Multinomial Distribution Based Blind Interleaver Parameters Estimation

Changryoul Choi and Jechang Jeong
Dept. of Electronic and Communication Engineering Hanyang University
Seoul, Korea
e-mail: denebchoi@gmail.com & jjeong@hanyang.ac.kr

***Abstract*— In this paper, we propose a blind interleaver parameters estimation algorithm. By modeling the distribution of the ranks of the random matrices as a multinomial distribution, we can easily identify the parameters of the interleavers blindly. Experimental results show that the proposed algorithm outperforms other blind interleaver parameter estimation algorithms.**

Keywords- interleaver; channel code; error-correcting codes; blind estimation

I. INTRODUCTION

Under the inherent channel impairments during communication, Error Correcting Codes (ECC) are indispensable for reliable transmission. In general, many ECCs are robust to the random errors but they are very weak to burst errors. For this reason, the interleaver which permutes the symbols (or bits) from several codewords so that any given codeword are well separated is introduced to handle this problem. Note that, for reliable communication, the receiver has to synchronize the data and deinterleave them before a channel decoder starts to operate [1].

In a non-cooperative context, an eavesdropper tries to find information without any knowledge of the communication parameters used. For a perfect recovery of data, one of the most important steps is blind estimation of the interleaver parameters using only the intercepted sequences.

Some algorithms exploiting the linearity of ECCs are proposed in the literature [2]-[11]. Algorithms using the properties of the dual codes are proposed in [2]-[4]. By finding a basis of a dual code by using the parity check relations, interleaver parameters can be blindly estimated. Algorithms using the linear dependence within a codeword were also proposed in [5]-[9]. Sicot et al. used both of the approaches and showed very good results [10]. Another approach exploiting the linear dependence among codewords and the specific distribution of the ranks of the random matrices are first proposed in [11]. Their algorithm, first, tries to identify errorless symbols by exploiting the distribution of the ranks of the random matrices and makes a rectangular matrix using the errorless symbols. If the interleaver period is not the same as the (horizontal) dimension of the rectangular matrix, it will have full rank. Otherwise, it does not have full rank [11].

In this paper, we propose a blind interleaver parameter estimation algorithm by modeling the distribution of the ranks of the random matrices as a multinomial distribution. By this modeling, we can transform the problem of estimating interleaver parameters into that of the probability matching. Using this probabilistic setup, we can efficiently determine interleaver parameters in a non-cooperative context.

The rest of this paper is organized as follows. Section II gives a review of some previous algorithms. In Section III, we explain our proposed algorithm. Simulation results and analyses are in Section IV, and we conclude in Section V.

II. PREVIOUS WORKS

In this section, we describe the system setup. And we explain in detail the property of linear dependence among codewords and the distribution of the ranks of the random matrices since the proposed algorithm is heavily dependent upon these properties.

A. System Setup

Let C be an (n, k, d) linear code over $GF(2)$, where n is the codeword length, k is the code dimension, d is the minimum Hamming weight of the codewords, and $GF(2)$ represents the Galois field of order 2. By linearity, we can represent any codeword $\mathbf{c} \in C$ as follows:

$$\mathbf{c} = \mathbf{m}G \tag{1}$$

where $\mathbf{c}$ is a $1 \times n$ row vector, $\mathbf{m}$ is a $1 \times k$ row vector, and G is a $k \times n$ matrix having full rank.

Since in almost all the communication systems, the interleaver size S is a multiple of the codeword size, we can represent $S = \beta n$, where β is the number of codewords within an interleaver. We assume that the channel is a Binary Symmetric Channel (BSC) with transition probability of P_e. Let l be a predicted interleaver period.

Note that the most fundamental and frequent operations of the proposed algorithm are the calculations of the ranks of the matrices. In this case, the matrix is of size $l \times (l + q)$ $(q \geq 0)$. When making a sequence into a matrix of size $l \times (l + q)$, we pile up the received symbols from leftmost top to rightmost bottom in raster scanning order.

