 to 0.7

NANYANG TECHNOLOGICAL UNIVERSITY

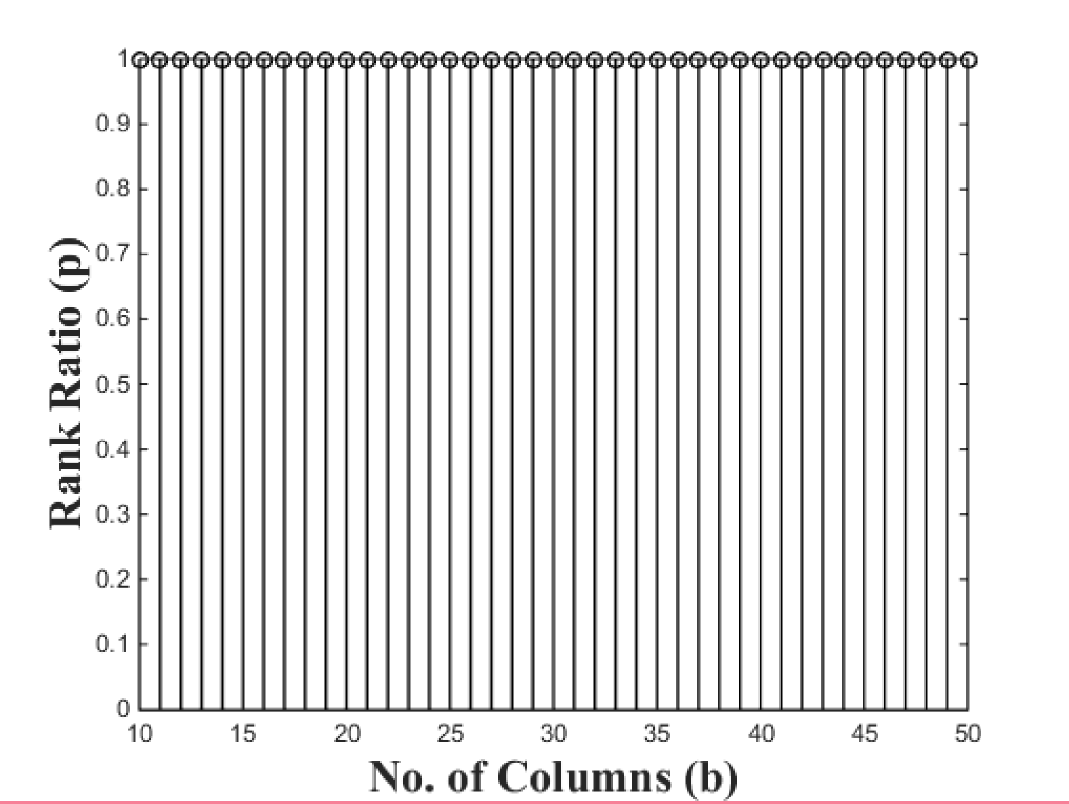
Simulation Results

- As the BER increases, the range for choosing threshold value decreases and incorrect value will change the rank ratio characteristics of the block and convolutional codes

TABLE II
THRESHOLD VALUES $\Gamma_{\text{opt}}^{\text{th}}$ FOR VARIOUS TEST CASES

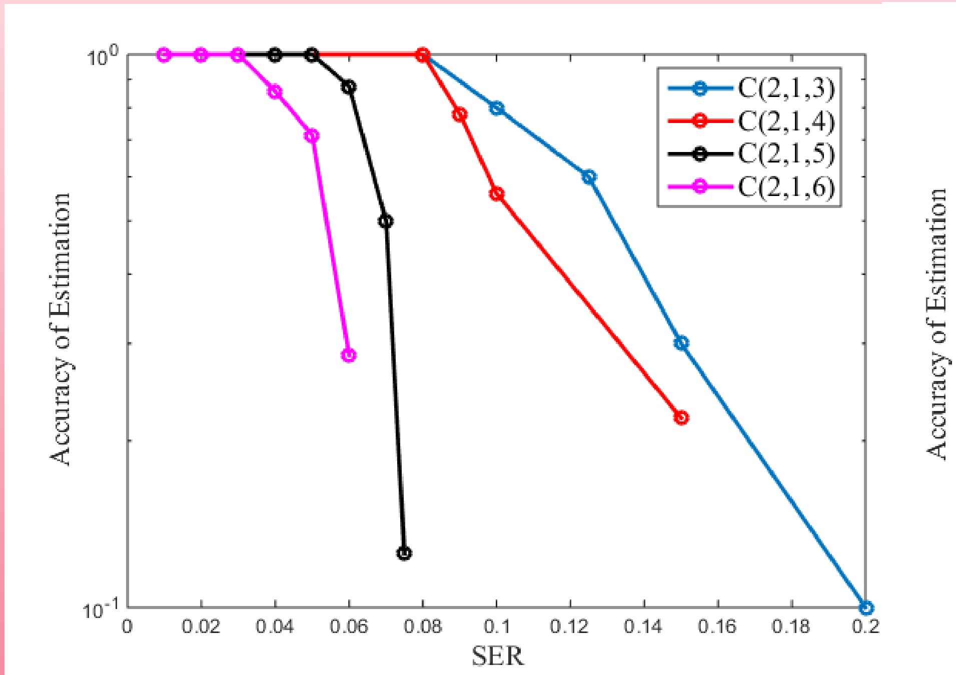
BER	FEC codes	Number of rows	Γ^{th}
10^{-2}	C[2,1,3], C[2,1,4] C[2,1,5], C[2,1,6] C[2,1,7], C[3,1,4] C[3,1,7], C[3,1,11] C[4,1,7], C[4,1,10] B(8,5), B(7,4) B(6,3), B(3,2)	$a = 20 \times b$	0.55
2×10^{-2}	C[2,1,3], C[2,1,4] C[2,1,5], C[3,1,4] C[3,1,7], C[4,1,7] C[4,1,10] B(8,5), B(7,4) B(6,3), B(3,2)	$a = 20 \times b$	0.55
	C[2,1,6], C[3,1,11]	$a = 50 \times b$	0.52
	C[2,1,7]	$a = 70 \times b$	0.51

Simulation Results

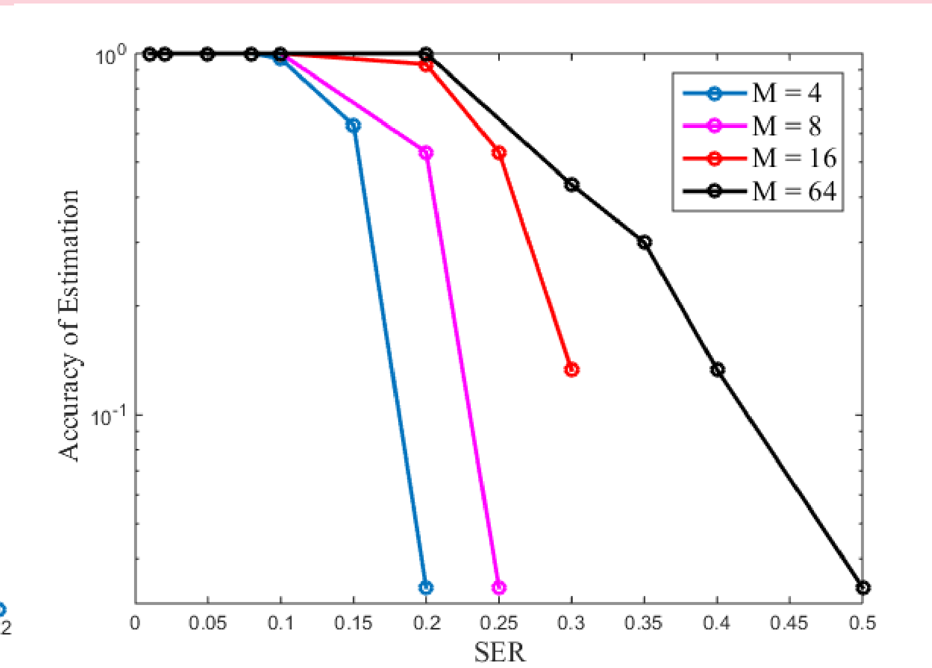


Variation of Rank ratio with respect to number of columns for uncoded data symbols assuming BER = 10^{-2}

Simulation Results



(a)



(b)

(a) Accuracy of estimation of rate 1/2 convolutional codes considering QPSK constellation by varying SER values

