한국통신학회 1984년도 춘계학술발표회 논문집 (1984. 5. 25)

순환성 코드를 사용한 Majority logic 디코딩

84306

강 창 언 정 연 호
연 세 대 학 교 공 과 대 학 전 자 공 학 과

The majority-logic decoding for cyclic codes.

Chang-Eon Kang Yon - Ho Jeong
Dept. of Electronic Engineering, Yonsei Univ.

* Abstact *

In this paper, the (15,7) cyclic codes used EG(2,2) were decoded by one step majority logic decoding. This decoding algorithm is based on the properties of finite geometries and can be simply implemented for moderate length n. Especially one step majority logic decoding is attractive because the complexity and the cost of the majority logic decoder increase very rapidly with L, the number of decoding steps. The theorectical and experimental results show that the majority logic decoding presented in this paper is a relatively effective decoding scheme.

1. 서 론

송신된 Code Word가 채널을 경유한 후 수신될 때 radom error에 의해 변화되어 통신의 장애가 되고 있다. 이 때 디코딩을 통하여 본래의 Code Word를 재생하는 여러가지 방법들이 연구되어 왔다. 본 논문에서는 코드 길이가 적당한 경우에 다른 디코딩 알고리즘에 비해서 실행이 간단하고 정정 능력의 저하가 적은 majority logic decoding이 연구된다. 이 디코딩은 1954년에 Reed에 의해 처음 개발되었으며, 그 후 다수의 에러를 정정 시키는 계층은 Muller에 의해 개발되었다. 통일된 공식화는 Massey에 의해 완성되었다. 이 디코딩은 finite geometries(EG 와 PG)의 성질에 의존하며, 대부분의 Majority logic decodable code는 순환성 코드이다.

2. Majority logic decodable codes.

Hamming Codes, difference-set Codes, maximum length codes, EG Codes, PG Codes, Reed Muller Codes, BCH Codes 등은 Majority logic 디코딩이 가능하며 one -step 방식 또는 L-step의 방식으로 구분하여 취급한다. One - step과 L-step의 특징을 비교하면 다음과 같다.

A. one-step 방식

하나의 error digit에 대하여 orthogonal이다.
패리티 체크 합의 수 J가 최소 거리 d에 가까운 값일 때 이 방식은 효과적이므로 이에 해당되는 코드의 수는 적다.
필요한 majority gate의 수는 1개이다.

B. L-step 방식

여러개의 error digit의 집합 E 에 대하여 orthogonal 인 패리티 체크 합을 만드는 것부터 시작하고 여러 step으로 계속된다.
이에 해당되는 코드의 수는 많다.
필요한 majority gate의 수는 다수이다.

3. 디코딩의 원리

디코더를 구성하려면 필요한 요소들을 다음의 순서에 따라 고려해야 한다.

1. 전체 시스템에 적합한 코드 유형의 선택
2. 선택된 코드의 바탕이 되는 제너레이터 행렬, 패리티 체크 행렬의 구성
3. 에러 패턴에 대응하는 신드럼을 eH^t에 의해 계산
4. 패리티 체크 합의 구성, 이것은 신드럼의 modulo-2 합이며 동가적으로 에러 비트의 modulo -2 합이다.

e_{n-1}에 대해서 orthogonal인 패리티 체크합을 구성하면, 순환성 코드(cyclic code)의 성질에 의해서, 나머지 에러 디지트에 대해서 orthogonal인 패리티 체크 합들은 에러의 벡터를 순환시킬 때 얻어진다. 이 때 (J/2) 이하의 갯수의 에러들이 발생한 경우에 에러의 패턴은 올바르게 정정될 수 있다. 일반적인 L-step방식 경우에는 에러 디지트의 집합에 대하여 orthogonal인 J개의 패리티 체크 합을 만들게

되며, 여러 step 의 majority gate들을 거쳐 디코딩 한 후에,에러 패턴은 올바르게 정정 될 수 있다.

majority-logic decodable codes의 큰 갈래는 finite geometry에 바탕을 둔 EG Codes와 PG Codes이며 이에 해당되는 디코딩 원리는 다음과 같다. EG Codes에서, 코드 길이 p^{sm}이고 order r에 대하여 $(d_{ML}-1)/2$ 이하 갯수의 에러가 발생하였다면, (r+1) - step으로 디코딩 된다. PG Codes에서, 코드 길이 $p^{s(m+1)}/(p^s-1)$이고 order r에 대하여 $(d_{ML}-1)/2$ 이하 갯수의 에러가 발생하였다면 r-step으로 디코딩된다.

그림 1.은 디코더의 한 가지 유형이며, 이 디코더의 에러 정정 과정은 다음과 같다.

