International Journal of Multimedia and Ubiquitous Engineering
Vol. 9, No. 10 (2014), pp. 91-100
http://dx.doi.org/10.14257/ijmue.2014.9.10.09

Hybrid Maximum Likelihood Decoding for Linear Block Codes

Young Joon Song

Department of Electronic Engineering,
Kumoh National Institute of Technology,
1 Yangho-dong, Gumi, Gyungbuk, 730-71, Korea
yjsong@kumoh.ac.kr

Abstract

In this paper we propose a hybrid maximum likelihood decoding (MLD) for linear block codes. For the reliable data transmission over noisy channels, convolutional and block codes are widely used in most digital communication systems. Much more efficient algorithms have been found for using channel measurement information in the decoding of convolutional codes than in the decoding of block codes. Word correlation method can be utilized to use channel measurement information in the decoding of block codes. However as the number of code words becomes larger, the decoding complexity increases dramatically to the power of the number of information bits. The hybrid maximum likelihood decoding can solve the problem of the hardware complexity as well as the computational time. Simulation result for Reed Muller code is presented to demonstrate the effectiveness of the algorithm.

Keywords: *Block code, hybrid maximum likelihood decoding, channel measurement information*

1. Introduction

In most modern digital communication systems, various error correction coding schemes are adopted to improve system performance [1-5]. There are two distinct error correction coding methods: convolutional and block codes [6-9]. The most important difference in terms of decoding between two codes is that the convolutional code can use channel measurement information more efficiently than block codes. Viterbi algorithm and BCJR algorithm can be used to decode convolutional codes [10-11].

Wolf presented the maximum likelihood decoding (MLD) of linear block codes using channel measurement information, which is very practical in decoding high-rate codes since the complexity of the algorithm is upper-bounded by a function of the number of parity symbols [9]. Using the algorithm, we can perform MLD of any (n, k) linear block code over GF (q) using the Viterbi algorithm applied to a trellis having no more than $q^{(n-k)}$ states. For example, if this method is applied to a (23, 11) binary Golay code, we need a trellis with 2^{12} states to do MLD using channel measurement information. In this case, the decoding complexity is higher than the word correlation decoding which requires 2^{11} correlations. Thus the Wolf's method is not so effective for medium-rate or low-rate codes.

In this paper we propose a hybrid maximum likelihood decoding (H-MLD) for linear block codes. This method divides a generator matrix of a linear block code into two sub-generator matrices. One sub-generator matrix is used to construct a parallel correlation bank and the parallel correlation is repeated for every code word generated from the other sub-generator matrix. And then we estimate the transmitted message with affordable hardware complexity while maintaining the same performance of MLD.

ISSN: 1975-0080 IJMUE

The algorithm described here is very efficient for a linear block code when the code rate is not high-rate. An experimental result for a Reed Muller code is presented to demonstrate the effectiveness of the algorithm.

2. Maximum Likelihood Decoding

Assume a code word $\boldsymbol{c} = (c_1, c_2, \dots, c_n)$of an (n, k) linear block code C is transformed into a binary antipodal signal $\boldsymbol{x} = (x_1, x_2, \dots, x_n)$ with $x_i = (-1)^{c_i}$, and the signal is transmitted over additive white Gaussian noise (AWGN) channel. Then a received signal $\boldsymbol{r} = (r_1, r_2, \dots, r_n)$ is represented as $r_i = x_i + n_i$ where $n_i$is an independent and identically distributed Gaussian random variable with zero mean and variance σ^2. Then if we use maximum likelihood decoding, the optimum decoded word $d = (d_1, d_2, \dots, d_n)$ is given by [12]

$$\boldsymbol{d} = \boldsymbol{c}^{(i)} \text{if} \left|\boldsymbol{r} - \boldsymbol{c}^{(i)}\right|^2 \le \left|\boldsymbol{r} - \boldsymbol{c}^{(j)}\right|^2 \quad \forall j \in [1, 2^k],\ i \ne j \tag{1}$$

where $\boldsymbol{c}^{(i)} = (c_1^{(i)}, c_2^{(i)}, \dots, c_n^{(i)})$ is the i-th (n, k) linear block code and the squared Euclidean distance between $\boldsymbol{r}$ and $\boldsymbol{c}^{(i)}$ is

$$\left|\boldsymbol{r} - \boldsymbol{c}^{(i)}\right|^2 = \sum_{t=1}^{n} (r_t - x_t^{(i)})^2. \tag{2}$$