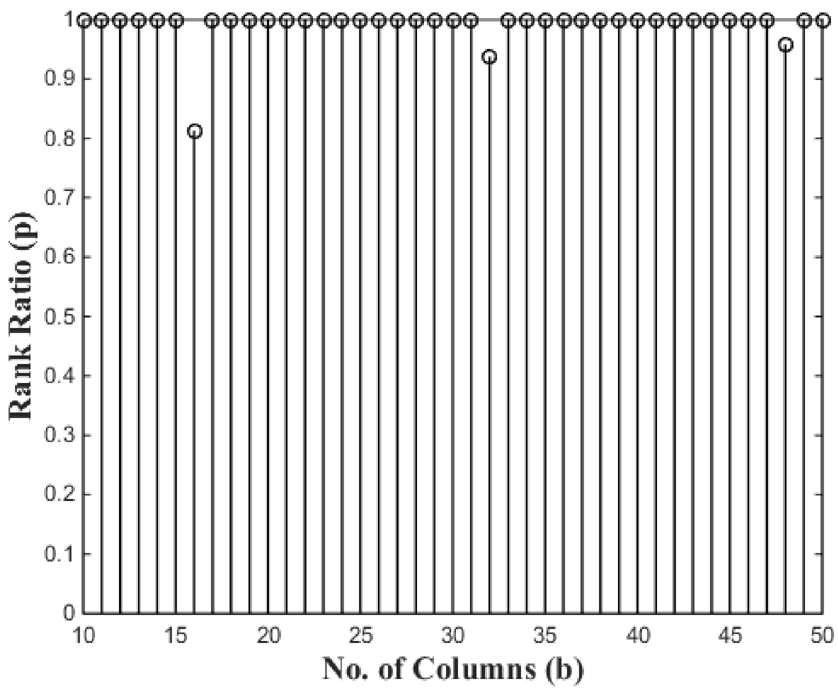
(b) Accuracy of estimation of block interleaver parameters for different M-QAM modulation schemes by varying SER values assuming N_r = 4, N_c = 3, and C(3, 1, 4)[13, 15, 17]

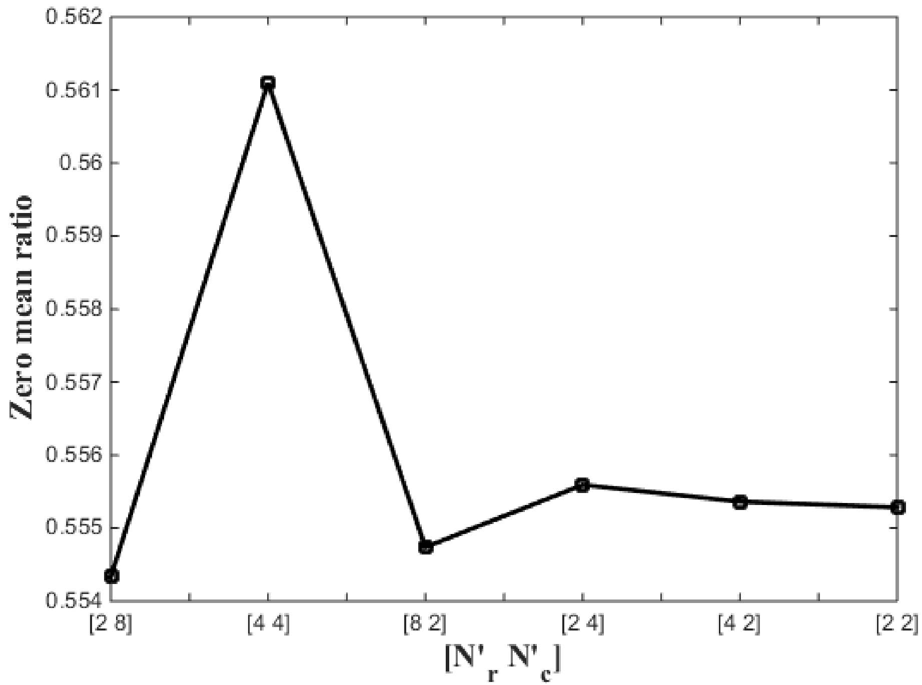
NANYANG TECHNOLOGICAL UNIVERSITY

Discussions

- The code classification in the presence of interleaver can be performed with 100 % accuracy until BER ≤ 2×10^{-2} based on histogram approach
- When BER > 2×10^{-2}, the proposed methodology fails to classify the incoming data symbols
- Reason: Unique rank ratio characteristics will change drastically due to more number of erroneous bits
- However, the estimation of interleaver parameters are observed to be successful until BER of 6×10^{-2}
- For BER $> 6 \times 10^{-2}$, the proposed algorithm (histogram approach) fails to recognize the interleaver parameters
- For the case without interleaver, the histogram approach fails to recognize the type of FEC codes for BER > 4×10^{-2}
- If optimal threshold value is fixed based on analytical approach, then code classification can be performed with 100% accuracy until BER of 5×10^{-3}
- For BER > 5×10^{-3}, optimal threshold based on the analytical approach fails to classify the incoming symbols
- However, interleaver parameters can be estimated correctly until BER of 2×10^{-2}

Simulation Results





- Variation of rank ratio p with b for $B(8,5)$ considering block interleaver assuming $N_r = 4$, $N_c = 4$, and BER $= 6 \times 10^{-2}$
- Variation of zero mean ratio $\delta'(b)$ with all possible values of $[N_r' \ N_c']$ for $B(8,5)$ considering block interleaver with $N_r = 4$, $N_c = 4$, and BER $= 6 \times 10^{-2}$

NANYANG TECHNOLOGICAL UNIVERSITY

Simulation Results

TABLE III
COMPARISON OF ACCURACY OF ESTIMATION OF DIFFERENT METHODOLOGIES

Test case	Actual No. of dependent columns for $b = 48$	Estimated number of dependent columns for $b = 48$ (% of Accuracy)		
		Fixing Γ^{th}_{opt} based on (25)	Fixing Γ^{th}_{opt} based on [6, eq.(A.4)]	Fixing Γ^{th}_{opt} based on histogram approach
C(2,1,3)	22	19 (86.4%)	15 (68.2%)	22 (100%)
C(2,1,4)	21	17 (81%)	17 (81%)	21 (100%)
C(3,1,4)	29	28 (96.6%)	26 (89.7%)	29 (100%)
C(3,1,7)	26	23 (88.5%)	23 (88.5%)	26 (100%)
C(3,1,10)	23	16 (82.6%)	16 (82.6%)	23 (100%)
C(4,1,7)	30	29 (96.7%)	26 (86.7%)	30 (100%)

[6] G. Sicot, S. Houcke, and J. Barbier, “Blind detection of interleaver parameters,” *Signal Process.*, vol. 89, no. 4, pp. 450–462, Apr. 2009.

Observations

- Histogram approach: Distribution of mean value of number of zeros in each columns has been predicted accurately.
- Analytical approach: Approximated the binomial distribution of mean value of number of zeros to normal distribution
- The performance degradation is mainly due to the approximation of binomial to normal distribution
- All the three methodologies are compared by keeping the computation time constant

Conclusions

- Innovative algorithms for joint estimation of type of FEC codes and block interleaver parameters have been proposed
- Firstly, estimation of interleaver period along with code classification among block, convolutional coded, and uncoded data symbols is performed
- After that while de-interleaving, rest of the block interleaver parameters are estimated
- It can be concluded that the deficient rank ratio remains constant at r for block codes
- For convolutional codes, the deficient rank ratio decays rapidly and remain approximately constant slightly above r
- Moreover, irrespective of the number of columns, full rank is obtained for uncoded data stream
- To justify the proposed claims, simulation results for recognizing the type of FEC codes and interleaver parameters are shown

NANYANG TECHNOLOGICAL UNIVERSITY

Part 2: Blind Reconstruction of Reed-Solomon Encoder and Interleavers Over Noisy Environment

Swaminathan R, A.S.Madhukumar, Wang Guohua, and Ting Shang Kee, ``Blind reconstruction of Reed-Solomon encoder and interleavers over noisy environment'', IEEE Transactions on Broadcasting, vol. 99, no. PP, pp. 1 - 16, Early Access, 2018

Motivations

The main motivations are given as follows:

- Non-cooperative scenario: It is mandatory to recognize the code and interleaver parameters at the receiver
- To propose an intelligent receiver system which adapts itself to any specific applications
- Previously proposed algorithm in [R1] for blind reconstruction of RS encoder can recognize only codeword length
- LLR-based technique [R2]: Assumes a predefined candidate set of RS encoders at transmitter and receiver
- The bit position adjustment parameter to achieve time synchronization is not recognized in [R1] and [R2]

[R1] 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. Wireless Commun. Netw.*, vol. 2015, no. 43, pp. 1–16, 2015

[R2] H. Zhang, H.-C. Wu, and H. Jiang, “Novel blind encoder identification of Reed-Solomon codes with low computational complexity,” in *Proc. IEEE GLOBECOM*, Atlanta, GA, USA, 2013, pp. 3294–3299

Motivations

- Block interleaver parameter estimation algorithms were restricted to convolutional encoded data.
- Only Interleaver period was estimated for non-binary RS codes [R3]
- Algorithms are not proposed for estimating all block interleaver parameters for non-binary codes
- Bit/symbol position adjustment parameter to achieve time synchronization is not estimated
- What is the probability of correct detection of RS code and block interleaver parameters using blind estimation algorithms ?