수신된 word가 버퍼 레지스터와 신드럼 레지스터에 들어온다. 신드럼이 계산되고, 신드럼으로 부터 e_{n-1}에 대하여 orthogonal인 J개의 패리티 체크합이 만들어지고 이들 패리티 체크 합들은 J-input majority gate의 입력이 된다. majority gate는 J개의 입력과 하나의 출력을 가지며, 입력의 과반수가 1일때 출력은 1, 그렇지 않을 때 출력은 0이다. 출력이 1이면 수신된 word의 처음 수신된 비트가 에러임을 의미하며, 출력이 0이면 처음 수신된 비트는 올바른 값임을 의미한다. 버퍼 레지스터로 부터 나오는 처음 수신된 비트는 majority gate의 출력과 함께 EOR 에 더해져서 정정이 수행된다.

4. 디코더의 설계

표 1. EG codes 와 PG Codes의 파라미터

Table 1. Parameters of EG Codes and PG Codes

n	k	dML	GEometry	order r
7	4	3	EG (3,2)	1
	1	7	EG (3,2)	0
15	11	3	EG (4,2)	2
	7	5	EG (2,2)	0
	5	7	EG (4,2)	1
7	3	4	PG (2,2)	1
15	10	4	PG (3,2)	2
	4	8	PG (3,2)	1

표 1은 몇 가지의 finlte geometry Codes(EG와 PG)의 파라미터를 보여준다. 본 논문에서는 (15,7) EG(2,2) Code를 선택하여 디코더의 설계를 하겠다.

제너레이터 행렬 G와 패리티 행렬 H를 구성하는 방법은 다음과 같다. 제너레이터 다항식 $g(x)=x^8+x^7+x^6+x^4+1$ 에 의해 x^{n-k+i}, i=0,1....(k-1)을 나누어 얻은 나머지의 계수를 오름 차순으로 정리하여 G를 구성하고 $G=(P,I_k)$로 부터 행렬 $H=(I_{n-k}, P^T)$를 얻는다. 여기서 I_k는 kxk identity 행렬이고 I_{n-r}는 (n-k)x(n-k) identity 행렬이다. 행렬 G와 행렬 H는 다음과 같다.

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

$$H=\begin{bmatrix} 1&0&0&0&0&0&0&0&1&1&0&1&0&0&0\\ 0&1&0&0&0&0&0&0&0&1&1&0&1&0&0\\ 0&0&1&0&0&0&0&0&0&0&1&1&0&1&0\\ 0&0&0&1&0&0&0&0&0&0&0&1&1&0&1\\ 0&0&0&0&1&0&0&0&1&1&1&0&1&1&0\\ 0&0&0&0&0&1&0&0&0&1&1&1&0&1&1\\ 0&0&0&0&0&0&1&0&1&1&1&0&0&1&1\\ 0&0&0&0&0&0&0&1&1&1&0&1&0&0&0&1 \end{bmatrix} \quad (2)$$

에러 벡터는 $e=(e_0, e_1, e_2, e_3, e_4, \ , e_5, e_6, e_7, e_8, e_9, e_{10}, e_{11}, e_{12}, e_{13}, e_{14})$ (3)

이라고 하자. e에 대응하는 신드럼은

$$S=(S_0,S_1,S_2,S_3,S_4,S_5,S_6,S_7)=eH^T \quad (4)$$

그러면

$$S_0=e_0+e_8+e_9+e_{11}$$

$$S_1=e_1+e_9+e_{10}+e_{12}\ ,\ S_2=e_2+e_{10}+e_{11}+e_{13}$$

$$S_3=e_3+e_{11}+e_{12}+e_{14} \quad (5)$$

$$S_4=e_4+e_8+e_9+e_{11}+e_{12}+e_{13}$$

$$S_5=e_5+e_9+e_{10}+e_{12}+e_{13}+e_{14},\ S_6=e_6+e_8+e_9+e_{10}+e_{13}+e_{14}$$

$$S_7=e_7+e_8+e_{10}+e_{14}$$

식 (5)의 신드럼으로 부터 e_{14}에 대하여 orthogonal인 패리티 체크 합은 $J=d_{ML}-1=4$개 이며 다음과 같다.

$$A_1=S_3=e_3+e_{11}+e_{12}+e_{14}$$

$$A_2=S_7=e_7+e_8+e_{10}+e_{14}$$

$$A_3=S_1+S_5=e_1+e_5+e_{13}+e_{14}$$

$$A_4=S_0+S_2+S_6=e_0+e_2+e_6+e_{14} \quad (6)$$

다른 에러 e_{n-i} 에 대해서 orthogonal인 패리티 체크는 마찬가지로 구할 수 있다. J-input majority gate는 4개의 패리티 체크 합을 입력으로 하여 하나의 출력을 내놓는다. 이 때 입력의 과반수인 3개이상이 1 일때 출력은 1 이고, 그렇지 못하면 출력은 0이다. 출력의 1은 대응되는 수신된 비트가 에러임을 지시하며, 버퍼 레지스터로 부터 나오는 비트를 정정한다.

