

2진 BCH 부호의 새로운 연판정 복호법

A New Soft-Decision Decoding of Binary BCH Codes

심 용 결*

(Yong Geol Shim*)

*이 연구는 단국대학교 대학연구비의 지원으로 연구되었음.

요 약

2진 BCH 부호에 대한 새로운 연판정 복호법을 제안하였다. 후보부호어가 선출되지 않을 때의 성능 저하를 방지할 수 있는 개선된 알고리즘을 개발하여 오정정 확률과 정정 불능 확률이 낮아지게 하였다. 또한, 복잡도를 줄이는 방안도 개발하여 알고리즘 개선으로 인한 복잡도 증가가 거의 나타나지 않도록 하였다. (31,16) BCH 부호에 대한 시뮬레이션 결과로 이러한 사실들을 확인할 수 있었다.

ABSTRACT

A new soft decision decoding algorithm for binary BCH codes is proposed. The improved algorithm is developed to solve the performance degradation problem of missing candidate codewords. The incorrect decoding probability and the error detection probability can be decreased. Also, the method for reducing complexity is developed. This method removes the practical complexity increase caused by the improved algorithm. These facts are confirmed by the simulation results for (31,16) BCH code.

I. 서 론

오류 정정 부호는 잡음이 존재하는 디지털 통신 시스템의 채널에서 통신의 신뢰도를 유지하기 위한 목적으로 사용되고 있다. 이 때 수신 신호의 정확성에 대한 정보를 이용하는 연판정 복호법을 사용하면 통신 시스템의 성능을 크게 향상시킬 수 있다.[1-5] 그런데 연판정 복호법은 오류 정정 성능이 우수할수록 복호기의 복잡도가 증가한다. 따라서 복호의 복잡도를 줄이면서도 우수한 오류 정정 성능을 발휘하는 복호 방법을 개발하는 것이 필요하다. 오류 정정 부호 중 컨벌루션 부호는 실용적인 연판정 복호법들이 많이 개발되어 있다. 이러한 이유로 현재는 컨벌루션 부호가 통신 시스템에 널리 사용되고 있다. 그러나 블록 부호에 대한 효율적인 연판정 복호법은 아직도 완전히 확립되지 않았으며 이를 해결하기 위한 연구들이 진행 중이다. 현재까지 알려진 블록 부호의 연판정 복호법들은 수신된 신호를 중심으로 몇 가지의 후보부호어들을 얻어내는 방법을 사용하고 있다.[1,3-5]

2진 BCH 부호는 블록 부호 중 성능이 우수하고 경판정 복호법이 잘 확립되어 있는 대표적인 부호이다. 그런데 2진 BCH 부호는 경판정 복호 과정에서 정정 불능의

오류 패턴이 검출되어 후보부호어를 찾을 수 없는 경우가 많다. 따라서 2진 BCH 부호에 현재까지 알려진 연판정 복호법들을 적용하면 성능이 저하되는 것을 피할 수 없다. 본 논문에서는 이렇게 정정 불능의 오류 패턴이 검출되는 경우에도 새로운 후보부호어를 찾아낼 수 있는 연판정 복호법을 제안한다. 이 복호법은 참고문헌 [5]에 제시된 방법을 개선한 것이다. 수신 신호 중 연판정 신뢰도가 낮은 위치들을 선택하고 이들의 경판정 값을 여러 가지 조합을 취하여 반전시켜서 후보부호어를 찾을 수 있도록 한다. 이 때 복잡도가 늘어나는 것을 방지하기 위하여 두 가지 방안을 도입한다. 첫 번째 방안은 한 후보부호어가 최우복호 결과인지의 여부를 판정하여 복호의 과정을 축소하는 것이다. 두 번째 방안은 수신 신호들의 일부 비트를 반전시켜 얻어진 벡터들 중 새로운 후보부호어를 얻을 가능성이 있을 조건을 도출하고, 이 조건을 만족하는 경우에만 경판정 복호를 수행하는 것이다. 이러한 방법으로 복호의 복잡도가 증가하지 않으면서 후보부호어들을 찾아내어 성능을 높이고자 한다.