[R3] L. Lu, K. H. Li, and Y. L. Guan, "Blind detection of interleaver parameters for non-binary coded data streams," in *Proc. IEEE ICC*, Dresden, Germany, 2009, pp. 1–4.

NANYANG TECHNOLOGICAL UNIVERSITY

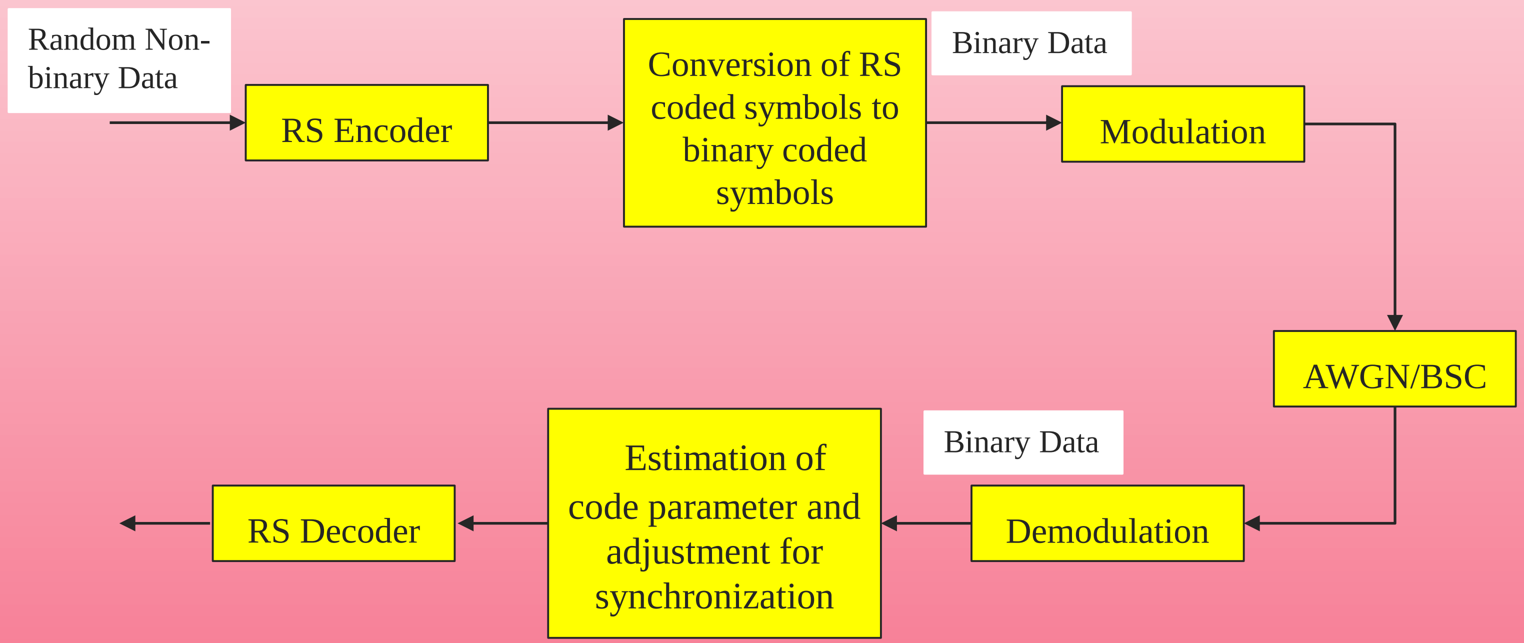
Contributions

The main contributions are given as follows:

- Innovative algorithms are proposed for the blind recognition of RS encoder (with and without block interleaver)
- Estimated RS code parameters: codeword length n, code dimension k, number of bits per symbol m, primitive polynomial p, and generator polynomial $g(x)$
- Estimated interleaver parameters: Interleaver period β and number of rows N_r and columns N_c of block interleaver matrix
- An innovative approach for synchronization compensation through appropriate bit/symbol positioning is discussed
- Simulation results are given for different test cases validating the proposed algorithms
- Performance of the algorithm in terms of accuracy of estimation is given and compared with the prior works

NANYANG TECHNOLOGICAL UNIVERSITY

Generic Block Diagram



Blind reconstruction of RS encoder

Reed-Solomon Codes

- RS codes are different from binary linear block codes and hence, the parameter estimation is slightly different
- The code symbols generated from RS codes belong to $GF(q)$, where $q = 2^m$ and $m \geq 3$
- Let α be a primitive element of $GF(q)$ such that $\alpha^{q-1} = 1$
- In the case of `t' error correcting (n, k) RS codes, $\alpha, \alpha^2, \ldots, \alpha^{2t}$ are the roots of *g(X)* with degree $n - k$, which is given by

$$g(X) = (X - \alpha)\ (X - \alpha^2)\ldots(X - \alpha^{2t})$$

- For RS codes, $n = q - 1$ and $n - k = 2t$
- Parameters to be estimated are n, k, m, primitive polynomial used for generating the Galois field (GF), and $g(X)$
- $g(X)$ can be estimated by recognizing n and k, since $n - k = 2t$ and $\alpha, \alpha^2, \ldots, \alpha^{2t}$ are the roots of *g(X)*

Algorithm 1: Estimation of RS code parameters - Noiseless case

- **Notations:** Let ϕ denotes the adjustment of bit position to achieve synchronization. a, b, $\rho(m,p,\phi)$, and $\rho'(m,p,\phi)$ denote the number of rows, columns, rank, and rank ratio of data matrix S, respectively
- **Assumptions:** $a \geq 2b$, $m \in [m_{\text{min}}, m_{\text{max}}]$, $p \in [p_{\text{min}}, p_{\text{max}}]$, and $\phi \in [0, ((q-1)m)-1]$
- $p = \text{primpoly}(m, 'all')$
- Shift the binary data symbols by ϕ bit positions and convert the same into non-binary symbols
- Create a GF array from the non-binary data symbols using primitive polynomial p
- Reshape the RS encoded GF array elements into a data matrix S of size $a \times b$, where $b = q-1$
- Convert S into F using finite-field Gauss elimination process
- Compute $\rho(m,p,\phi)$ from the number of non-zero columns in F
- Compute $\rho'(m,p,\phi) = \rho(m,p,\phi)/b$
- 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 $k_{\text{est}} = \rho(m_{\text{est}}, p_{\text{est}}, \phi_{\text{est}})$

NANYANG TECHNOLOGICAL UNIVERSITY

Observations

- If $b = n_{\text{est}} = 2^{m_{\text{est}}} - 1$, then rank deficiency will be obtained. $\rho(m_{\text{est}}, p_{\text{est}}, \phi_{\text{est}})$ and $\rho'(m_{\text{est}}, p_{\text{est}}, \phi_{\text{est}})$ for $b = n_{\text{est}}$ are, respectively, given by

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

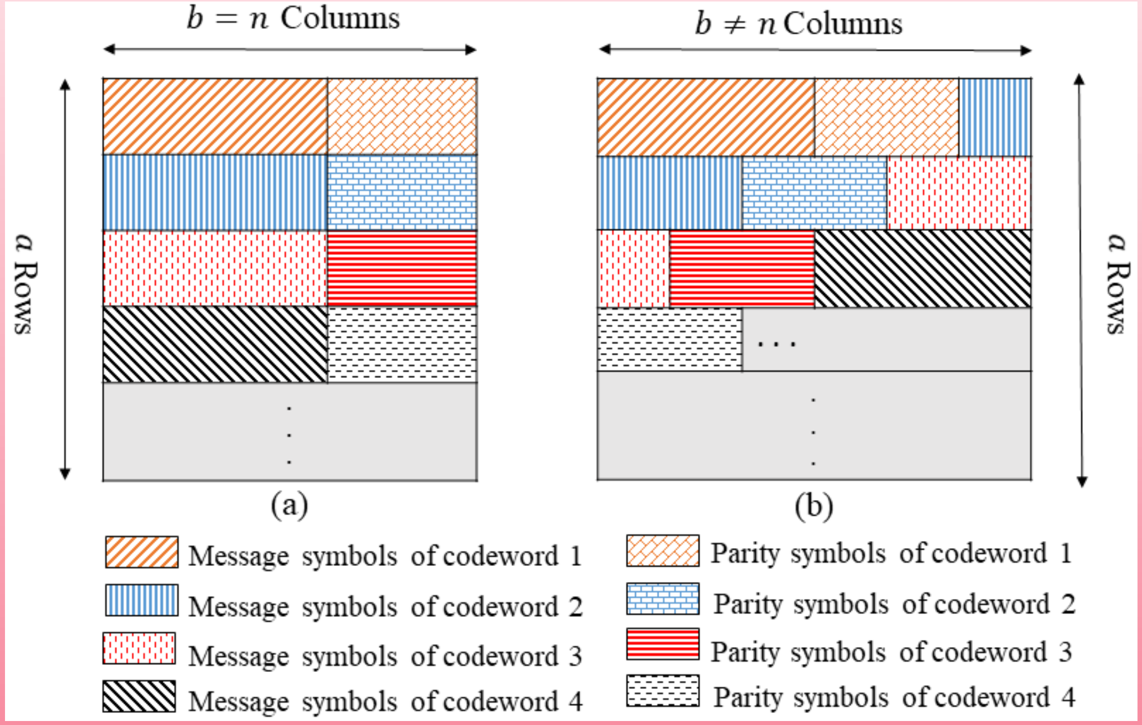
- If b is a multiple of n_{est} (i.e. $b = \alpha.n_{\text{est}}$), then the deficient rank value is given by $\alpha.k_{\text{est}}$. However, if $b \neq \alpha.n_{\text{est}}$, then full rank will be obtained.