4-input majority gate 는 출력의 논리식이

$$f = A_1A_2A_4 + A_1A_2A_3 + A_1A_3A_4 + A_2A_3A_4 \quad (7)$$

이며 AND 게이트와 OR 게이트에 의해 구성된다.

이 코드의 one-step majority-logic 디코더는 그림 2.

에서 보여준다.

5. 실험 및 결과 고찰

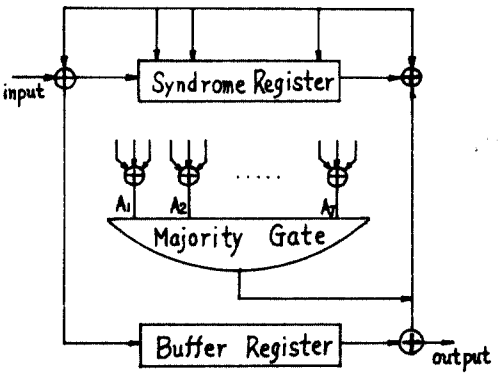
(15,7) code word에, 두 자리의 에러를 가지는 에러 벡터를 더하여 변질된 word를 만들고, 이를 디코더의 입력에 넣어 디코딩 과정을 통해서 본래의 code word를 얻었다. 전체 디코딩은 BCH 의 디코딩에 비해서 비교적 쉽게 실행되는 장점을 가지는 반면에, 정정 능력은 약간 못하다. 코드 길이가 길수록 정정 능력은 더욱 못하며, 디코더는 더욱 복잡하므로 코드 길이가 적당한 경우에 이 디코딩은 적합하다. one step 방식에 의해서 실행 될 수 없는 코드 중에서 많은 것이 일반화된 L-step 방식에 의해 가능하다. 한편 majority-logic decoder의 복잡성, 이와 관련된 cost는 step의 수 L과 더불어 지수적으로 증가하므로, one - step 디코딩이 더욱 주목을 끈다. L >1일 경우에도 에러의 정정 능력의 일부를 희생시키면서 여전히 one - step 디코딩이 가능하며 때때로 에러의 정정 능력은 적게 감소되면서 디코더의 복잡성은 사실상 감소되어 보상된다. 또 EG 코드와 Reed-Muller 코드에 관하여, L-step 방식이면서 step의 수를 줄일 수 있는 향상된 알고리즘도 제시되고 있다.

6. 결 론

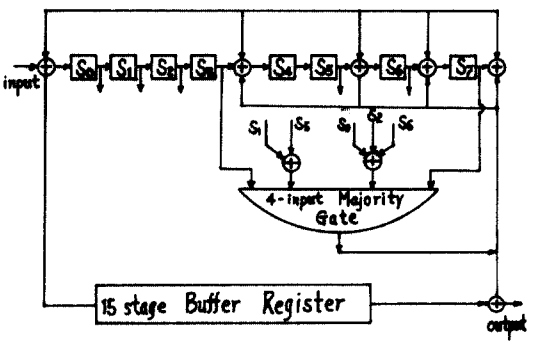
본 논문에서는 majority logic decoding 에 관해서 연구했다. 이 디코딩은 코드의 길이가 비교적 짧은 경우에 다른 디코딩에 비해서 간단하고 cost가 적게 드는 장점을 지닌다. 이 디코딩 중에서 one - step 디코딩이 주목을 끈다. one - step에 의해서 실행될 수 없는 경우에는, 정정 능력의 저하가 작으면서 step의 수를 줄일 수 있는가를 검토해야 한다.

* 참 고 문 헌 *

1. Shu Lin, "An Introduction to Error-Correcting Codes", Prentice-Hall, 1970.
2. Lucky, Salz and Weldon, "Principles of Data Communication ", Mc-Graw Hill, 1968.
3. Peterson and Weldon, "Error - Correcting Codes ", 2nd Editon, The MIT Press, 1972.
4. L.D. Rudolph, " A Class of Majority Logic Decodable Codes", IEEE Trans. on Information Theory Vol. 13 pp. 305-307 APRIL 1967.
5. Kasami, T., S,Lin and W.W. Peterson "New Gererations of the Reed-Muller Codes-Part I IEEE Trans. on Information Theory IT-14 March 1968.
6. E.J. Weldon, J.R. " New Generalizations of the Reed-Muller Codes - Par II. IEEE Trans. on Information Theory Vol. IT-14 pp. 199 - 205 March 1968.



그 림 1. 1 단계의 다수논리 디코더
one-step majority-logic decoder



그 림 2. (15,7) 코드에 대한 1단계의 다수 논리 디코더
- one-step majority-logic decoder for the (15,7) code -