II. 연판정 복호법

(n, k) BCH 부호 C 는 2원 선형 블록 부호이며, 최소 해밍거리 d 이다. C 의 부호어를 $c = (c_1, c_2, \dots, c_n)$

* 단국대학교 전자공학과

접수일자 : 1998년 8월 4일

으로 표시하며, $c_i \in \{0, 1\}$ 이다. 각각의 비트를 BPSK로 변조하여 전송하며 정보 비트 당 에너지는 E_b 이다. 채널에서 양측 전력 스펙트럼 밀도가 $N_0/2$ 인 가산성 백색 가우시안 잡음이 부가되고 복조기에서는 $\mathbf{r} = (r_1, r_2, \dots, r_n)$ 이 출력된다. 이 \mathbf{r} 로부터 경관정 $\mathbf{y} = (y_1, y_2, \dots, y_n)$ 과 신뢰도 벡터 $\mathbf{b} = (b_1, b_2, \dots, b_n)$ 이 얻어진다. 여기서 $r_i \geq 0$ 이면 $y_i = 0$ 이고 $r_i < 0$ 이면 $y_i = 1$ 이며, $b_i = |r_i|$ 이다. 연관정복호기는 \mathbf{y} 와 \mathbf{b} 를 이용하여 전송된 부호어를 추정한다. 추정된 부호어를 $\hat{\mathbf{c}}$ 로 표시한다. 한 부호어 \mathbf{c} 에 대한 에리페턴은 $\mathbf{e} = \mathbf{y} \oplus \mathbf{c}$ 로 주어진다. 여기서 \oplus 는 2진 덧셈을 나타낸다. 복호의 목표는 에리페턴 $\mathbf{e} = (e_1, e_2, \dots, e_n)$ 의 이진로그 무게 $W_0(\mathbf{e})$ 를 최소로 하는 부호어를 찾는 것이며, 이를 위하여 후보부호어들을 찾는다.[5]

본 논문에서는 정정 불능의 오류 패턴이 검출되는 경우에도 새로운 후보부호어를 찾아낼 수 있게 하기 위하여 \mathbf{y} 의 비트들 중에서 신뢰도가 가장 낮은 $\lfloor d/2 \rfloor$ 개의 위치를 선택한다. ($\lfloor x \rfloor$ 는 x 의 정수 부분을 표시한다.) 선택된 위치들에 대해서 가능한 모든 조합을 취하여 그 위치를 반전시킨 n 차원 벡터들을 구하고 각각의 n 차원 벡터를 경관정 복호하여 후보부호어들과 그에 대한 에리페턴들을 얻는다. 후보부호어들 중 에리페턴의 이진로그 무게가 가장 작은 것을 \mathbf{c}_1 으로 선택한다. 이때 복호의 복잡도를 줄이기 위하여 두 가지 방안을 도입한다. 첫 번째 방안은 한 후보부호어가 최우복호 결과와 일치하면 복호를 종료하는 것이다. 후보부호어가 최우복호 결과와 일치하는가를 판단하려면 다음 조건 중 하나를 만족해야 한다. 먼저 에리페턴이 $\mathbf{e} = \mathbf{0}$ 이면 된다. 그렇지 않은 경우에는 $W_H(\mathbf{e}) < d$ 이면서 $W_0(\mathbf{e}) \leq W_0(\mathbf{e} \oplus \mathbf{u}_j^*(\mathbf{e}))$ 이어야 한다. 이때 벡터 $\mathbf{u}_j^*(\mathbf{e})$ 의 해밍 무게는 j 이고 $\mathbf{u}_j^*(\mathbf{e})$ 의 원소가 1이 되는 곳은 $e_i = 1$ 인 $W_H(\mathbf{e})$ 개의 위치와 $e_i = 0$ 이면서 신뢰도가 가장 작은 $[j - W_H(\mathbf{e})]$ 개의 위치이다. $\mathbf{u}_j^*(\mathbf{e})$ 는 $j = d$ 로 한 것이다.

두 번째 방안으로는 \mathbf{y} 의 일부 비트를 반전시켜서 얻어진 n 차원 벡터들을 모두 경관정 복호할 것이 아니라, 새로운 후보부호어를 얻을 수 있을 가능성이 있는 경우에만 그 n 차원 벡터를 경관정 복호한다. 즉, 경관정 복호를 하기 전에 먼저 n 차원 벡터와 이미 얻어진 후보부호어들 사이의 해밍 거리를 계산한다. 만약 한 후보부호어와의 해밍거리가 $\lfloor (d-1)/2 \rfloor$ 이하로 된다면 경관정 복호 결과는 동일한 후보부호어가 될 것이다. 결국 이미 얻어진 모든 후보부호어들과의 해밍거리가 $\lfloor (d-1)/2 \rfloor$ 보다 큰 n 차원 벡터들만을 경관정 복호하는 것으로 충분하다.