Explanation:

- The output n data symbols depend only on k input symbols in the case of RS codes
- Therefore, $\alpha.n_{\text{est}}$ output symbols of S depend on $\alpha.k_{\text{est}}$ input symbols
- When $b = \alpha.n_{\text{est}}$, then α codewords in all the rows will be aligned properly in the same column
- If the data and parity symbols in all the rows are aligned properly in the same column, linear relation is satisfied in all the rows
- There will exist linear relations between columns in S
- After converting S into F through finite field Gauss elimination process, all $\alpha.(n_{\text{est}} - k_{\text{est}})$ dependent columns will be eliminated, which will give rise to rank deficiency

NANYANG TECHNOLOGICAL UNIVERSITY

Observations

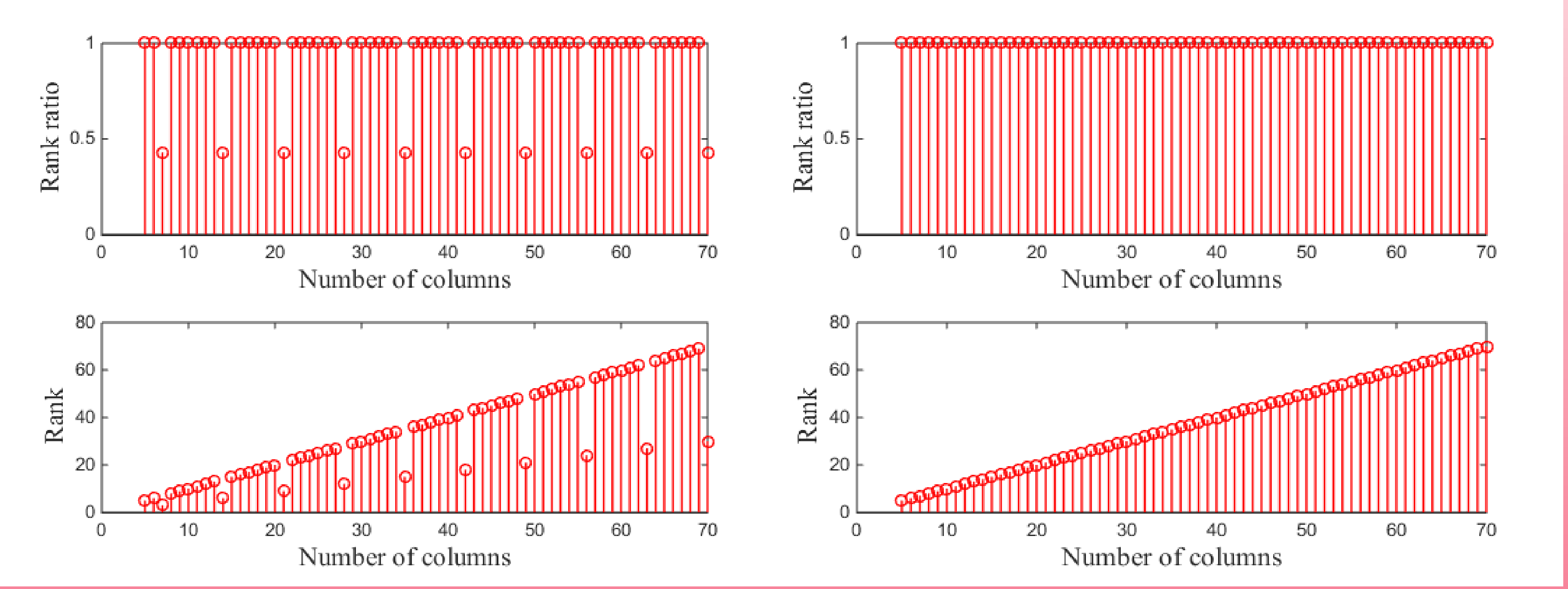


Structure of data matrix for the case when (a) $b = n$ and (b) $b \neq n$

- If data and parity symbols are segregated in different rows and are not aligned properly in the same column, then the linear relation will be affected
- 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.

NANYANG TECHNOLOGICAL UNIVERSITY

Observations



- Variation of rank ratio and rank versus number of columns for $\mathrm{RS}(7,3,3,11)$ considering non-erroneous case
- Variation of rank ratio and rank versus number of columns for $\mathrm{RS}(7,3,3,11)$ considering $\mathrm{SER}{=}3\times10^{-2}$

Parameter Estimation: Noisy case

- The dependent columns in *S* will be converted into all-zero-columns in *F* using finite-field Gauss elimination process
- The Algorithm 1 proposed for non-erroneous scenario fails for erroneous scenario, since full rank will be obtained
- Rank-deficient matrix under erroneous channel conditions will have less number of non-zero elements compared to the full-rank matrix
- Therefore, the rank-deficient data matrix is identified based on evaluating the non-zero-mean-ratio in the case of erroneous scenario

Algorithm 2: Estimation of RS code parameters - Noisy case

- **Notations:** The mean and normalized mean values of number of non-zero elements in c^{th} column of F are denoted as $\sigma(c, m, p, \phi)$ and $\sigma'(c, m, p, \phi)$, respectively
- $p = \text{primpoly}(m, 'all')$
- Shift the binary data symbols by ϕ bit positions and convert the same into non-binary symbols
- Create a GF array from the non-binary data symbols using primitive polynomial p
- GF array is created using primitive polynomial p from the non-binary data symbols
- RS encoded GF array elements are reshaped into S of size $a \times b$, where $b = q - 1$
- Using finite-field Gauss elimination process, S is converted into F
- Evaluate $\sigma(c, m, p, \phi)$, where $c \in \{1, 2, ..., b\}$ and obtained values are normalized with respect to maximum value
- Calculate the normalized non-zero-mean-ratio, which is given by $\mu'(m, p, \phi) = \frac{\sum_{c=1}^{b} \sigma'(c, m, p, \phi)}{b}$
- Obtain $[m_{\text{est}}, p_{\text{est}}, \phi_{\text{est}}] = \underset{m,p,\phi}{\text{argmin}}(\mu'(m, p, \phi))$ and $n_{\text{est}} = 2^{m_{\text{est}}} - 1$

Discussions

- The rank deficiency will be observed for correct values of m, p, and ϕ
- Since rank-deficient data matrix will have less number of non-zero elements, $\mu'(m_{\text{est}}, p_{\text{est}}, \phi_{\text{est}})$ will be smaller compared to other possible combinations of $[m, p, \phi]$
- Code and generator polynomials of RS codes have equal number of roots and is given by $n - k = 2t$
- By finding the number of roots of code polynomial, $n_{\text{est}} - k_{\text{est}}$ is identified
- k_{est} can be recognized from $n_{\text{est}} - k_{\text{est}}$
- After recognizing the number of roots of code polynomial, $g(x)$ is obtained