B. Linear Dependence among Codewords

The (n, k, d) linear code C over $GF(2)$ is a k-dimensional subspace in an n-dimensional vector space. Due to this, there are k basis vectors in the n-dimensional vector space. If there are $k + 1$ codewords, at least one of the codewords can be described by the linear combination of k basis vectors. This

 ISBN: 978-1-61208-650-7

property of linear dependence among codewords can elucidate the rank behavior better than the property of linear dependence within codewords [11].

C. Distribution of the Ranks of the Random Matrices

Let the probability P_s be the probability that the rank of the $l \times l$ square matrix is $l - s$ ($s \neq 0$) when $l \to \infty$. In this case, we assume that the entries in an $l \times l$ square random matrix take the values in $GF(2)$ with equal probability. In [12], P_s is given by

$$P_s = 2^{-s^2}\left(\prod_{i=s+1}^{\infty}(1-2^{-i})\right)\left(\prod_{i=1}^{s}(1-2^{-i})^{-1}\right) \quad (2)$$

and when $s = 0$, P_0 is given by

$$P_0 = \prod_{i=1}^{\infty}(1-2^{-i}) . \quad (3)$$

Table I shows the values of P_s for some values of s. Note that as l increases, the calculated P_s rapidly converges to theoretical values. From Table I, we can see that an $l \times l$ square binary random matrix would very rarely have a rank as low as $l - s$ ($s \geq 3$).

TABLE I. P_S FOR SMALL VALUES OF S

s	P_S
0	0.288788
1	0.577576
2	0.128350
3	0.005238
4	4.65669×10^{-5}
5	9.69136×10^{-8}

If the rank of an $l \times l$ square binary matrix A happens to be ($s \geq 3$), we can assume that there are some structures in this matrix A. That is, we can presume that the matrix has $l - s - m$ ($m \geq 1$) basis vectors and m distinct errors [11]. If we plug such ideas into the blind interleaver parameters estimation algorithm, when $l = S$, low ranks can happen frequently. When $l \neq S$, the rank of matrix A follows the distribution in Table I.

III. PROPOSED ALGORITHM

As is pointed out in Section II-C, when $l = S$, the $l \times l$ square matrices would have low ranks frequently. Otherwise, i.e., when $l \neq S$, the ranks of the $l \times l$ square matrices follow the distribution in Table I. Therefore, we can consider the problem of finding the interleaver parameters as that of the probability matching. That is, when $l \neq S$, the distribution of the ranks of the $l \times l$ square matrices would be very close to the distribution in Table I. If the distribution of the ranks of the $l \times l$ square matrices is very different from the distribution in Table I, we can assume that $l = S$.

To assess the closeness between the distribution of the ranks of the $l \times l$ square matrices and the distribution in Table I, we consider the distribution in Table I as a multinomial distribution [13]. For brevity, we partition the events into 4 categories: EVENT_0 (whose rank is 0), EVENT _1 (whose rank is 1), EVENT _2 (whose rank is 2), EVENT_3 (whose rank is no less than 3). Then, we have the following table of cell probabilities in Table II.

TABLE II. PROBABILITY OF MULTINOMIAL DISTRIBUTION

$EVENT\_I$	P_{EVENT_I}
0	0.288788
1	0.577576
2	0.128350
3	0.005286

Assume that the number of trials is N and the numbers of events are (x_0, x_1, x_2, x_3) in N. Note that $N = x_0+x_1+x_2+x_3$. We assume that the random vector (x_0, x_1, x_2, x_3) follows the multinomial distribution. We also assume that the dimension of the matrices are $l \times l$. Then, the probability P_l of this random vector is calculated as follows [13]:

$$P_l = \frac{N!}{x_0!x_1!x_2!x_3!} P_{event\_0}^{x_0} P_{event\_1}^{x_1} P_{event\_2}^{x_2} P_{event\_3}^{x_3} . \quad (4)$$

Note that when the random vector follows the distribution in Table II, the probability P_m would be 1. Otherwise, its probability would be very small.

The proposed algorithm can be summarized as follows:

1) Randomly select l vectors and construct an $l \times l$ square matrix.
2) Calculate the rank s of the matrix.
3) Count the number of EVENT_i.
4) Repeat steps from 1) to 3) N times.
5) Calculate (4). If P_l is less than a predetermined threshold. Go to 7).
6) Increment l as $l + 1$ and go to 1).
7) Declare that the interleaver period is l.

