한국통신학회 1984년도 추계학술발표회 논문집 (1984. 11. 3)

Reed-Muller 부호의 인코더 및 디코더 설계

84321

○
김 영 곤　　강 창 언
연 세 대 학 교 공 과 대 학 전 자 공 학 과

Design of an Encoder and Decoder Using Reed-Muller Code

Young Gon Kim　　Chang Eon Kang
Dept. of Electronic Engineering, Yonsei Univ.

* ABSTRACT *

The majority - logic decoding algorithm for Geometry code is more simply implemented than the known decoding aigorithm for BCH codes.
Thus, the moderate code word, Geometry codes provide rather effective error control.

The purpose of this paper is to inves - tigate the Reed - Muller code and to design the encoder and decoder circuit and to find the performance for (15, 11) Reed -Muller code.

Experimental results show that the system has not only single error - correcting ability but also good performance.

1. 서 론

송신된 code word가 채널을 경유하여 수신될때 랜덤에러에 의해 통신이 큰 장애를 받는다. 이러한 에러가 발생시에 해결방법으로 많은 디코딩 방법이 연구되어왔다. Majority-logic decoding은 다른 디코딩 알고리즘보다 실행이 간단하고 에러 control이 효율적이다. 이러한 디코딩은 1954년에 Reed에 의해 처음 개발되었고, 다수의 에러를 정정시키는 계층은 Muller에 의해 개발되었으며, 그후 Massey에 의해 체계화 되었다. 본 논문에서는 Majority-logic decodable code의 하나인(15,11) Reed-Muller code의 인코더 및 디코더를 설계하고, Weight 분포와 Performance를 알아본다.

2. 이론 해석

Euclidean 기하학 부호에서 매개변수중 s=1인 경우가 Generalized Reed-Muller 부호이다. 여기서 매개변수를 정의하면,

Code Word : $n=2^m-1$ (1)

정보 Word : $k=1+\binom{m}{1}+\cdots+\binom{m}{r}$ (2)

패리티체크 비트의수 : $n-k=1+\binom{m}{r}+\cdots+\binom{m}{m-r-1}$ (3)

최소 거리 : $d_{min}=2^{m-r}-1$ (4)

단 계 수 : $L=r+1$ (5)

정정능력 : $t=(d_{min}-1)/2$ (6)

패리티 체크합 : $J=d_{min}-1$ (7)

이 된다. Generalized Reed-Muller 부호의 성질은,

. rth-order GRM 부호는 design된 거리 d=(q-R)(m-Q-1)의 확장 BCH 부호의 subcode 이다. 여기서 Q와 R은 r를 q-1로 나누었을때의 몫과 나머지이다.

. rth-order GRM 부호 dual은[(q-1)m-r-1]st-order GRM 부호와 같다.

. Zero th-order GRM 부호는 반복 부호이다.

. [(q-1m-2] nd-order GRM 부호는 확장된 한개의 에러 정정 BCH 부호이다.

. GRM 부호는 cyclic 이다.

GF(gm)에 대해 code word $n=g^m-1$의 lengh를 가진 rth-order GRM 부호는 순환부호이므로,생성 다항식은

$$g(x)=\prod_{\substack{j \\ 0<\max w_g(j)\le(m-r-1)(q-1) \\ 0\le j\le q^m-1}}(x-\alpha^j) \quad (8)$$

이 되고, 여기서 w(j)는 정수 J의 q-ary 확장된 디지트의 합이고, α는 $GF(g^m)$에서 원시 원소이다.

K 디지트의 정보 block m(x)의 인코딩 방법은, v(x)=r(x)+x^{n-k} m(x)로 여기서 r(x)는 X^{n-k} m(x)를 생성다항식 g(x)에 의해서 나누어진 나머지 이므로, 이것은 생성다항식에 따른 궤환연결한 Shift Register로 구성되는 division 회로에 의해 수행된다. 신드롬 계산은 전송기에서 인코딩 회로와 같은 division회로에 의해 수행된다.