NANYANG TECHNOLOGICAL UNIVERSITY

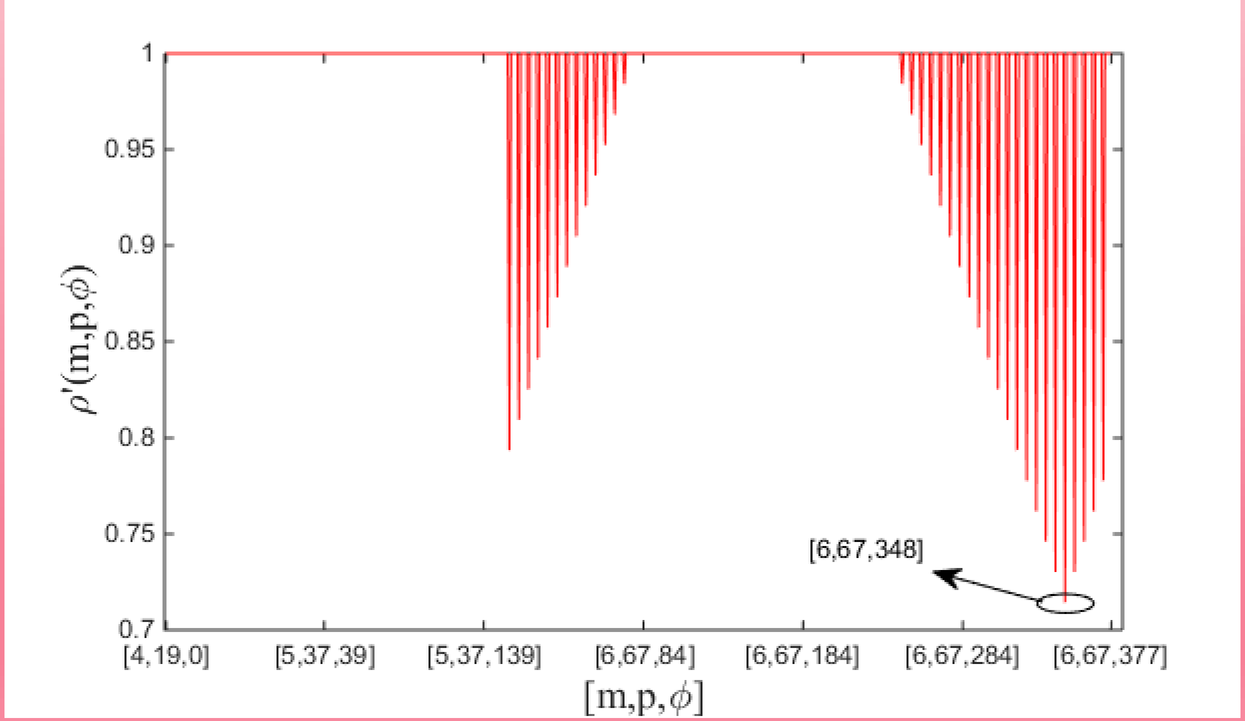
Simulation parameters

Table 1: 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	$\mathrm{RS}(7,3,3,11)$, $\mathrm{RS}(15,7,4,19)$, $\mathrm{RS}(15,9,4,19)$, $\mathrm{RS}(15,11,4,19)$, $\mathrm{RS}(31,15,5,37)$, $\mathrm{RS}(31,19,5,37)$, $\mathrm{RS}(31,23,5,37)$, $\mathrm{RS}(63,45,6,67)$, $\mathrm{RS}(255,127,8,285)$
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 $N_c = 6$

Simulation Results

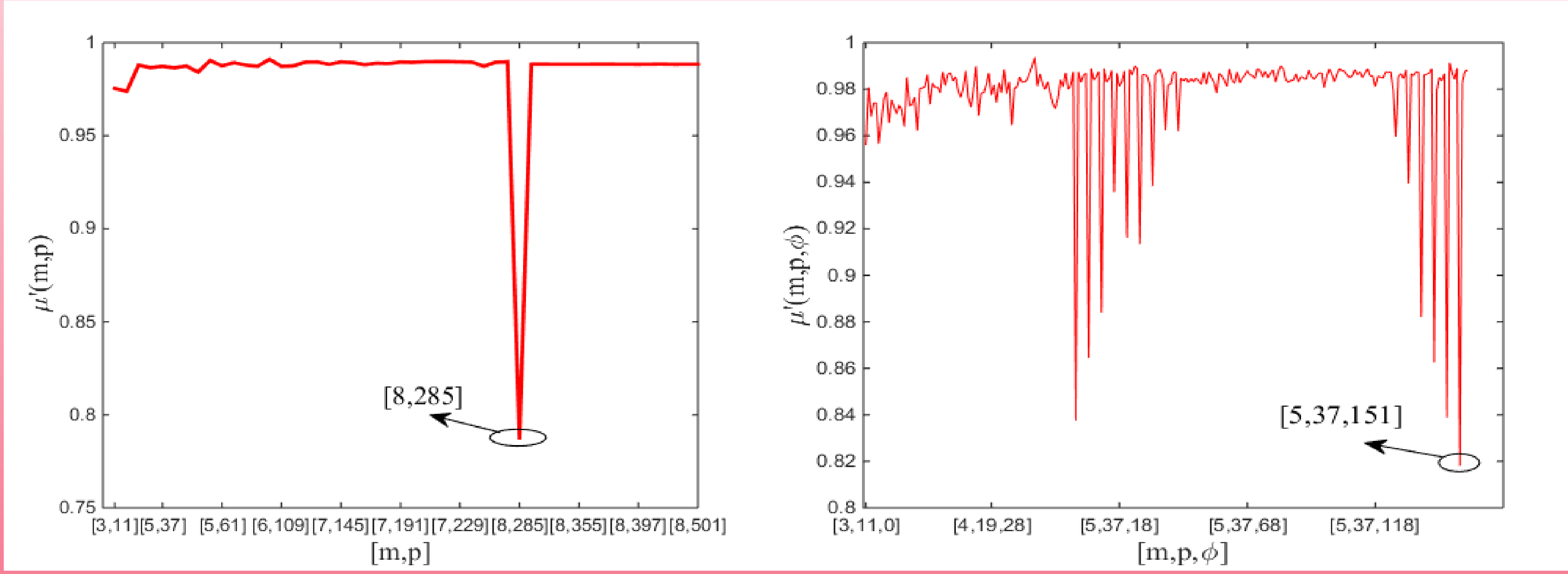
- We assume $a = 2b$ for non-erroneous case and $a > 2b$ for erroneous case
- Higher the number of rows, better is the accuracy for erroneous case
- If the receiver starts at Δ^{th} position of t^{th} RS code word, then frame synchronization is achieved by shifting $\phi = (tm(q-1)+1) - (\Delta M_1 - M_1 + 1)$ bit positions, where $M_1 = \log_2 M$



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

NANYANG TECHNOLOGICAL UNIVERSITY

Simulation Results

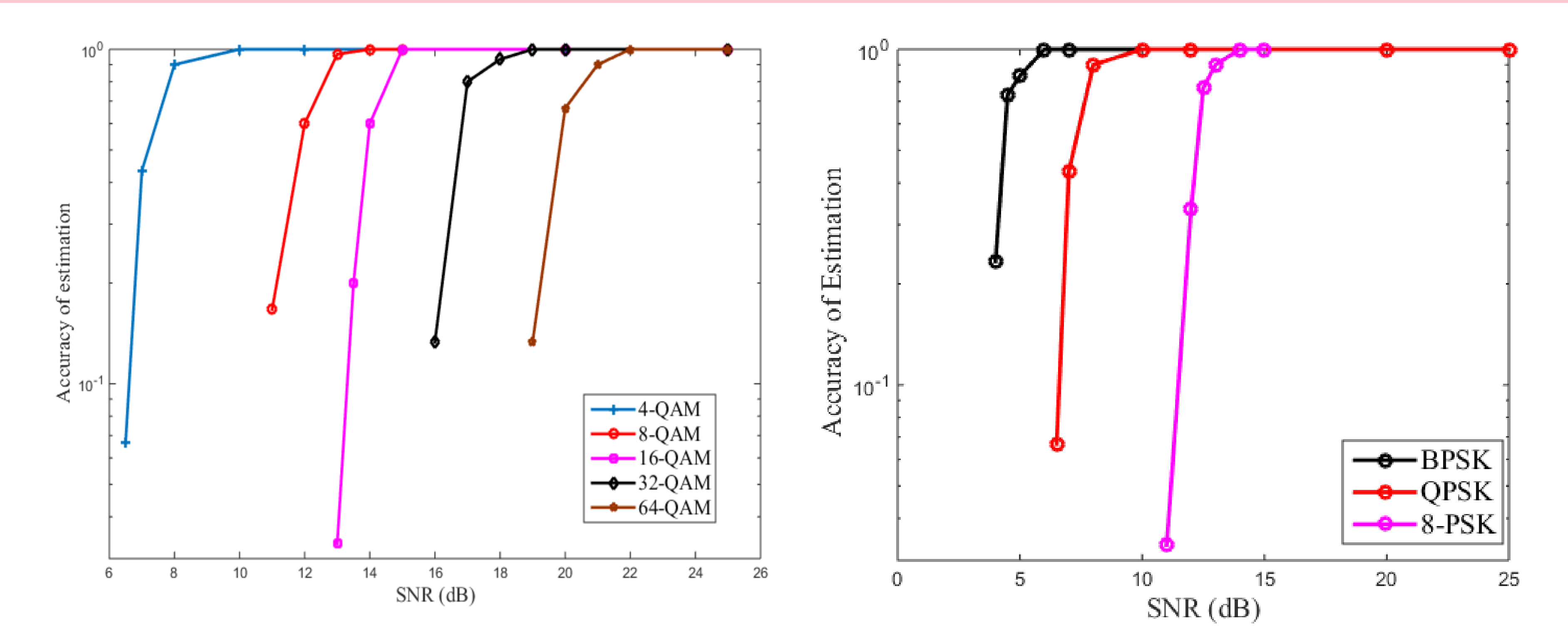


(a) Variation of normalized non-zero-mean-ratio $\mu'(m,p)$ with $[m,p]$ for $\mathrm{RS}(255,127,8,285)$ coded data symbols assuming 256-QAM scheme and SER$=2\times 10^{-3}$

