

Reconstruction Method for Reed-Muller Codes Using Fast Hadamard Transform

I.S. KANG*, H. LEE*, S.J. HAN**, C.S. PARK***, J.H. SOH***, Y.J. SONG*

*Electronic Engineering, KIT (Kumoh National Institute of Technology), Korea

**LIG Nex 1, Korea

***ADD (Agency for Defence Development), Korea

yjsong@kumoh.ac.kr

Abstract— The use of an error-correcting code is essential in communication systems where the channel is noisy. We present a new technique to reconstruct RM (Reed-Muller) codes from a noisy intercepted bit stream. RM codes have several decoding methods, including a method that uses the FHT (Fast Hadamard Transform). The FHT algorithm is composed of several butterfly operations. To verify whether or not a received code is RM, FHT is first performed assuming that the code is first-order RM. If the received code is a higher order RM other than first-order, we perform FHT after the removal of the masking components. We verified our proposed algorithm by performing intensive computer simulations.

Keywords— RM code, FHT, masking component, butterfly operation

I. INTRODUCTION

The use of an error-correcting code is mandatory in communication systems where the channel is noisy. This code adds redundant bits to the information to protect it from noise. The channel coding methods can be divided into block coding methods and convolutional coding methods. To perform decoding without the channel coding information, we must find the parameters and identify the channel coding type. We present a new technique to reconstruct RM (Reed-Muller) codes from a noisy intercepted bit stream.

RM codes have several decoding methods, including a method that uses the FHT (Fast Hadamard Transform). The FHT algorithm is composed of several butterfly operations [1]-[2]. For RM codes, the peak position of the FHT results is used to decode the RM code. This peak amplitude is referred to as the FHT operation and the order of RM codes. In noiseless channel condition, the peak value is given by $\alpha = 2^\beta$, where β is the number of stages for the FHT operation. For example, if an RM code performs the 3-stages FHT, the peak value is eight since the generation basis elements of RM code are similar to the row vectors of the Hadamard matrix. If we perform FHT by assuming a random non-RM code to be RM code, the resulting peak value is half of α . RM code is classified on the basis of this characteristic. To verify whether or not a received code is RM, FHT is first performed by assuming that the code is RM. After observing

the resulting peak value, we can conclude that the code is RM if the peak value is the same as the assumed α . For a first-order RM code, the classification is performed assuming that the code length is α . If the received code is a higher order RM code other than first-order, we perform FHT after the removal of the masking components. This method can recognize all the RM codes. We verified our proposed algorithm by performing intensive computer simulations.

II. BASIS OF RM CODE AND HADAMARD CODE

In general, RM codes have an excellent minimum distance property although they have a simple encoding structure [3]-[4]. An RM code is denoted $RM(r, m)$, where r is the order of the code, and m is a parameter related to the length of the code; this relation is given by $n = 2^m$. The minimum distance of the $RM(r, m)$ code is 2^{m-r} . To encode an RM code, k basis vectors are needed where

$$k = 1 + \binom{m}{1} + \binom{m}{2} + \dots + \binom{m}{r}. \quad (1)$$

For example, the basis vectors of the $RM(1,3)$ code are

$$\begin{aligned} 1 &= (1111111) \\ V_3 &= (00001111) \\ V_2 &= (00110011) \\ V_1 &= (01010101) \end{aligned} \quad (2)$$

and the vectors are used as row vectors of the generator matrix of the RM code. For a second-order RM code, additional basis vectors are constructed using the basis vectors of (2). The basis vectors of the $RM(2,3)$ code are given by (3).

To illustrate the relationship between an RM code and a Hadamard code, consider the 8×8 Hadamard matrix of (4). The basis vectors h_1, h_2, h_4 can be used as row vectors of the generator matrix of the Hadamard code of length 8 by simply replacing + by 0 and - by 1.

$$\begin{aligned}
1 &= (11111111) \\
V_3 &= (00001111) \\
V_2 &= (00110011) \\
V_1 &= (01010101) \\
V_3V_2 &= (00000011) \\
V_3V_1 &= (00000101) \\
V_2V_1 &= (00010001)
\end{aligned} \quad (3)$$

$$H_8 = \begin{bmatrix} + & + & + & + & + & + & + & + \\ + & - & + & - & + & - & + & - \\ + & + & - & - & + & + & - & - \\ + & - & - & + & + & - & - & + \\ + & + & + & + & - & - & - & - \\ + & - & + & - & - & + & - & + \\ + & + & - & - & - & - & + & + \\ + & - & - & + & - & + & + & - \end{bmatrix} = \begin{bmatrix} h_0 \\ h_1 \\ h_2 \\ h_3 \\ h_4 \\ h_5 \\ h_6 \\ h_7 \end{bmatrix} \quad (4)$$

All the row vectors of the Hadamard matrix can be constructed using the three basis vectors h_1, h_2, h_4 that correspond to the basis vectors V_1, V_2, V_3 of the RM(1,3) code. Using this mapping relationship, we can use the FHT to decode an RM code [5].