If we use an exhaustive search for the optimum code word $\boldsymbol{d}$, the computational complexity increases dramatically and becomes unrealistic for the long information bits. To solve this problem, Chase proposed an algorithm of low complexity for near maximum likelihood decoding of linear block codes [13]. This algorithm limited the reviewed code words of (1) to those in the sphere of radius $(\delta - 1)$, where δ is the minimum distance of the code. Chase used the channel information to reduce the number of reviewed code words within the sphere. However this method does not always achieve maximum likelihood decoding.

Afterwards, Wolf presented the maximum likelihood decoding of linear block codes using a trellis which is efficient in decoding high-rate codes [9]. Using the algorithm, we can perform maximum likelihood decoding of any (n, k) linear block code over GF (q) using the Viterbi algorithm applied to a trellis having no more than $q^{(n-k)}$ states. The following is the Wolf's algorithm. Denote the elements of the finite field GF (q) as $\alpha_j, j = 0,1,2, \dots, (q-1)$. Let $\boldsymbol{H}$be a parity check matrix of a (n, k) linear code over GF (q) and $\boldsymbol{h}_i$, $i = 1,2, \dots, n$ are $(n-k)$-tuples with elements from GF(q). Constructing a trellis for a linear code is based on the concept $\boldsymbol{c}\boldsymbol{H}^T = 0$. Each distinct code word corresponds to a distinct path in the trellis. Using the following 3 steps, we can construct a trellis of a linear code:

Step 1) At depth k, the trellis contains only one node, namely $\boldsymbol{s}_0(0)$, the all-zero $(n-k)$-tuple.

Step 2) For each $k = 0,1, \dots, (n-1)$, the collection of nodes at depth $(k+1)$ is obtained from the collection of nodes at depth k by the formula

$$\boldsymbol{s}_l(k+1) = \boldsymbol{s}_i(k) + \alpha_j \boldsymbol{h}_{k+1}, \tag{3}$$

for all $i \in I_k$ and $j = 0,1, \ldots, (q-1)$, where $I_k \in \{0,1, \ldots, (q^{(n-k)} - 1)\}$.

Step 3) Remove any nodes that do not have a path to the all-zero state at depth n, and remove all lines drawn to these expurgated nodes.

For example, consider a (5, 2) linear block code with parity check matrix

$$\boldsymbol{H} = \begin{bmatrix} 10100 \\ 11010 \\ 01001 \end{bmatrix} = [\boldsymbol{h}_1 \boldsymbol{h}_2 \boldsymbol{h}_3 \boldsymbol{h}_4 \boldsymbol{h}_5].$$

Figure 1 shows the constructed trellis before expurgation of nodes after step 2. If we perform the final step, we obtain the expurgated trellis of figure 2 where the Viterbi algorithm can be used.

However, when this method is applied to a (30, 14) binary code, we need a trellis with 2^{16} states to do maximum likelihood decoding using channel measurement information. In this case, the decoding complexity is higher than the word correlation decoding which requires 2^{14} correlations. Thus the Wolf's method seems unrealistic for this case.