Note that a predetermined threshold is calculated according to the false alarm probability.

IV. EXPERIMENTAL RESULTS

We carry out some experiments to validate the proposed algorithm. In all the experiments, we use (7, 4) binary Hamming code and random interleavers. In this case, when the interleaver period is S, the search range of the interleaver period is set from 7 to $S + 1$, and the delay parameter is chosen randomly from 0 to $S - 1$. We set the threshold (which is related to a false alarm probability) as 10^{-10}. For each Bit Error Rate (BER) the number of iterations is set to

 ISBN: 978-1-61208-650-7

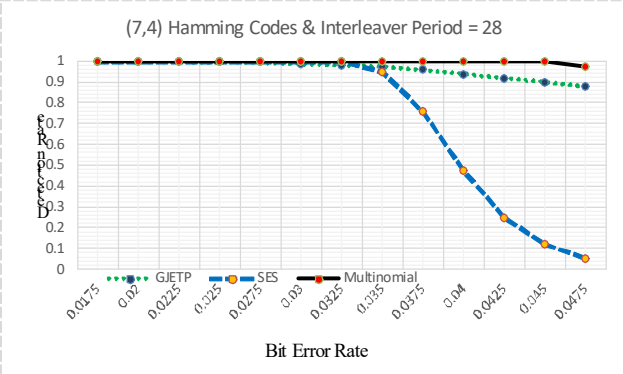

Figure 1. Detection probability for the algorithms when the interleaver size is 28.

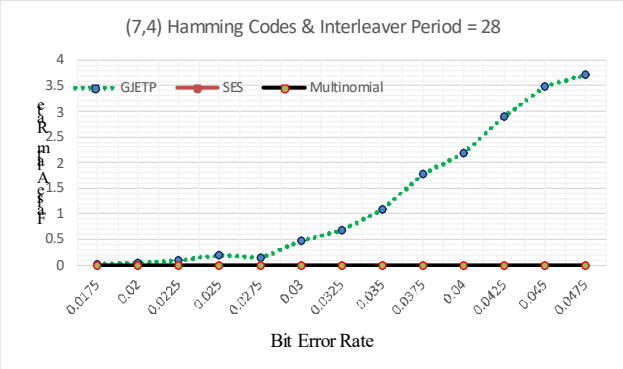

Figure 2. False alarm probability (%) for the algorithms when the interleaver size is 28.

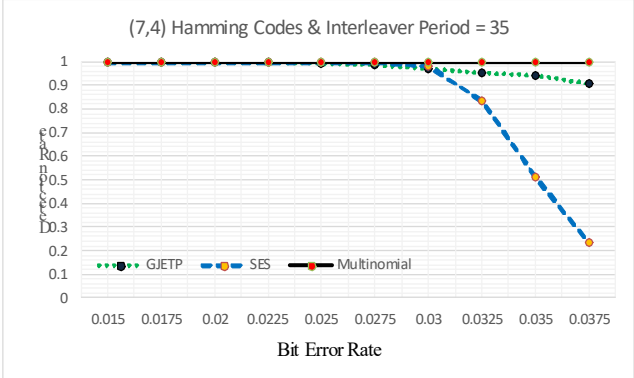

Figure 3. Detection probability for the algorithms when the interleaver size is 35.

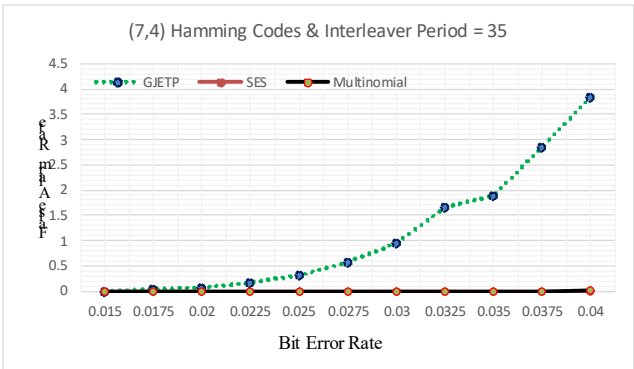

Figure 4. False alarm probability (%) for the algorithms when the interleaver size is 35.

