Estimation of Interleaving Period for Reed-Muller Coded Signals

Yeonsoo Jang, Jinwoo Jeong, Hyeongyong Lim, and Dongweon Yoon

***Abstract*—In digital communication systems, an interleaver rearranges the bits in a channel encoded data to overcome burst errors. Since the interleaved data is encrypted for any receiver ignorant of the parameters of the interleaver, non-cooperative contexts must estimate the interleaver parameters from an unknown interleaved data. In this paper, we propose a method of estimating an interleaving period, based on the linear characteristics of Reed-Muller code. First, we calculate the ratio of '1' bits in the matrix which is generated by a Gaussian elimination process. Then, we check the minimum value of the ratio and count the number of rows that have a smaller ratio than a certain threshold. To validate the proposed method, we show the correct detection probabilities for an interleaving period in a noisy channel through computer simulations.**

***Index Terms*—Interleaver, interleaving period estimation, reed-muller code.**

I. Introduction

Channel coding and interleaving enable transmitted signals to better withstand the effects of various channel impairments such as noise and interference, and are essential in assuring the reliability of performance in digital wireless communication systems [1], [2]. In addition, for a non-cooperative context such as the military or spectrum surveillance systems, interleaving acts as an encryption process for a receiver who lacks information about the interleaver's parameters [3], [4]. In this case, the interleaved data sequence can be regarded as an unknown sequence. To deinterleave the unknown interleaved data sequence, the interleaving period has to be estimated.

If the unknown data sequence is block channel coded, the period of the interleaver can be estimated based on the linear characteristics of a block channel code in the interleaved data sequence and, in this regard, estimation methods for an interleaving period have been presented in the literature [5], [6]. The previous methods perform well for systematic blocks code such as Hamming code, because the systematic block code generates redundant bits as linear combinations of message bits and the generated codeword consists of separate message bits and redundant bits. However, for Reed-Muller (RM) code, which is a non-systematic code, an improved method is required to estimate the interleaving period because the generator matrix of RM code is distinct from that of the systematic block code [7], [8].

In this paper, we propose an estimation method for the interleaving period when RM code is adopted. The first step of our method is to fill a block matrix with a sequence that has been interleaved in an unknown manner, and perform Gaussian elimination upon it. We then evaluate the ratio of '1' bits for each row. We check the minimum value of the ratio and count the number of rows that have a smaller ratio than a certain threshold. Based on those two criteria, we determine the estimated interleaving period. In this paper, we assume that interleaver frames are synchronized. For non-synchronization cases, the proposed algorithm can be applicable by the repeating process with delay shifts of input data.

The paper is organized as follows: In Section II, we analyze a linear characteristic of RM coded sequence and propose an improved estimation method. Section III contains simulation results to verify the proposed method. Finally, conclusions are drawn in Section IV.

II. Proposed Estimation Method

Channel codes can be characterized by the generator matrices and classified into systematic codes and non-systematic codes. As an example of the systematic code, a generator matrix of (7, 4) Hamming code can be presented as

$$G_H = (I \mid P) = \begin{pmatrix} 1001011 \\ 0101110 \\ 0010111 \end{pmatrix}. \quad (1)$$

The matrix generates a 7 bits codeword every 4 message bits. Since the matrix of Hamming code is divided into the identity matrix I and the parity matrix P, the linearity of the Hamming code can be explicitly analyzed [9].

RM code, which is one of the non-systematic codes, is specified by the order of the code and the length of the massage. As an example of the non-systematic code, a generator matrix of (8, 4) RM code with the first order can be presented as

$$G_R = \begin{pmatrix} 1 \\ V_3 \\ V_2 \\ V_1 \end{pmatrix} = \begin{pmatrix} 11111111 \\ 00001111 \\ 00110011 \\ 01010101 \end{pmatrix}, \quad (2)$$

Manuscript received September 24, 2015; revised March 10, 2016. This work was supported by the Research Fund of Survivability Technology Defense Research Center of Agency for Defense Development of Korea (No. UD120019OD).

The authors are with the Department of Electronics and Computer Engineering, Hanyang University, Seoul 133-791, Korea (e-mail: ysjang83@gmail.com, jhjeong@hanyang.ac.kr, hyl@hanyang.ac.kr, dwyoon@hanyang.ac.kr).

where V_i is a basis vector. Since the linearity of RM code is implicitly presented, previous estimation method for Hamming code cannot be applicable to RM code. Thus, a modified method is required to find the linearity patterns for the estimation of the interleaving period.

Now, we analyze the linearity characteristic of RM code and propose an estimation method for the interleaving period when RM code is used. Generally, the length of an interleaving period is an integer multiple of the length of a block channel codeword to reduce the hardware complexity requirement of the transmitter and receiver as

$$N_p = s \cdot n, \tag{3}$$

where N_p is the length of the interleaving period, n is the length of the codeword, and s is the number of codewords in an interleaved sequence as an integer.