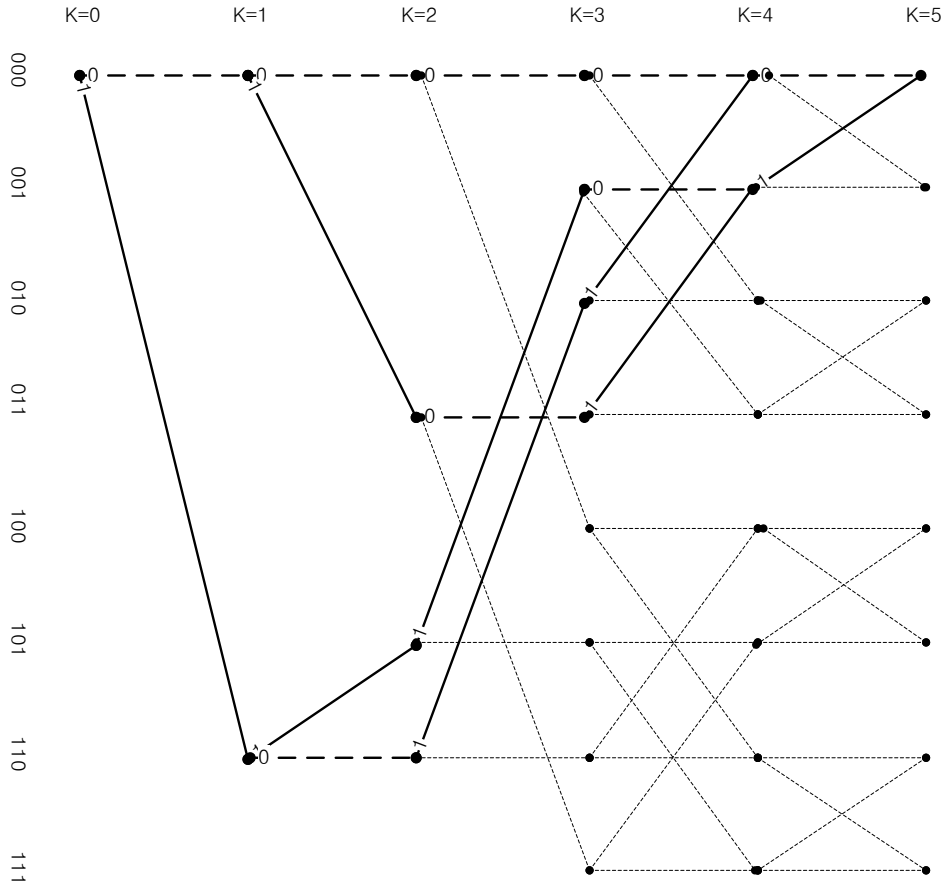

Figure 1. Trellis for Binary (5, 2) Linear Block Code before Expurgation

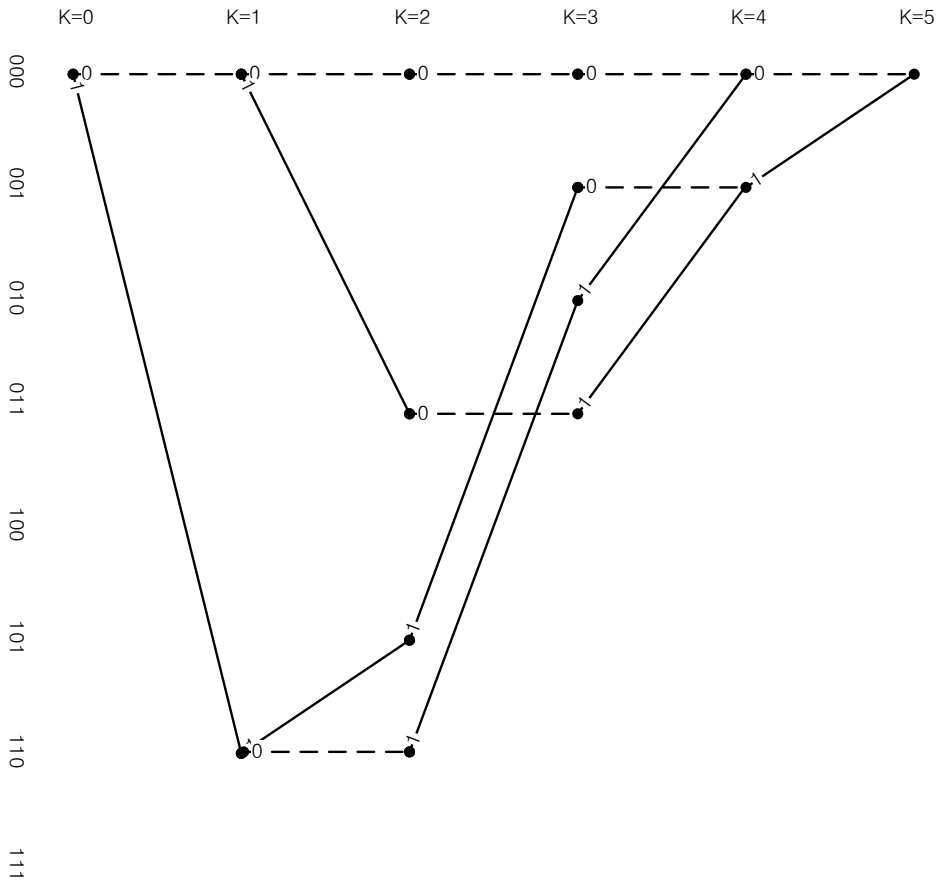

Figure 2. Expurgated Trellis for Binary (5, 2) Linear Block Code

3. Hybrid MLD

We can obtain the optimum decoded word $d = (d_1, d_2, \ldots, d_n)$using (1) and the squared Euclidean distance between $\boldsymbol{r}$ and $\boldsymbol{c}^{(i)}$ is

$$\left|\boldsymbol{r} - \boldsymbol{c}^{(i)}\right|^2 = \sum_{t=1}^{n}(r_t - x_t^{(i)})^2 = \sum_{t=1}^{n}(r_t^2 + {x_t^{(i)}}^2 - 2r_t x_t^{(i)}). \quad (4)$$

Since, $r_t^2 + {x_t^{(i)}}^2$ is constant for all code words, the optimum decoded word becomes

$$\boldsymbol{d} = \boldsymbol{c}^{(i)} \text{if} \langle \boldsymbol{r}, \boldsymbol{c}^{(i)} \rangle \geq \langle \boldsymbol{r}, \boldsymbol{c}^{(j)} \rangle \quad \forall j \in [1, 2^k],\ i \neq j \quad (5)$$

where the correlation between $\boldsymbol{r}$ and $\boldsymbol{c}^{(i)}$ is

$$\langle \boldsymbol{r}, \boldsymbol{c}^{(i)} \rangle = \sum_{t=1}^{n} r_t x_t^{(i)}. \quad (6)$$

Thus minimum Euclidean distance means maximum correlation and we use correlation instead of Euclidean distance to find optimum decoded word.

Let $\boldsymbol{G}$ be a$k \times n$ generator matrix of an (n, k) binary linear block code given by

$$\boldsymbol{G} = \begin{bmatrix} \boldsymbol{g}_1 \\ \boldsymbol{g}_2 \\ \vdots \\ \boldsymbol{g}_k \end{bmatrix}$$

where $\boldsymbol{g}_i$, $i = 1,2,\dots,k$, are n-tuples and $\boldsymbol{m} = (m_1, m_2, \dots, m_k)$ be a k-tuple message. Then the code word for the message is represented by

$$\boldsymbol{c} = \boldsymbol{mG} = m_1\boldsymbol{g}_1 + m_2\boldsymbol{g}_2 + \cdots + m_k\boldsymbol{g}_k. \quad (7)$$