본 논문에서 제안하는 연관정 복호 알고리즘은 다음과 같다. 단, 알고리즘을 시작하기 전에 에리페턴 \mathbf{e}_j 찾기를 제한하는 집합 $T = (t_1, t_2, \dots, t_{|T|})$ 와 파생된 에리페턴

\mathbf{e}_j' 찾기를 제한하는 집합 $S = (s_1, s_2, \dots, s_{|S|})$ 를 결정해야 한다. 이때 S 는 T 의 부분집합이다.

- 1) \mathbf{y} 의 비트들 중에서 신뢰도가 가장 낮은 $\lfloor d/2 \rfloor$ 개의 위치에 대해서 가능한 모든 조합을 취하여 그 위치를 반전시킨 n 차원 벡터들을 경관정 복호하여 \mathbf{c} 와 \mathbf{e} 들을 구한다. 만약 $\mathbf{e} = \mathbf{0}$ 인 경우 또는 만약 $W_H(\mathbf{e}) < d$ 이면서 $W_0(\mathbf{e}) \leq W_0(\mathbf{e} \oplus \mathbf{u}_j^*(\mathbf{e}))$ 인 경우이면 $\hat{\mathbf{c}} = \mathbf{c}$ 로 하고 종료한다. 그 외의 경우에는, 후보부호어들 중 에리페턴의 이진로그 무게가 가장 작은 것을 \mathbf{c}_1 으로 선택하고 에리페턴을 \mathbf{e}_1 이라 한다.
- 2) 변수 j 를 1에서 $\lfloor |T| \rfloor$ 까지 증가시키며 각각의 j 에 대하여 단계 i)에서 v)까지 수행한다.
 - i) $\mathbf{u}_j^*(\mathbf{e}_1)$ 을 경관정 복호하여 $\mathbf{u}_j(\mathbf{e}_1)$ 을 얻는다. 만약 $\mathbf{u}_j^*(\mathbf{e}_1)$ 의 경관정복호가 불가능하면 j 를 다음 값으로 한 후 다시 시도한다.
 - ii) $\mathbf{e}_j = \mathbf{e}_1 \oplus \mathbf{u}_j(\mathbf{e}_1)$ 으로 한다. 만약 $W_H(\mathbf{e}_j) < d$ 이고 $W_0(\mathbf{e}_j) \leq W_0(\mathbf{e}_j \oplus \mathbf{u}_d^*(\mathbf{e}_j))$ 이면, $\hat{\mathbf{c}} = \mathbf{y} \oplus \mathbf{e}_j$ 로 하고 종료한다.
 - iii) 만약 $j \in S$ 이면 다음 단계로 진행하고, 그렇지 않으면 j 를 다음 값으로 한 후 단계 i)로 간다.
 - iv) $q = \max\{W_H(\mathbf{e}_j), \lfloor d/2 \rfloor\} + 1$ 로 하고 $\mathbf{u}_q^*(\mathbf{e}_j)$ 를 경관정 복호하여 $\mathbf{u}_q(\mathbf{e}_j)$ 를 얻는다.
 - v) $\mathbf{e}_j' = \mathbf{e}_j \oplus \mathbf{u}_q(\mathbf{e}_j)$ 로 한다. 만약 $W_H(\mathbf{e}_j') < d$ 이고 $W_0(\mathbf{e}_j') \leq W_0(\mathbf{e}_j' \oplus \mathbf{u}_d^*(\mathbf{e}_j'))$ 이면, $\hat{\mathbf{c}} = \mathbf{y} \oplus \mathbf{e}_j'$ 으로 하고 종료한다.
- 3) 탐색된 에리페턴들 (\mathbf{e}_1 과 여러 가지 $\mathbf{e}_j, \mathbf{e}_j'$) 중에서 이진로그 무게가 가장 작은 것을 $\hat{\mathbf{e}}$ 로 선택한다. $\hat{\mathbf{c}} = \mathbf{y} \oplus \hat{\mathbf{e}}$ 로 하고 종료한다.