If we divide the unknown sequence into sub blocks of an arbitrary estimated interleaving period N_e and load the sub blocks into a matrix $H(N_e, 2N_e)$ column by column, then we can obtain a matrix for the estimation of the interleaving period. Fig. 1 shows an example of $H(N_e, 2N_e)$, where N_e is an arbitrary estimated interleaving period and $C_{i,j}$ is the j-th bit in the i-th codeword.

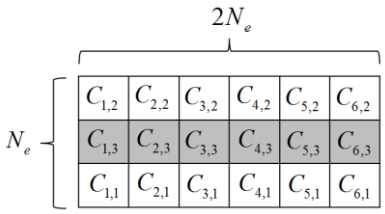

Fig. 1. Example of a matrix $H(N_e, 2N_e)$. ($N_e = 3$, $N_p = 3$).

In this example, we assume that the outputs of the interleaver are $[C_{1,2}, C_{1,3}, C_{1,1}, C_{2,2}, ..., C_{6,1}]$ when the inputs of the interleaver are $[C_{1,1}, C_{1,2}, C_{1,3}, C_{2,1}, ..., C_{6,3}]$, where the length of the codeword is 3, the length of the message bits is 2, the code rate is 2/3, and the original interleaving period is 3. In Fig. 1, the shadowed blocks are the redundant bits. When N_e is an integer multiple of N_p, the bits with same j are aligned in the same row. Then, we can find the linearity between the rows in the matrix $H(N_e, 2N_e)$ by applying Gaussian elimination. Fig. 2 show an example of a Gaussian eliminated matrix.

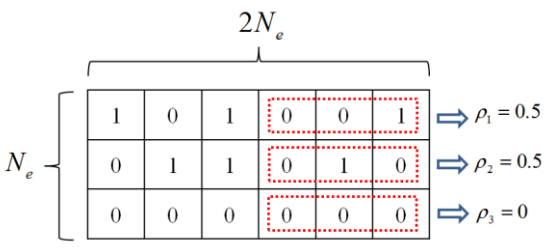

Fig. 2. Example of a Gaussian eliminated matrix.

As shown in Fig. 2, after the Gaussian elimination, there is the row having all zero elements. To determine the criteria of the estimation, we focus on the square matrix $H_S(N_e, N_e)$, which is the right side of the Gaussian-eliminated matrix and define ρ_j, $j = 1, 2, ..., N_e$ as the number of '1' bits to number of '0' bits ratio (OZR) for each row in $H_S(N_e, N_e)$. When N_e is an integer multiple of N_p, rows having OZR of 0 value exist in $H_S(N_e, N_e)$ for a noiseless channel. Fig. 3 shows the minimum OZR for a Hamming coded sequence.

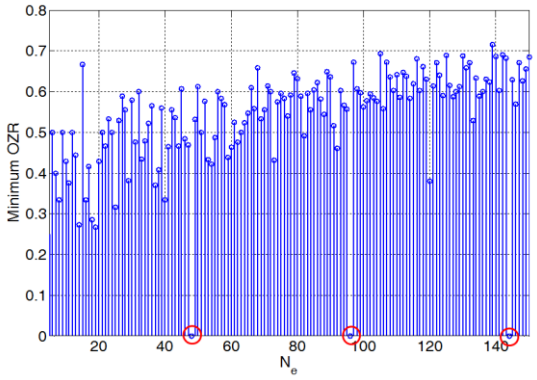

Fig. 3. Minimum OZR for Hamming code, (interleaving period=48).

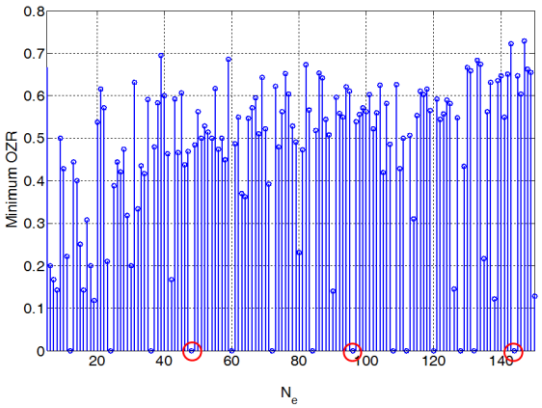

Fig. 4. Minimum OZR for RM code, (interleaving period=48).

We adopted a [16, 11] Hamming code as a channel code and used a helical scan interleaver where the step size was 1 and the period was 48. In Fig. 2, OZRs with zero value appear at the points that are integer multiples of N_p.

Fig. 4 shows the minimum OZR for an RM coded sequence.