디코딩 방법은 생성 다항식에서 제너레이트 행렬과 패리티 체크행렬을 구성한후 에러패턴에 대응하는 신드롬을 eH^T 에 의해서 구한후, 이것에 의해 패리티 체크합을 구성하면 신드롬의 modulo-2 합이며, 결국 에러비트의 modulo-2 합이다. e_{n-1} 에 대해서 orthogonal인 패리티 체크합을 구성하면, 순환성부호의 성질에 의해서, 나머지 에러 디지트에 대해서 orthogonal인 패리티 체크합들은 에러의 백터를 순환시킬때 얻어진다. 일반적인 L-단계 방식 경우에는 에러디지트의 집합에 대하여 orthogonal인 J개의 패리티체크합을 만들게 되며, 여러단계의 majority gate 들을 거쳐 디코딩 한후에, 에러패턴은 올바르게 정정된다. 그림1은 L-단계 orthogonalizable 부호에 대한 일반적인 Type I 다수 논리 디코더이며,

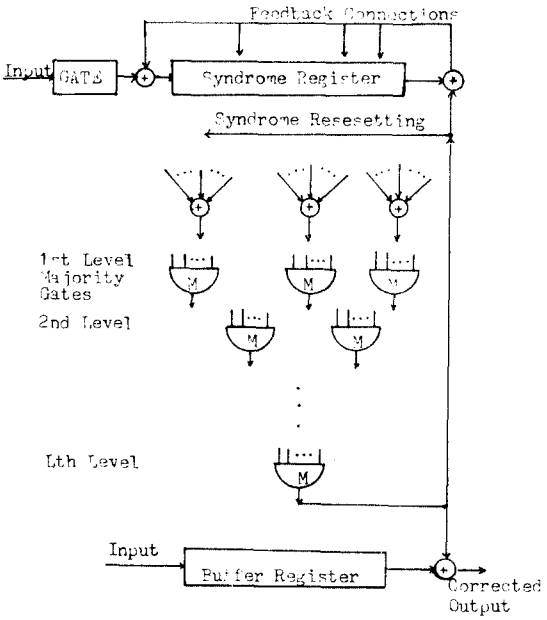

그림 1. L-단계형식 다수 논리 디코더

이 디코더의 에러 정정과정은 다음과 같다. 수신된 Word가 버퍼 레지스터와 신드롬 레지스터에 들어오면, 신드롬이 계산되고, 체크합의 set가 첫 단계 다수 gate에 각 J 입력을 가진$(J)^{L-1}$ 이 입력되고, 첫 gate의 출력이 두번째 gate의$(J)^{L-2}$ 가 입력된다. 이와 같이 계속하여 마지막 단계에서 gate가 하나가 될 때까지 수행한다. 이러한 gate에 대해 J 입력은 첫 에러 디지트 e_{n-1} 에 대해 패리티 체크합이 orthogonal 된다. Majority gate는 J개의 입력과 하나의 출력을 가지며, 입력의 과반수이상이 '1'이면, 출력은 '1'이고, 그렇지 않으면 '0'이 된다. 첫 수신된 디지트가 버퍼로부터 읽혀지고, 마지막 gate 의 출력과 EXOR에 의한 에러정정이 수행된다. 신드롬과 버퍼 레지스터가 동시에 한면씩 Shift되어 마지막까지 위와같이 한 디지트씩 수행하면, 또는 그보다 작은 에러를 정정할 수 있다.

3. (15,11) RM 부호의 인코더및 디코더 설계

m=4인 RM 부호는 식(2)-(7)에 의해 r=2, dmin=3, J=2, L=3이 된다. α 를 GF(2^4)의 원시원소와 하고, j를 15이하의 음아닌 정수라 하면, $0 < \max W_2(j) \leq 1$을 만족하는 정수는 1,2,4,8 이므로, 식(8)에 의해 생성 다항식은,

$g(x)=(x+\alpha)(x+\alpha^2)(x+\alpha^4)(x+\alpha^8) = 1+x+x^4$

이 된다. 위의 생성 다항시게 의해 (n-k) stage Shift Register 인코더 회로는 그림 2와 같다.

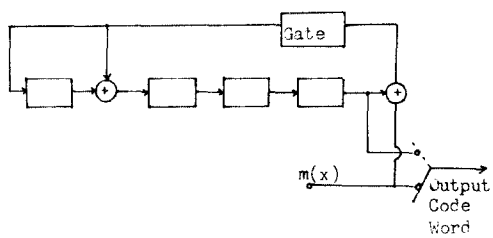

그림 2. (15,11) 다수식 인코더

정보디지트 11개가 Channel로 들어가고, 동시에 레지스터에 들어가서11번 Shift 후 gate가 개방되어 레지스터의 내용 4개가 Channel 속으로 들어가면 완전한 코드 word가 된다.