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

NANYANG TECHNOLOGICAL UNIVERSITY

Simulation Results

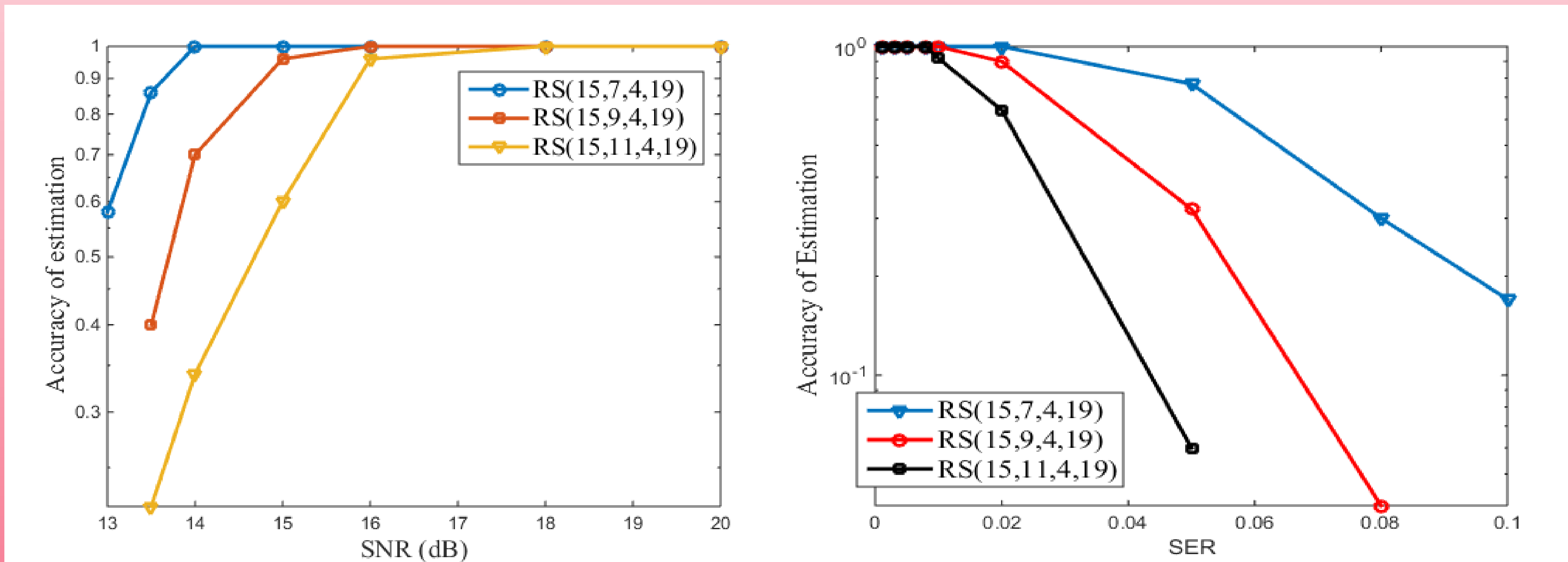


(a) Accuracy of estimation of RS codes RS$(15, 9, 4, 19)$ for different M-QAM schemes

(b) Accuracy of estimation of RS codes RS$(15, 9, 4, 19)$ for different M-PSK schemes

NANYANG TECHNOLOGICAL UNIVERSITY

Simulation Results

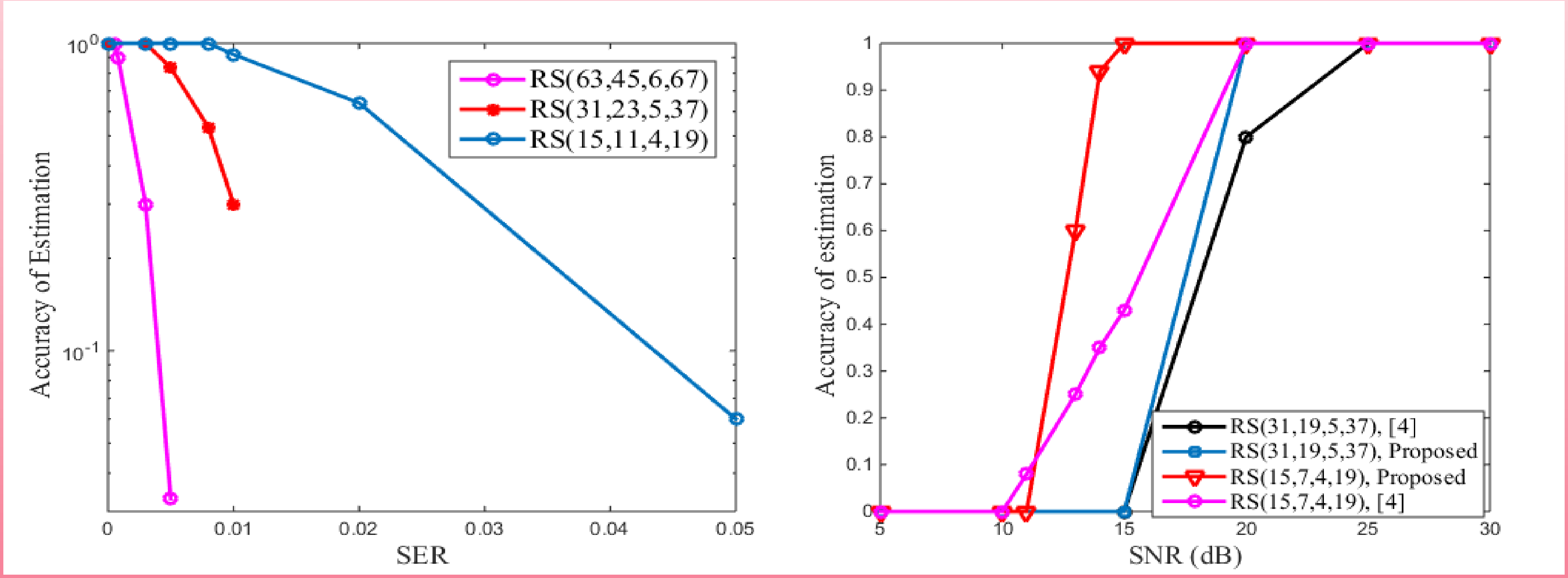


(a) Accuracy of estimation of RS codes assuming $n = 15$, $m = 4$, $p = 19$, and 16-QAM scheme for different values of code dimension k

(b) Accuracy of estimation of RS codes assuming $n = 15$, $m = 4$, $p = 19$, and 16-QAM scheme for different values of code dimension k

NANYANG TECHNOLOGICAL UNIVERSITY

Simulation Results



(a) Accuracy of estimation of RS codes with 16-QAM scheme for different values of codeword length n

(b) Performance comparison of the proposed algorithm with the algorithm proposed in [4]

[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.

NANYANG TECHNOLOGICAL UNIVERSITY

Simulation Results

Table 1: Comparison of probability of correct detection of RS code $RS(15, 7, 4, 19)$

SER	Probability of detection [2]	Probability of 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

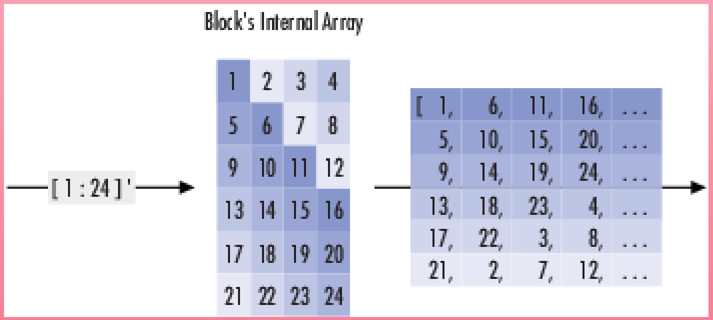
Proposed algorithm outperforms existing algorithm

[2] 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.