III. DECODING OF RM CODE USING FHT

When one of the row vectors of an $n \times n$ Hadamard code is received, FHT can be used to determine to which vector it corresponds. The basic operation of FHT is the butterfly operation depicted in Fig. 1.

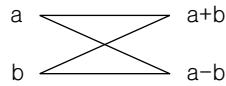


Figure 1. Butterfly operation

Fig. 2 shows the FHT for a Hadamard code of length 8.

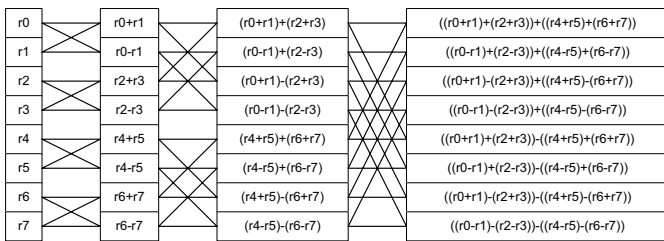


Figure 2. Fast Hadamard Transform

If the received vector is a first-order RM code, we can estimate the information bits of the code using the FHT and the basis mapping relationship. By detecting the minus or plus

peak output of FHT, we find whether the first information bit corresponding to all-one basis vector is zero or one.

The basis vectors of a second-order RM code are composed of the basis vectors of a first-order RM code and additional vectors obtained by the combination of basis vectors. The additional vectors are often called masking components. If the masking components of a second-order RM code are removed, it becomes a first-order RM code. When one or more masking components are removed, we can estimate the transmitted information bits by detecting the peak value of the FHT. The decoding process of the RM code is shown in Fig. 3 [6].

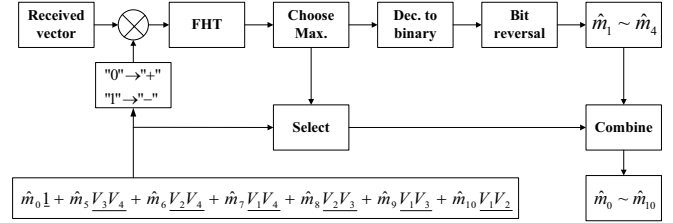


Figure 3. Decoding of RM code using FHT

IV. CODE RECOGNITION USING FHT

A. Recognition of first-order RM code

In the process of decoding an RM code using FHT, the magnitude of the FHT output is important. The output has two values: zero and α when the noiseless channel is used. If the received code is not RM or random, the average magnitude of the FHT output is $\alpha/2$. Hence, we can determine whether or not the received code is RM. Fig. 4 shows the code recognition process for a first-order RM code.

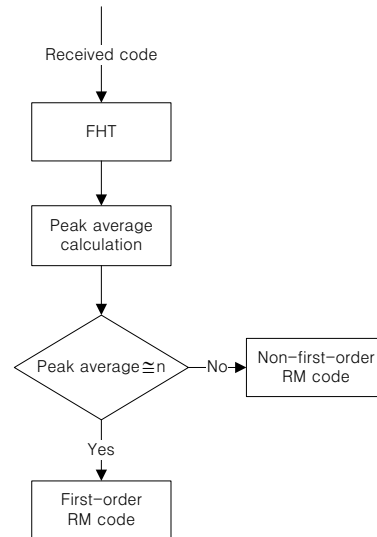


Figure 4. Recognition process for first-order RM code

B. Recognition of second-order RM code

As shown in Fig. 5, the recognition process for second-order RM codes is similar to that for first-order codes except that the masking components must be considered. If the masking vectors are removed, the recognition process is exactly the same as that for first-order RM codes.