We divide the $\boldsymbol{G}$ matrix into two sub-matrices $\boldsymbol{G}_1$ and $\boldsymbol{G}_2$

$$\boldsymbol{G}_1 = \begin{bmatrix} \boldsymbol{g}_1 \\ \vdots \\ \boldsymbol{g}_{k_1} \end{bmatrix}$$

$$\boldsymbol{G}_2 = \begin{bmatrix} \boldsymbol{g}_{k_1+1} \\ \vdots \\ \boldsymbol{g}_{k_1+k_2} \end{bmatrix}$$

where $k = k_1 + k_2$. Accordingly we divide the $\boldsymbol{m} = (m_1, m_2, \dots, m_k)$ k-tuplemessage into $\boldsymbol{m}_1 = (m_1, \dots, m_{k_1})$ k_1 -tuple and $\boldsymbol{m}_2 = (m_{k_1+1}, \dots, m_{k_1+k_2})$ k_2 -tuple. Two n-tuples $\boldsymbol{c}_1$ and $\boldsymbol{c}_2$ are generated by

$$\boldsymbol{c}_1 = \boldsymbol{m}_1\boldsymbol{G}_1 = m_1\boldsymbol{g}_1 + \cdots + m_{k_1}\boldsymbol{g}_{k_1} \quad (8)$$

$$\boldsymbol{c}_2 = \boldsymbol{m}_2\boldsymbol{G}_2 = m_{k_1+1}\boldsymbol{g}_{k_1+1} + \cdots + m_{k_1+k_2}\boldsymbol{g}_{k_1+k_2}. \quad (9)$$

And we find that

$$\boldsymbol{c} = \boldsymbol{c}_1 + \boldsymbol{c}_2 = (c_{1,1} + c_{2,1}, c_{1,2} + c_{2,2}, \dots, c_{1,n} + c_{2,n}) \quad (10)$$

An element-wise multiplication between the received signal $\boldsymbol{r} = (r_1, r_2, \dots, r_n)$ and an n-tuple $\boldsymbol{c}_1 = (c_{1,1}, c_{1,2}, \dots, c_{1,n})$ isdefined by

$$\boldsymbol{b} = \boldsymbol{r}.* \boldsymbol{c}_1 = (r_1x_{1,1}, r_2x_{1,2}, \dots, r_nx_{1,n}) \quad (11)$$

with $x_{1,i} = (-1)^{c_{1,i}}$.Correlating two n-tuples $\boldsymbol{b}$and $\boldsymbol{c}_2$,from (10)we find that

$$\langle \boldsymbol{b}, \boldsymbol{c}_2 \rangle = \sum_{t=1}^{n} r_t x_{1,t}\, x_{2,t} = \sum_{t=1}^{n} r_t x_t = \langle \boldsymbol{r}, \boldsymbol{c} \rangle. \quad (12)$$

If we define the set of 2^{k_1} code words of n-tuples $\boldsymbol{c}_1$ as

$$\boldsymbol{C}_1 = \begin{bmatrix} \boldsymbol{c}_1^{(1)} \\ \boldsymbol{c}_1^{(2)} \\ \vdots \\ \boldsymbol{c}_1^{(2^{k_1})} \end{bmatrix}$$

then the element-wise multiplications between the received signal $\boldsymbol{r}$ and $\boldsymbol{C}_1$ are expressed as

$$\boldsymbol{B} = \boldsymbol{r} .* \boldsymbol{C}_1 = \begin{bmatrix} \boldsymbol{b}^{(1)} \\ \boldsymbol{b}^{(2)} \\ \vdots \\ \boldsymbol{b}^{(2^{k_1})} \end{bmatrix} = \begin{bmatrix} \boldsymbol{r} .* \boldsymbol{c}_1^{(1)} \\ \boldsymbol{r} .* \boldsymbol{c}_1^{(2)} \\ \vdots \\ \boldsymbol{r} .* \boldsymbol{c}_1^{(2^{k_1})} \end{bmatrix}. \quad (13)$$

Matrix $\boldsymbol{B}$ is a memory bank of 2^{k_1} n-tuples. Let the parallel operation between memory bank $\boldsymbol{B}$ and $\boldsymbol{c}_2^{(j)}$ for a given $\boldsymbol{m}_2^{(j)} = (m_{k_1+1}^{(j)}, \dots, m_{k_1+k_2}^{(j)})$ be

$$\langle \boldsymbol{B}, \boldsymbol{c}_2^{(j)} \rangle = \begin{bmatrix} \langle \boldsymbol{b}^{(1)}, \boldsymbol{c}_2^{(j)} \rangle \\ \vdots \\ \langle \boldsymbol{b}^{(i)}, \boldsymbol{c}_2^{(j)} \rangle \\ \vdots \\ \langle \boldsymbol{b}^{(2^{k_1})}, \boldsymbol{c}_2^{(j)} \rangle \end{bmatrix}. \quad (14)$$