We adopted (16, 5) RM code as a channel code and used a helical scan interleaver with a step size of 1 and a period of 48. As shown in Fig. 4, OZRs with zero value appear not only at the points that are multiples of N_p but also other points.

In this regard, to estimate the interleaving period for an RM coded sequence, additional criterion is required, and so we adopt the parameter M_{N_e}, defined as the number of rows that have an OZR of zero value in $H_S(N_e, N_e)$. For a noiseless channel, when N_e is an integer multiple of N_p, M_{N_e} is satisfied as follows.

$$\begin{aligned} M_{N_e} &= M_{i \cdot N_p} \\ &= i \cdot s \cdot \left[n - rank\left(H(N_e, 2N_e) \right) \right], \quad i = 1, 2, 3, ... \end{aligned} \tag{4}$$

Fig. 5 shows M_{N_e} for an (16, 5) RM coded sequence where N_p is 48 and s is 3.

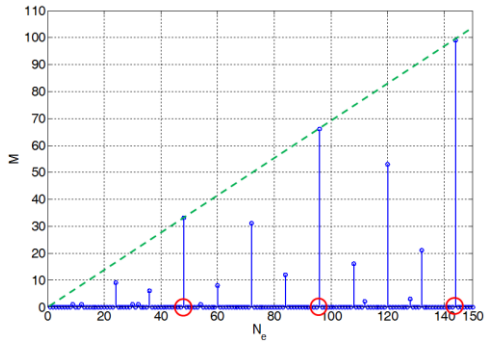

Fig. 5. M_{N_e} versus N_e, (interleaving period=48).

As shown in Fig. 5, M_{N_e} has the values 33, 66, and 99 at points $N_e = 48$, 96, 144, respectively. From Fig. 5, we can confirm that M_{N_e} at the integer multiple points of N_p satisfy Eq. 4, however, M_{N_e} at the other points of N_e cannot satisfy Eq. 4.

From the above analysis, we can summarize the proposed estimation method for a noiseless channel. First, we make a candidate set of N_e that has OZR with zero value from the Gaussian-eliminated matrix. In the candidate set, N_e having exactly multiple values of M_{N_e} at the integer multiple points is finally determined as the estimated interleaving period.

For the case of a noisy channel with acceptable errors, the minimum value of OZR slightly increases from zero and M_{N_e} has a slightly smaller value than Eq. 4 when N_e is an integer multiple of N_p. Thus, we use a threshold T_h to estimate the interleaving period and propose the estimation process as follows:

1) Make a matrix $H(N_e, 2N_e)$ by using the unknown interleaved sequence.
2) Apply Gaussian elimination to $H(N_e, 2N_e)$ and obtain $H_S(N_e, N_e)$ from the right side of the Gaussian eliminated matrix.
3) Make a candidate set of N_e where the minimum OZR is smaller than the threshold T_h.
4) Count the number of rows, M'_{N_e}, that have smaller OZR than T_h.
5) Determine N_e as the estimated interleaving period in the candidate set if M'_{N_e} is equal to or smaller than $i \cdot s \cdot \left[n - rank\left(H(N_e, 2N_e) \right) \right]$ and larger than $(i-1) \cdot s \cdot \left[n - rank\left(H(N_e, 2N_e) \right) \right]$.

III. Numerical Results

In this section, we validate the proposed estimation method by showing the simulation results for a 16x4 helical scan interleaved data sequence with a helical step size of 1 when (16, 5) and (16, 11) RM codes are used. We assume the binary symmetric cannel and run 1000 Monte Carlo simulations for each bit error rate (BER). For each simulation, 50000 randomly generated bits are used and a threshold of 0.1 is adopted.

Fig. 6 depicts the correct detection probability of interleaving period versus BER.

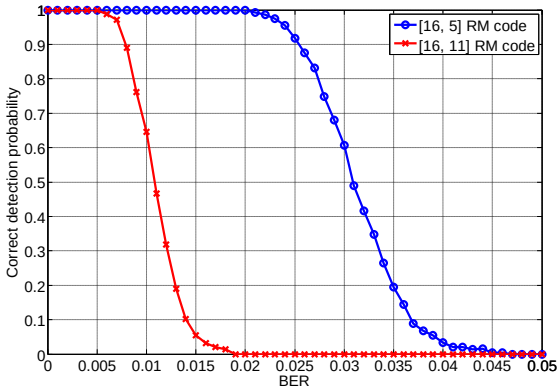

Fig. 6. Correct detection probability versus BER.

For (16, 5) RM code, the proposed method perfectly estimates the interleaving period up to a BER of 0.02 and when the BER is larger than 0.037, the proposed method can find the correct interleaving period under the detection rate of 10%. For (16, 11) RM code, the proposed method shows a correct detection probability of 1 up to a BER of 0.005 and we can see that the correct detection probability is 0.1 at a BER of 0.014. Since the proposed method performs estimation based on the linearity of RM code, the estimation performance is affected by a code rate of a channel code. From the simulation results, we confirm that the correct detection probability decreases as the code rate increase.