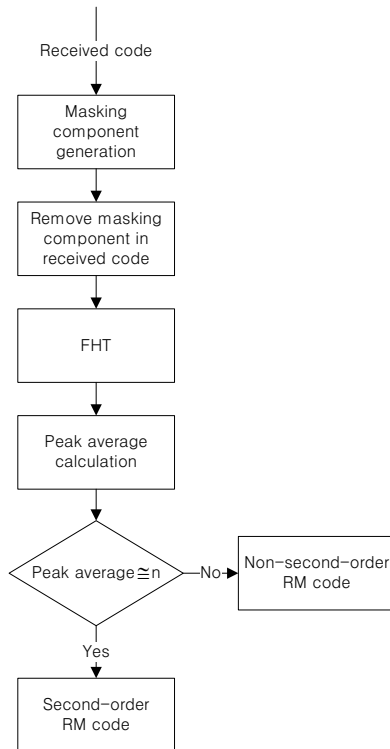


Figure 5. Recognition process for second-order RM code

V. SIMULATION

To verify the proposed recognition algorithm, we performed simulation for various RM codes in the AWGN (Additive White Gaussian Noise) channel. We ran the simulation 100 times from -5 dB to 15 dB at steps of 1 dB and found the mean value for each step. Fig. 6 shows the simulation results for various RM codes and a random code. At high SNR, the average FHT peak value for first-order RM codes approaches α . However the average peak value of second-order RM codes is much lower than that of first-order RM codes. The value for random codes approaches $\alpha/2$. But at low SNR, the average FHT peak values are higher than α and the gap between the values becomes close. Hence, at low SNR, RM code recognition becomes difficult. The simulations show that the average peak value of the FHT output is the same for different first-order RM codes. However, it varies between the first- and second-order RM codes. Hence, by setting a threshold value as $\alpha - \Delta$, we can determine the type of the RM code, where Δ is a parameter related to the performance of code recognition. Fig. 7 shows the average FHT peak values for the various second-order RM

codes and a random code after the removal of the masking components.

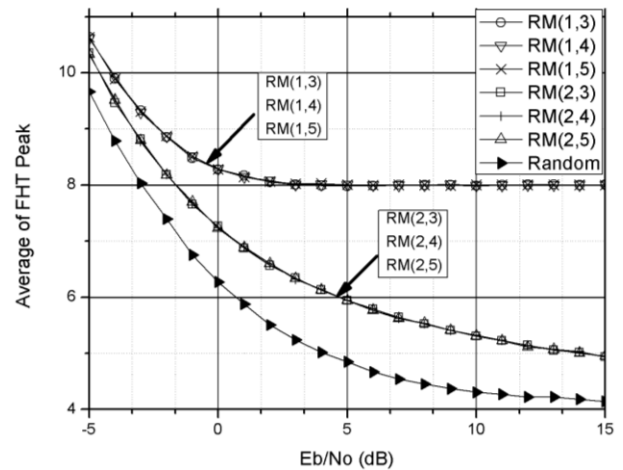


Figure 6. Average peak values of FHT output in AWGN channel

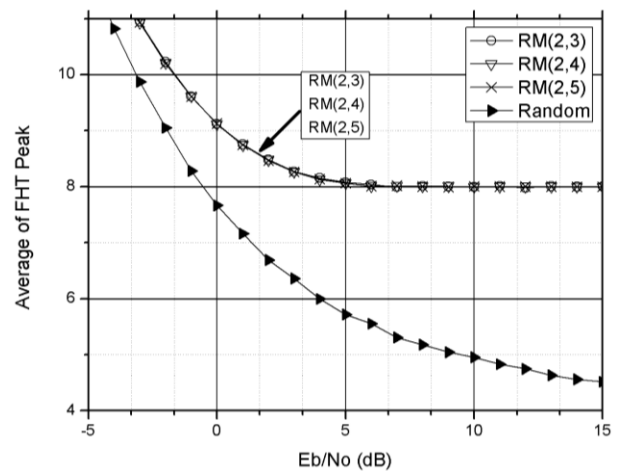


Figure 7. FHT peaks after removal of masking components

VI. CONCLUSIONS

When the parameters of the channel coding are unknown at receiver side, decoding is difficult. This paper proposed a recognition algorithm to determine whether or not a received code is RM code by using FHT with unknown channel coding parameters. Since the proposed method is based on the FHT, it can be applied to the decoding of RM codes. The performance of the algorithm was verified via simulation. If E_b/N_0 is higher than 5 dB, the average peak value of the FHT output for first-order RM codes approaches α . However, non-first-order RM codes approach $\alpha/2$. Hence, by setting an appropriate threshold value, we can determine whether or not an unknown code is first-order RM. If we remove the masking components, we can also determine whether or not an unknown code is second-order RM code.

REFERENCES

- [1] N. Ahmed and K. R. Rao, Orthogonal Transforms for Digital Signal Processing, Springer, 1975.
- [2] Nasir Ahmed Ahmed and T. Natarajan, Discrete-Time Signals and Systems, Reston, 1983.
- [3] S. Lin and D. J. Costello, Error Control Coding: Fundamentals and Applications, Prentice Hall, Inc., 1983.
- [4] Robert H. Morelos-Zaragoza, The Art of Error Correcting Coding, John Wiley & Sons, Ltd, 2007.
- [5] Y. J. Song, Coding Theory for Communications Engineering, Infinity Books, 2008.
- [6] Young-Joon Song, "Optimized Channel Coding of Control Channels for Mobile Packet Communication", Journal of the Korea Electromagnetic Engineering Society, vol. 3, no. 1, May 2003.