If the correlation $\langle \boldsymbol{b}^{(i)}, \boldsymbol{c}_2^{(j)} \rangle$ is the maximum value in (14), we store the maximum correlation value and its corresponding $\boldsymbol{m}_1^{(i)} = (m_1^{(i)}, \dots, m_{1+k_1}^{(i)})$ k_1-tuple along with the given $\boldsymbol{m}_2^{(j)} = (m_{k_1+1}^{(j)}, \dots, m_{k_1+k_2}^{(j)})$ k_2-tuple. If this operation is performed for all $\boldsymbol{c}_2^{(j)}$, $1 \le j \le 2^{k_2}$, then we have 2^{k_2} indiceswith local maximum correlation values where we can choose one maximum correlation value and its index from which we obtain the optimum code word $\boldsymbol{c} = \boldsymbol{c}_1^{(i)} + \boldsymbol{c}_2^{(j)}$ and its corresponding k bits message $\boldsymbol{m} = (\boldsymbol{m}_1^{(i)}, \boldsymbol{m}_2^{(j)})$.

3.1. Decoding Algorithm

Using the following 5 steps, we can achieve maximum likelihood decoding for a linear block code.

Step 1) Divide the $\boldsymbol{G}$ matrix into two sub-matrices $\boldsymbol{G}_1$ and $\boldsymbol{G}_2$with $k = k_1 + k_2$.

Step 2) Construct a memory bank of $2^{k_1}$$n$-tuples $\boldsymbol{B}$.

Step 3) Perform parallel operation between memory bank $\boldsymbol{B}$ and $\boldsymbol{c}_2^{(j)}$ for$\boldsymbol{m}_2^{(j)}$.

Step 4) Store the maximum correlation value from $\langle \boldsymbol{B}, \boldsymbol{c}_2^{(j)} \rangle$ and its corresponding$\boldsymbol{m}_1^{(i)}$$k_1$-tuple along with the given$\boldsymbol{m}_2^{(j)}$. If this is done for all $\boldsymbol{c}_2^{(j)}$,$1 \le j \le 2^{k_2}$, then go to Step 5). Otherwise go to Step 3).

Step 5) From 2^{k_2} indices with local maximum correlation values, we choose one maximum correlation value and its index from which we obtain the optimum code word $\boldsymbol{c} = \boldsymbol{c}_1^{(i)} + \boldsymbol{c}_2^{(j)}$and its corresponding k bits message $\boldsymbol{m} = (\boldsymbol{m}_1^{(i)}, \boldsymbol{m}_2^{(j)})$.

3.2. Application of the Algorithm

Consider a Reed Muller (RM) code to illustrate the effectiveness of the proposed algorithm. The RM code used in [14] is RM(r, m) = RM(2,5). The length of the code is $n = 2^m = 32$ and the number of information bits is [6]-[8]

$$k = 1 + \binom{m}{1} + \binom{m}{r} = 16. \tag{15}$$

The RM(2,5) code becomes systematic form using some elementary row operations. After removing the first two information bits becomes (30, 14) RM code. The systematic form of the generator matrix of the code is

$$\boldsymbol{G} = \begin{bmatrix} \boldsymbol{g}_1 \\ \boldsymbol{g}_2 \\ \vdots \\ \boldsymbol{g}_{14} \end{bmatrix} = [\boldsymbol{I}_{14} | \boldsymbol{P}] \tag{16}$$