IV. Conclusions

In this paper, we proposed an estimation method for an interleaving period when RM code is used as a channel code. To find the interleaving period, the proposed method used a ratio of '1' bits in the Gaussian eliminated matrix, which was filled with an unknown interleaved sequence. Then, the estimated period was determined based on two criteria: The minimum value of the ratio and the number of rows that have a smaller ratio than a certain threshold. Through computer simulations, we have confirmed that the proposed method can estimate the interleaving period for RM code in practical communication systems which have the performance requirements of the BER below 10^{-3} for voice communications and the BER below 10^{-5} for data communications. Our results can be applied to practical cases of unknown signal estimation involving non-cooperative contexts such as military electronic warfare or spectrum surveillance systems.

References

[1] B. Sklar, *Digital Communications: Fundamentals and Applications*, Prentice-Hall, Upper Saddle River, NJ, 2001.
[2] G. Proakis, *Digital Communications*, McGraw-Hill, New York, 2001.
[3] J. L. Ramsey, "Realization of optimum interleavers," *IEEE Trans. Inf. Theory*, vol. 16, no. 3, pp. 338-345, 1970.

[4] R. Garello, G. Montorsi, S. Benedetto, and G. Canellieri, "Interleaver properties and their applications to the trellis complexity analysis of turbo codes," *IEEE Trans. Commun*., vol. 49, no. 5, pp. 793-807, 2001.
[5] G. Burel and G. Canellieri, "Blind estimation of encoder and interleaver characteristics in a non cooperative context," *Int. Conf. Communications, Internet and Information Technology*, pp. 275-280, 2003.
[6] G. Sicot, S. Houcke, and J. Barbier, "Blind detection of interleaver parameters," *Signal Processing*, vol. 89, issue 4, pp. 450-462, 2009.
[7] N. Alon, T. Kaufman, M. Krivelevich, S. Litsyn, and D. Ron, "Testing reed-muller codes," *IEEE Trans. Inf. Theory*, vol. 51, no. 11, pp. 4032-4039, 2005.
[8] K. Paterson, "Generalized reed-muller codes and power control in OFDM modulation," *IEEE Trans. Inf. Theory*, vol. 46, no. 1, pp. 104-120, 2000.
[9] J. Odenwalder, *Error Control Coding Handbook*, Linkabit Corporatio, San Diego, CA, 1976.

Yeonsoo Jang received the B.S. and Ph.D. degrees in electronics and computer engineering from Hanyang University, Seoul, Korea, in 2009 and 2015, respectively. Since 2015, he has been with Agency for Defense Development, Daejeon, Korea. His research interest includes signal processing, digital communications theory, and FPGA implementation of radar and communication system.

Jinwoo Jeong received the B.S. and M.S. degrees in electronics and computer engineering from Hanyang University, Seoul, Korea in 1999 and 2001, respectively. During 2001-2007, he worked at Digital Media Laboratory, LG Electronics Inc., Korea. He is currently working toward a Ph.D. degree in the Department of Electronics and Computer Engineering of Hanyang University, Seoul, Korea. His research interests lie in the field of military communications systems, signal intelligence, electronic warfare, and satellite and deep space communications.

Hyeongyong Lim received the B.S. degree in electronic engineering from Hanyang University, Seoul, Korea, in 2012. He is currently pursuing the integrated M.S. and Ph.D. degrees in the Department of Electronics and Computer Engineering, Hanyang University. His research interests are in digital communication system, wireless communication theory, and statistical signal processing.

Dongweon Yoon received the B.S. (summa cum laude), M.S. and Ph.D. degrees in electronic communications engineering from Hanyang University, Seoul, Korea, in 1989, 1992 and 1995, respectively. From March 1995 to August 1997, he was an assistant professor in the Department of Electronic and Information Engineering of Dongseo University, Pusan, Korea. From September 1997 to February 2004, he was an associate professor in the Department of Information and Communications Engineering of Daejeon University, Daejeon, Korea. Since March 2004, he has been on the faculty of Hanyang University, Seoul, Korea, where he is now a professor in the Department of Electronic Engineering and the Director of Signal Intelligence Research Center. He has twice been an invited researcher at the Electronics and Telecommunications Research Institute (ETRI), Daejeon, Korea (February-December 1997, November 2002-December 2005). He was a visiting professor at the Pennsylvania State University, University Park, Pennsylvania, for the academic year 2001-2002, and was a visiting professor at the University of California, Riverside, California, for the academic year 2010-2011. His research interests include new modulation techniques, accurate performance evaluations, digital communications theory and system, satellite and space communications, wireless communications, and signal intelligence.