즉, $V(x)=r(x)+x^4$ m(x)가 된다. 디코더 설계방법은 먼저 X^{4+i}, i=0,1,2,..,10을 생성 다항식 $g(x)=1+x+x^4$으로 나누어 얻은 나머지의 계수를 오름차순으로 정리하여 G=[P,Ik]를 구성하고, G로 부터 패리티 체크 행렬 H=[In-k, P^T]를 구한다. 여기서 Ik는 KxK identity 행렬이고, In-k는 (n-k)x(n-k) identity 행렬이다.

제너레이터 행렬 G와 패리티 행렬 H는 다음과 같다.

$$G=\begin{bmatrix}
1&1&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&1&1&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&1&1&0&0&1&0&0&0&0&0&0&0&0\\
1&1&0&1&0&0&0&1&0&0&0&0&0&0&0\\
1&0&1&0&0&0&0&0&1&0&0&0&0&0&0\\
0&1&0&1&0&0&0&0&0&1&0&0&0&0&0\\
1&1&1&0&0&0&0&0&0&0&1&0&0&0&0\\
0&1&1&1&0&0&0&0&0&0&0&1&0&0&0\\
1&1&1&1&0&0&0&0&0&0&0&0&1&0&0\\
1&0&1&1&0&0&0&0&0&0&0&0&0&1&0\\
1&0&0&1&0&0&0&0&0&0&0&0&0&0&1
\end{bmatrix}$$

$$H=\begin{bmatrix}
1&0&0&0&1&0&0&1&1&0&1&0&1&1&1\\
0&1&0&0&1&1&0&1&0&1&1&1&1&0&0\\
0&0&1&0&0&1&1&0&1&0&1&1&1&1&0\\
0&0&0&1&0&0&1&1&0&1&0&1&1&1&1
\end{bmatrix}$$

에러벡터를 e=(e0, e1, e2, ... e14)라 하면, e에 대응하는 신드롬은,

$S=eH^T=(S_0, S_1, S_2, \ldots, S_{14})$

이므로, $S_0 = e_0 + e_4 + e_7 + e_8 + e_{10} + e_{12} + e_{13} + e_{14}$

$S_1 = e_1 + e_4 + e_5 + e_7 + e_9 + e_{10} + e_{11} + e_{12}$ (9)

$S_2 = e_2 + e_5 + e_6 + e_8 + e_{10} + e_{11} + e_{12} + e_{13}$

$S_3 = e_3 + e_6 + e_7 + e_9 + e_{11} + e_{12} + e_{13} + e_{14}$

식(9)의 신드롬으로 부터 e_{14}에 대하여 3단계 orthogonal하게 할려면, 1단계의 입력은 총 8개되고 각 gate의 입력은 J=dmin-1=2가 되고, 패리티 체크합의 set는 다음과 같다.

.E1= e_6, e_{11}, e_7, e_{14}

$A_{11}=S_3 = e_3 + e_6 + e_7 + e_9 + e_{11} + e_{12} + e_{13} + e_{14}$

$A_{12}=S_0 \oplus S_2 = e_0 + e_2 + e_4 + e_5 + e_6 + e_7 + e_{11} + e_{14}$

.E2= e_8, e_{10}, e_7, e_{14}

$A_{21}= S_0 = e_0 + e_4 + e_7 + e_8 + e_{10} + e_{12} + e_{13} + e_{14}$

$A_{22}= S_2 \oplus S_3 = e_2 + e_3 + e_5 + e_7 + e_8 + e_9 + e_{10} + e_{14}$

.E3= $e_4, e_{10}, e_{13}, e_{14}$

$A_{31}= S_0 = e_0 + e_4 + e_7 + e_8 + e_{10} + e_{12} + e_{13} + e_{14}$

$A_{32}= S_1 \oplus S_3 = e_1 + e_3 + e_4 + e_5 + e_6 + e_{10} + e_{13} + e_{14}$

.E4= $e_9, e_{11}, e_{13}, e_{14}$

$A_{41}=S_3 = e_3 + e_6 + e_7 + e_9 + e_{11} + e_{12} + e_{13} + e_{14}$

$A_{42}=S_0 \oplus S_1 = e_0 + e_1 + e_5 + e_8 + e_9 + e_{11} + e_{13} + e_{14}$

이 코드의 3단계 다수논리 디코더는 그림 3과 같다.