And the parity check matrix of the code is

$$\boldsymbol{H} = [\boldsymbol{P}^T | \boldsymbol{I}_{16}] \tag{17}$$

where $\boldsymbol{I}_k$ is the identity matrix of size $k$and

$$\boldsymbol{P} = \begin{bmatrix} 1001101101100000 \\ 0010110111100000 \\ 1111110000100000 \\ 1110000000111100 \\ 1001100000111010 \\ 0101010000110110 \\ 0010110000101110 \\ 1111111111011111 \\ 1000001100111001 \\ 0100001010110101 \\ 0010000110101101 \\ 0001001001110011 \\ 0000100101101011 \\ 0000010011100111 \end{bmatrix}.$$

The m basis vectors of RM(r, m) code are equal to those of Walsh code of length $n = 2^m$ [15]. So we can use the FHT (Fast Hadamard Transform) to decode RM(r, m) [16]. The computational complexity using FHT for RM(r, m) requires $m \cdot 2^{k-m}$ correlations and this means $5 \cdot 2^{11}$ correlations for RM(2,5) code. However, it is not easy to use FHT (Fast Hadamard Transform) for the shortened (30, 14) RM code because (30, 14) code is encoded in systematic form and thus we need mapping between systematic code word and non-systematic code word which introduces additional complexity and finding the mapping relationship is not clear in this case. Furthermore, the first two bits of the RM(2,5) code has been removed to be 30 bits and thus the orthogonal property of the Walsh code is not satisfied.

We can consider the Wolf's MLD using a trellis to get optimum decoded word. This method requires2^{16} states to use Viterbi algorithm to decode (30, 14) RM code, which is more complex than a correlation decoder requiring2^{14}operations.

Now consider the proposed algorithm to decode (30, 14) RM code. We set $k_1 = k_2 = 7$ and divide the generator matrix $\boldsymbol{G}$ matrix into two sub-matrices $\boldsymbol{G}_1$ and $\boldsymbol{G}_2$. And construct a memory bank of $2^{k_1} = 2^7$ n-tuples $\boldsymbol{B}$ for the parallel processing which reduces the decoding time by 2^7 times. The memory bank $\boldsymbol{B}$ needs a memory of$n \times 2^{k_1}$ bits which is equal to 480 bytes. This is very affordable size to implement. Since one parallel operation time is equal to one correlation time, the total time to decode an optimum code word is equal to the processing time of $2^{k_2} = 128$ correlations which is negligible compared to the speed of processor in modern communication equipment. Thus we can easily implement optimum decoder for (30, 14) RM code using hybrid MLD. Figure 3 shows the performance of (30, 14) RM code over AGWN channel where we see about 4 dB performance gain.