NANYANG TECHNOLOGICAL UNIVERSITY

Helical Scan Interleaver

- Helical Scan Interleaver uses a fixed size matrix, arranges input symbols across rows, and outputs all the symbols without using default value or values from previous call
- Interleaver parameters (similar to block interleaver): Number of columns (N_c), Number of rows (N_r), Helical array step size (*d*), Interleaver period (β)

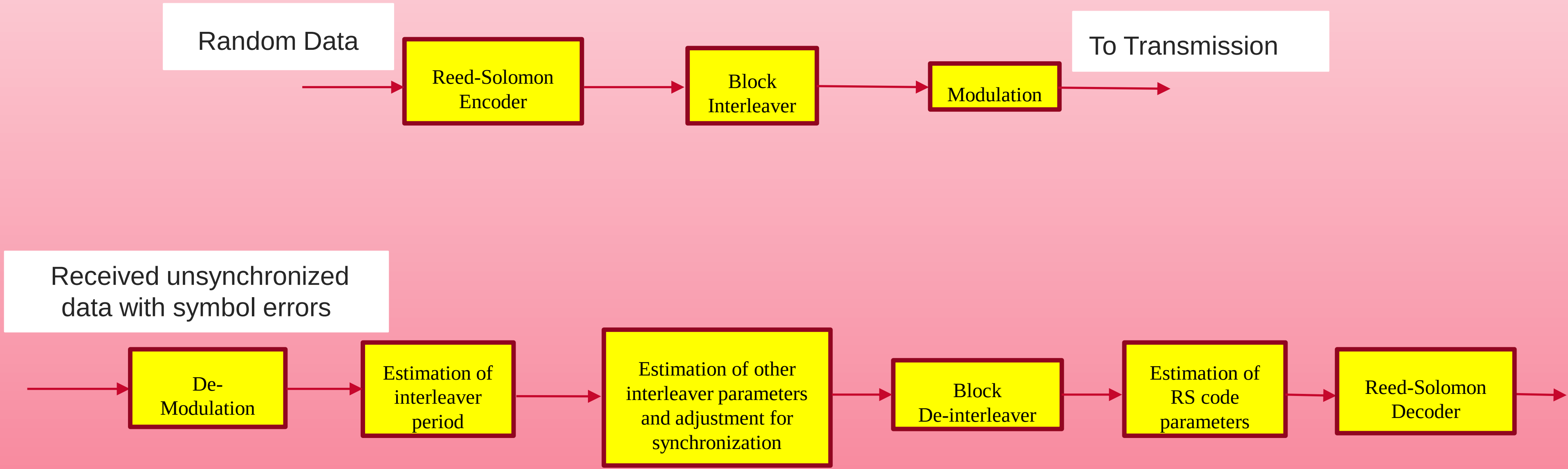


Helical Scan Interleaver [1] $N_r = 6$, $N_c = 4$, $d = 1$, β = 24

1. http://www.mathworks.com/help/comm/ref/matrixhelicalscaninterleaver.html

Generic Block Diagram

- The generic block diagram for blind recognition of interleaver and RS code parameters is given as follows:



Algorithm 3: Estimation of interleaver period - Noiseless case

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

Observations

If β is a multiple of n i.e. $\beta = \gamma \cdot n$ and $b = \alpha' \cdot \beta$, then the rank deficiency will be obtained. The deficient rank and rank ratio are, respectively, given by

$$\begin{aligned} \rho(m_{\text{est}}, p_{\text{est}}, b_{\text{est}}) &= \alpha' \cdot \gamma \cdot k_{\text{est}}, \\ \rho'(m_{\text{est}}, p_{\text{est}}, b_{\text{est}}) &= \frac{\rho(m_{\text{est}}, p_{\text{est}}, b_{\text{est}})}{b} = r\,. \end{aligned} \tag{1}$$

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

If β is not a multiple of n, then rank deficiency will be obtained for $b = \alpha' \cdot \mathrm{lcm}(n, \beta)$. Assuming $\mathrm{lcm}(n, \beta) = \Gamma \cdot n$, the deficient rank and rank ratio values are, respectively, given by

$$\begin{aligned} \rho(m_{\text{est}}, p_{\text{est}}, b_{\text{est}}) &= \alpha' \cdot \Gamma \cdot k_{\text{est}}, \\ \rho'(m_{\text{est}}, p_{\text{est}}, b_{\text{est}}) &= \frac{\rho(m_{\text{est}}, p_{\text{est}}, b_{\text{est}})}{b} = r\,. \end{aligned} \tag{2}$$

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

Observations

- From Algorithm 3, $\beta_{\text{est}} = b_{\text{est}}$ for the case when β is a multiple of n
- For the case when β is not a multiple of n, $\text{lcm}(n_{\text{est}}, \beta_{\text{est}}) = b_{\text{est}}$
- 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
- $\text{lcm}(n, \beta)$ is identified from $b' - b$ for the case when $\beta \neq \gamma \cdot n$ and $\text{lcm}(n, \beta) = \Gamma \cdot n$

Algorithm 4: Estimation of interleaver period - Noiseless case

- **Notations:** Mean value and normalized mean value of number of non-zero elements in c^{th} column of F - $\sigma(c, m, p)$ and $\sigma'(c, m, p)$. Normalized non-zero-mean-ratio - $\mu'(m, p, b)$
- **Assumptions:** $a \geq t\, b$, $b \in [b_{\text{min}}\ ,\ b_{\text{max}}]$, $m \in [m_{\text{min}}\ ,\ m_{\text{max}}]$
- $p = \text{primpoly}(m, 'all')$
- Convert the incoming RS coded and block interleaved binary data symbols into the respective elements of GF using p
- Reshape the RS encoded GF array elements into a data matrix S of size $a \times b$
- Convert S into F using finite-field Gauss elimination process
- Evaluate $\sigma(c, m, p)$, where $c \in \{1, 2, ..., b\}$, and normalize the obtained values with respect to the maximum value
- Calculate normalized non-zero-mean-ratio $\mu'(m, p, b)$, where $\mu'(m, p, b) = \frac{\sum_{c=1}^{b} \sigma'(c,m,p)}{b}$
- Obtain $[m_{\text{est}}, p_{\text{est}}, b_{\text{est}}] = \underset{m,p,b}{\text{argmin}}(\mu'(m, p, b))$ and $n_{\text{est}} = 2^{m_{\text{est}}} - 1$

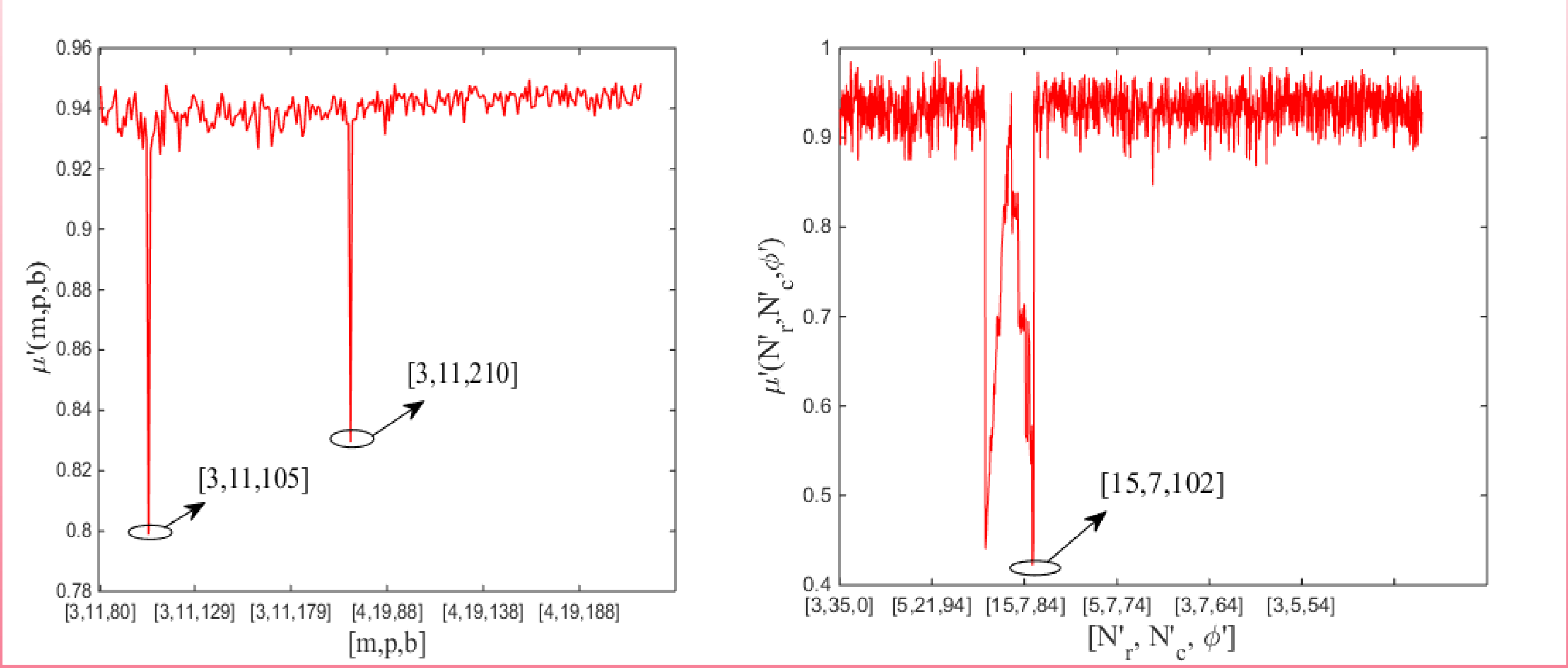
Algorithm 5: Estimation of rest of interleaver parameters