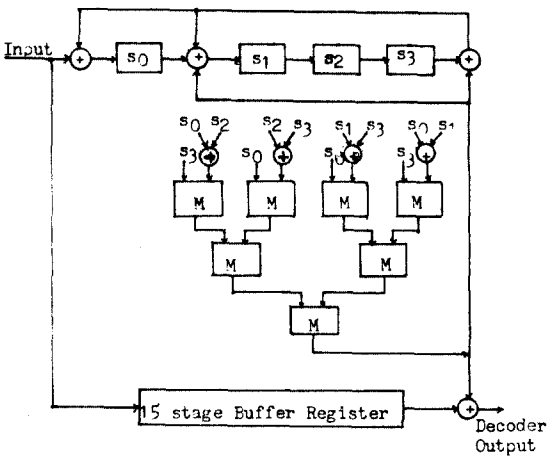

그림 3. (15,11)코드에 대한 3단계형의 다수 논리 디코더

4. 실험 및 결과 고찰

본 연구에서 RM 부호의 인코더 및 디코더를 구성하여 실험하기 위한 구성도는 그림4와 같다.

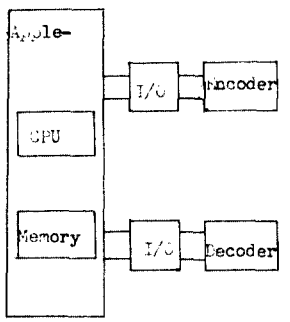

그림 4. 시스템 구성도

Weight	# of Weight
0	1
1	0
2	0
3	35
4	105
5	168
6	280
7	435
8	435
9	280
10	168
11	105
12	35
13	0
14	0
15	1

표 1. Weight 분포

위의 표에서 Dmin이 3임과 weight 분포가 대칭임을 알수 있다.

Performance는 Channel을 BSC이라 하고, 각 비트의 에러는 서로 독립으로 발생된다고 하면, (15, 11) RM 부호는 dmin=3 이고 t=1 이므로 Perfect 부호가 되므로 디코딩 못할 확률은,

$$P_M = \sum_{m=2}^{15} \binom{15}{m} P^m (1-P)^{15-m} \qquad (10)$$

이 되고, RM 부호의 m=4인 것은 (15,5) RM 부호도 성립되므로, (15,5)RM 부호는 dmin=7 이고 t=3이 이므로 Perfect 부호가 되므로 디코딩못할 확률은,

$$P_M = \sum_{m=4}^{15} \binom{15}{m} P^m (1-P)^{15-m} \qquad (11)$$

이 된다. 위의 식(10),(11)을 표(2)에 나타내었다.

DATA	PM-11	PM-5
0.1	0.459957	0.655555
0.05	0.170953	5.467266E-03
0.01	9.629783-03	1.2[illegible]E-05
5E-03	2.513779E-03	8.16365-07
1E-03	1.0[illegible]E-04	1.353[illegible]E-09
9E-04	6.673577E-05	5.55183E-10
5E-04	2.613653E-05	8.[illegible]E-11
1E-05	1.0[illegible]E-08	1.3[illegible]E-17
3E-06	9.449777E-10	1.105623E-19
3E-07	9.449999E-12	1.1[illegible]E-23

표2. m=4인 RM Code의 Performance

5. 결 론

본 논문은 RM 부호의 인코더 및 디코더의 설계에 관해서 연구했다. 이러한 디코더는 코드 word 가 비교적 짧은 경우에 다른 디코더에 비해서 간단하고 cost가 적게드는 장점을 지녔고, 효율적인 에러 control 이 되므로, 에러 control technique에 널리 이용된다. 또 코드 Word를 좀더 크게하면 위성통신에도 이용할 수 있다.

* 참 고 문 헌 *

1. Shu Lin, "An Introduction to Error-Correcting Codes", Prentice-Hall, 1970.
2. Peterson and Weldon, "Error-Correcting Codes", 2nd Edition, The MIT Press, 1972.
3. R.E.Blahut, "Theory and Practice or Error Control Codes", 1983.
4. Djimitri Wiggert, "Error-Control Coding and Applications", 1978.
5. Reed,I.S, "A Class of Multiple Error-Correcting Codes and the Decoding Scheme",I.R.E. Trans. Inform. Theory, PGIT-4, PP.38-49, 1954.
6. Muller, D.E, "Application of Boolean Algebra to Switching Circuit Design and to Error Detection", I.R.E.Trans. Electron Computer, EG-3, PP. 6-12, 1954.
7. Tadao Kasami and Shulin and W.Wesley Peterson, "New Generalization of the Read Muller Codes", IEEE Trans. on Information Theory, Vol. IT-14, PP.189-198, 1968.
8. Chin-Long Chen, "Note on Majority-Logic Decoding of Finite Geometry Codes" IEEE Trans. on Information Theory, Vol.IT-18, PP.539-541.