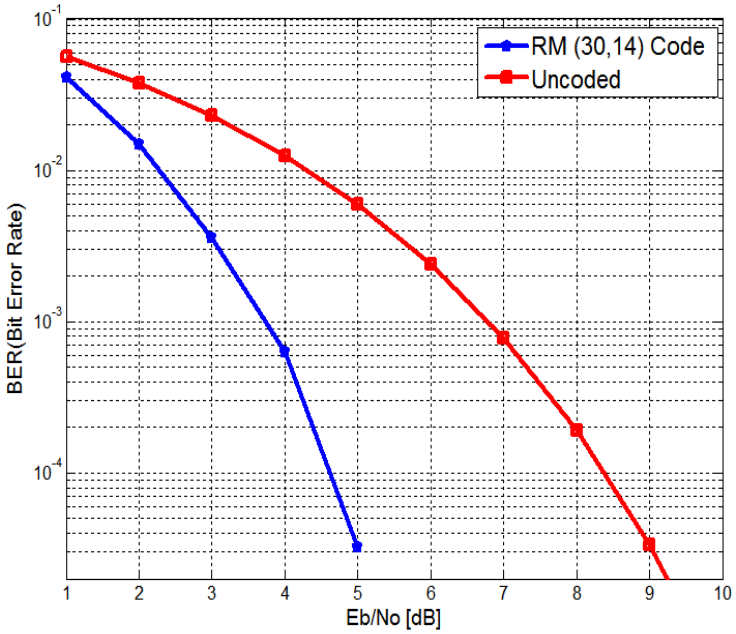

Figure 3. Performance of (30, 14) RM Code over AWGN Channel

4. Conclusion

In this paper we have proposed a new maximum likelihood decoding algorithm to get optimum decoded word for a linear block code. Following 5 steps of the algorithm we can easily implement the decoder. The hybrid maximum likelihood decoding could solve the problem of the hardware complexity as well as the computational time. Wolf's method is only effective for a high-rate code. In fact there are many popular linear block codes which are not high-rate codes. To show the effectiveness of the proposed method, we demonstrated the decoding of (30, 14) RM code over AWGN channel which shows about 4dB performance gain with affordable hardware complexity.

Acknowledgements

This paper was supported by Research Fund, Kumoh National Institute of Technology.

References

[1] J. G. Proakis, "Digital Communications", McGraw-Hill, New York (**2007**).
[2] B. Sklar, "Digital Communications", Prentice Hall, New Jersey (**2001**).
[3] H. Jang, S. Lee and S. Park, "On Using Redundant Parity Check Equation for LDPCA decoding in Distributed Video Coding", IJAST, vol. 42, (**2012**) May, pp. 11-18.
[4] T. Park, M. Kim and J. Jung, "A New LLR Based MPE-FEC Decoding Algorithm", IJMUE vol. 8, no. 4, (**2013**), pp. 137-146.
[5] H. Park and D. Ko, "Performance Enhancement of Wireless Datalink Modem Using Channel Coding", IJMUE, vol. 6, no. 4, (**2011**) October , pp. 53-60.
[6] S. B. Wicker, "Error Control Systems for Digital Communication and Storage", Prentice Hall (**1995**).
[7] S. Lin and D. J. Costello, "Error Control Coding", Prentice Hall (**2005**).
[8] R. H. Morelos-Zaragoza, "The art of Error Correcting Coding", John Wiley & Sons (**2007**).
[9] J. K. Wolf, "Efficient Maximum Likelihood Decoding of Linear Block Codes Using a Trellis", IEEE Trans. Inform. Theory, IT-24, no. 1, (**1978**) January, pp. 76-80.
[10] A. J. Viterbi, "Error Bounds for Convolutional Codes and an Asymptotically Optimum Decoding Algorithm", IEEE Trans. Inform. Theory, vol. IT-13, (**1967**) April, pp. 260-269.
[11] L. R. Bahl, J. Cocke, F. Jelinek, and J. Raviv, "Optimal Decoding of Linear Codes for Minimizing Symbol Error Rate", IEEE Trans. Inform. Theory, vol. IT-20, (**1974**) March, pp. 284-287.
[12] R. Pyndiah, "Near-Optimum Decoding of Product Codes: Block Turbo Codes", IEEE, Trans. Comm., vol. 46, no. 8, (**1988**) August, pp. 1003-1010.
[13] D. Chase, A Class of Algorithm for Decoding Block Codes With Channel Measurement Information, IEEE Trans. Inform. Theory, IT-18, no. 1, (**1972**) January, pp. 170-182.
[14] ETSI EN 300 392-2 V3.4.1, Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 2; Air Interface (AI) (**2010**).
[15] N. Ahmed and K. Rao, "Orthogonal Transforms for Digital Signal Processing", Spring-Verlog (**1975**).
[16] Y. Song, "Optimized Channel Coding of Control Channels for Mobile Packet Communication", Journal of the Korea Electromagnetic Engineering Society, vol. 3, no. 1, (**2003**) May, pp. 50-56.

Author

Young Joon Song, he received the B.S., M.S., and Ph.D. degrees in electronic communications engineering from the Hanyang University, Korea, in 1987, 1994, and 1999, respectively.

He was a principle research engineer with LG Electronics Inc. from 1994 to 2002. Since 2002, he has been with the Department of Electronic Engineering, Kumoh National Institute of Technology, Gumi, Korea, where he is currently a Professor. During 2006, he was at the University of Hawaii at Manoa, as a visiting scholar. His research interests are in channel coding, sequence design, and mobile/multimedia communication systems.