10,000. The number of intercepted samples available is 50,000. We compared the performance of the proposed algorithm with that of Gauss-Jordan Elimination Through Pivoting (GJETP) algorithm [10] and that of the Selecting the Errorless Symbols (SES) based interleaver parameter estimation algorithm [11].

Figure 1 shows the detection performance of algorithms when the interleaver period is 28. As can be seen from the figure, the proposed algorithm outperforms the other algorithms. The false alarm probability of the proposed algorithm and the SES based algorithm is 0 over the BER range [0.0175, 0.0475] from the figure 2. On the contrary, the false alarm probability of the GJETP is relatively high and when BER is 0.0475, its false alarm probability is 3.72%.

Figure 3 shows the detection performance of algorithms when the interleaver period is 35. As with the figure 1, the proposed algorithm almost perfectly estimates the interleaver period and outperforms the other algorithms. Figure 4 shows the false alarm probabilities of the algorithms. To be specific, the false alarm events did not occur for the SES based algorithm. For the proposed algorithm, the false alarm events occurred only when BER = 0.04. In this case, the false alarm probability is 0.02%. As with the figure 2, the false alarm probability of the GJETP is relatively very high.

V. CONCLUSIONS

In this paper, we proposed an interleaver parameters estimation algorithm based on the probabilistic matching. By modeling the ranks of the random square matrices as a multinomial distribution, we can easily estimate the interleaver parameters. Experimental results show that the proposed algorithm outperforms other algorithms in terms of detection performance and the reliability.

ACKNOWLEDGMENT

This work was supported by the ICT R&D program of MSIP/IITP. [2014-0-00670, Software Platform for ICT Equipment]

REFERENCES

[1] S. B. Wicker, Error control systems for digital communications and storage, Englewood Cliffs, NJ, USA: Prentice-Hall, 1995.

[2] A. Valembois, “Detection and recognition of a binary linear code,” Discrete Applied Mathematics, vol. 111, no. 1-2, pp. 199-218, July 2001.

[3] M. Cluzeau, “Block code reconstruction using iterative decoding techniques,” in Proc. of ISIT06, Seattle, WA, USA, July 2006, pp. 2269-2273.

 ISBN: 978-1-61208-650-7

[4] M. Marazin, R. Gautier, and G. Burel, “Some interesting dual-code properties of convolutional encoder for standards for self-recognition,” IET Commun., vol. 6, no. 8, pp. 931-935, May 2012.

[5] G. Burel and R. Gautier, “Blind estimation of encoder and interleaver characteristics in a non cooperative context,” in Proc. of IASTED, Scottsdale, AZ, USA, Nov. 2003, pp. 275-280.

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

[7] R Swaminathan, A. S. Madhukumar, N. W. Teck, and C. M. S. See, “Parameter estimation of convolutional and helical interleavers in a noisy environment,” IEEE Access, vol. 5, pp. 6151-6167, May 2017.

[8] R Swaminathan, 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,” Digit. Signal Process., vol. 60, pp. 20–32, January 2017.

[9] R Swaminathan and A. S. Madhukumar, “Classification of error correction codes and estimation of interleaver parameters in a robust environment,” IEEE Trans. on Broadcast., vol. 63, no. 3, pp. 463-478, September 2017.

[10] G. Sicot, S. Houcke, and J. Barbier, “Blind detection of interleaver parameters,” Signal Processing, vol. 89, pp. 450-462, April 2009.

[11] C. Choi and D. Yoon, “Enhanced blind interleaver parameters estimation algorithm for noisy environment,” IEEE Access, vol. 6, pp. 5910-5915, 2018.

[12] V. F. Kolchin, Random Graphs, New York: Cambridge University Press, 1999.

[13] G. Casella and R. Berger, Statistical Inference, Duxbury Press, 2001.

 ISBN: 978-1-61208-650-7