- **Notations** : $\zeta_{\text{est}} = \text{lcm}(n_{\text{est}}, \beta_{\text{est}})$, ϕ' - symbol position adjustment to achieve synchronization, d - helical array step size, and Normalized non-zero-mean-ratio of F for matrix-based and helical scan interleavers - $\mu'(N_r', N_c', \phi')$ and $\mu'(N_r', N_c', d, \phi')$
- **Assumptions** : $a \geq t\, b$, $\phi' \in [0\ ,\ \zeta_{\text{est}} - 1]$, $d \in [1\ ,\ N_r' - 1]$
- Convert the incoming RS coded and block interleaved binary data symbols into the respective elements of GF using p_{est}
- Get all possible values of δ' that satisfy $\text{lcm}(n_{\text{est}}, \delta') = \zeta_{\text{est}}$
- Get all possible combinations of two factors N_r' and N_c' that satisfy $N_r' N_c' = \delta'$
- Shift the coded and interleaved non-binary symbols by ϕ' symbol positions
- De-interleave using N_r' and N_c' in the case of matrix-based block interleaver
- De-interleave using N_r', N_c', and d in the case of helical scan interleaver
- Fix b as a multiple of n_{est}
- Reshape the RS encoded GF elements into a data matrix S of size $a \times b$
- Convert S into F using finite-field Gauss elimination process

Algorithm 5 – Contd.

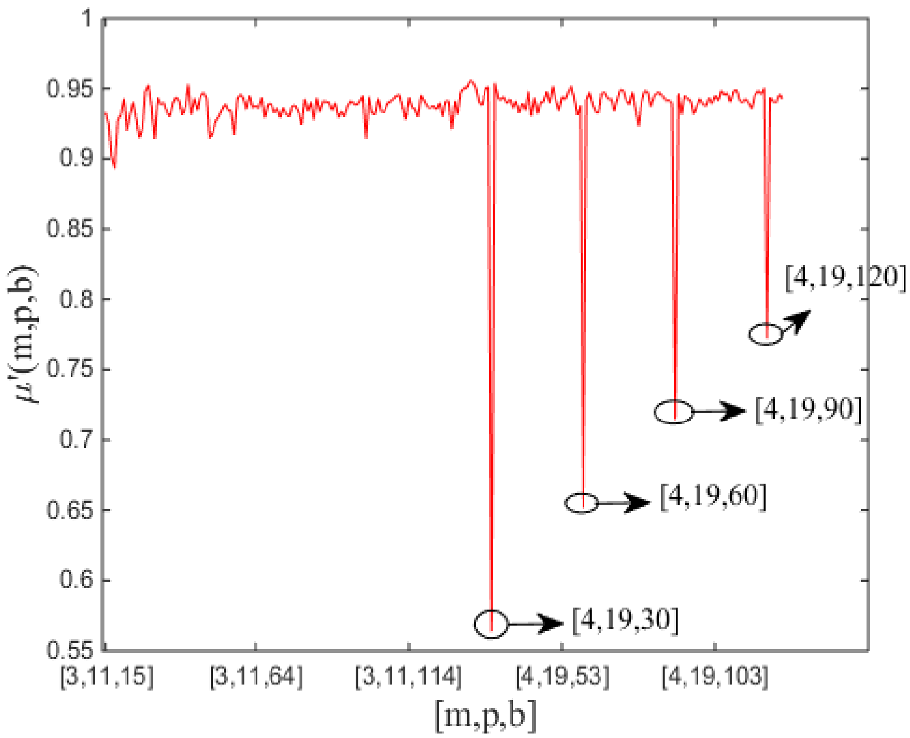
- Evaluate $\mu'(N_r', N_c', \phi')$ for all possible values of N_r' and N_c' in the case of matrix interleaver
- Evaluate $\mu'(N_r', N_c', d, \phi')$ for all possible values of N_r', N_c', and d in the case of helical scan interleaver
- **Matrix-based block interleaver:** Obtain $[N_r^{\text{est}}, N_c^{\text{est}}, \phi_1^{\text{est}}] = \underset{N_r', N_c', \phi'}{\text{argmin}}(\mu'(N_r', N_c', \phi'))$
- **Helical scan interleaver:** Obtain $[N_r^{\text{est}}, N_c^{\text{est}}, d^{\text{est}}, \phi_1^{\text{est}}] = \underset{N_r', N_c', d, \phi'}{\text{argmin}}(\mu'(N_r', N_c', d, \phi'))$
- **Matrix-based block interleaver:** Shift ϕ_1^{est} symbol positions and de-interleave using N_r^{est} and N_c^{est}
- **Helical scan interleaver:** Shift ϕ_1^{est} symbol positions and de-interleave using N_r^{est}, N_c^{est}, and d^{est}
- Identify the number of roots of generator polynomial and estimate $n - k$
- Obtain k_{est} from $n - k$
- Obtain the generator polynomial $g(x)$

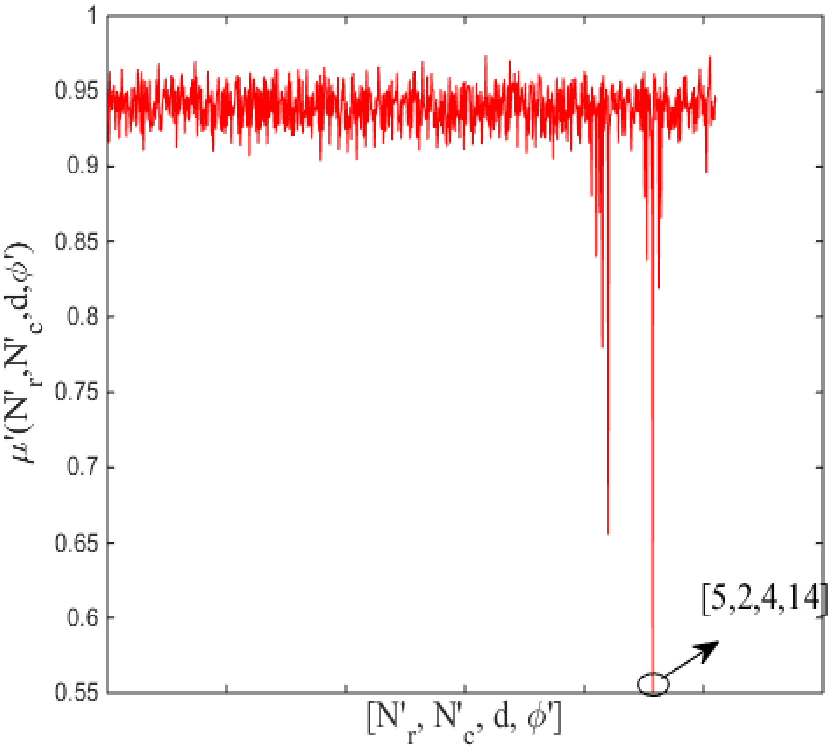
Simulation Results



- 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}.
- 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}

Simulation Results





- 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$=10^{-2}$
- 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$=10^{-2}$

NANYANG TECHNOLOGICAL UNIVERSITY

Simulation Results

Table 1: Comparison of probability of correct detection of interleaver period for RS code RS$(7, 3, 3, 11)$

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

Proposed algorithm outperforms existing algorithm

[1] 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.

NANYANG TECHNOLOGICAL UNIVERSITY

Conclusions

- Blind estimation algorithms have been proposed for estimating RS code and block interleaver parameters based on rank deficiency and normalized non-zero-mean-ratio values
- The bit/symbol positioning adjustment is also integrated with the proposed code parameter estimation algorithms
- The simulation studies show that the proposed algorithms can successfully estimate RS code and block interleaver parameters for various test cases
- Accuracy of estimation plots are shown for different M-QAM and M−PSK schemes, code dimension, and codeword length values

Observations:

- It has been inferred that the accuracy of parameter estimation improves with decrease in code dimension and codeword length values
- The lower modulation order schemes perform better then the higher modulation order schemes
- The proposed algorithm for noisy environment consistently outperforms the algorithms proposed in the prior works.

Thank you