III. 성능 평가 및 검토

가산성 백색 가우시안 잡음이 존재하는 채널에서 BPSK 변조를 사용하는 (31, 16) BCH 부호에 대하여 컴퓨터 시뮬레이션을 수행하였다. 이때 집합 T 와 S 는 모두 {4, 5, ..., 27}로 하였다. 정보 비트 당 에너지 대 잡음 전력 스펙트럼 밀도 E_b/N_0 값을 여러 가지로 변화시키면서 결과를 얻었다. 제안된 방법과의 비교를 위하여 후보부호어 선출 불능 문제를 개선하지 않은 방법[5]과 연관정 정보를 이용하지 않은 경관정 복호법에 대해서도 함께 시뮬레이션을 수행하였다. 그림 1은 옳지 않은 복호 결과를 얻게되는 확률이고, 그림 2는 정정이 불가능하여 복호 결과를 얻을 수 없게되는 확률이다. 제안된 알고리즘에 의하여 성능이 개선되는 사실을 확인할 수 있다. 복호의 복잡도를 비교하기 위하여 하나의 부호어를 복호하는데 소요되는 경관정 복호 과정 수의 평균값을 살펴보면, E_b/N_0 가 3.0 dB일 때 제안된 알고리즘은 4.624번이고 개선되

지 않은 알고리즘은 4.593번이다. E_b/N_0 가 6.0 dB일 때는 제안된 알고리즘은 1.028번이고 개선되지 않은 알고리즘은 1.025번이다. 제안된 알고리즘의 복잡도 증가량이 거의 무시할 수 있는 수준으로 된 이유는 제안된 방법에서 복잡도를 줄이기 위한 방안들을 도입했기 때문이다. 또한, E_b/N_0 가 증가할수록 이 값이 거의 1이 된다. 이상의 결과로부터 블록 에러 확률과 정정 불능 확률이 낮아지면서도 복잡도는 거의 증가되지 않는 제안된 복호 방법의 성능 개선 효과를 확인할 수 있다.

IV. 결 론

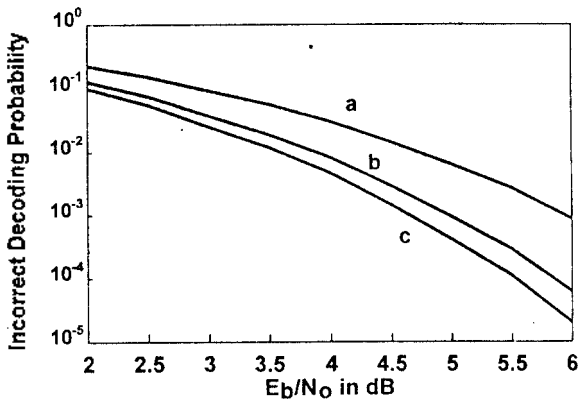
2진 BCH 부호의 연판정 복호과정에서 후보부호어가 선출되지 않는 경우의 발생을 억제할 수 있는 새로운 복호법을 제안하였다. 연판정 복호법은 오류 정정 성능이 우수하면서도 복호의 복잡도가 높지 않아야 한다. 본 논문의 제안 방법에서는 오정정 확률과 정정 불능 확률이 낮아지도록 개선하면서 복잡도 증가를 방지하는 방안들을 함께 도입하였다. 연판정 신뢰도가 낮은 위치들에 대한 경판정 값을 여러 가지 조합을 취하여 반전시킴으로써 후보부호어를 찾을 수 있도록 하였다. 또한, 후보부호어를 실제로 탐색하기 전에 이 탐색으로 최우복호에 가까운 결과를 얻을 수 있는가의 여부를 미리 알 수 있는 조건을 확립하여 복잡도 증가를 방지할 수 있었다.

2진 BCH 부호는 성능이 우수하고 경판정 복호법이 잘 확립되어 있는 대표적인 부호이다. 본 논문에서 제안한 방법으로 2진 BCH 부호에 대한 효율적인 연판정 복호법을 확립하면 디지털 통신 시스템의 신뢰도와 성능을 향상시킬 수 있을 것으로 기대된다.

참 고 문 헌

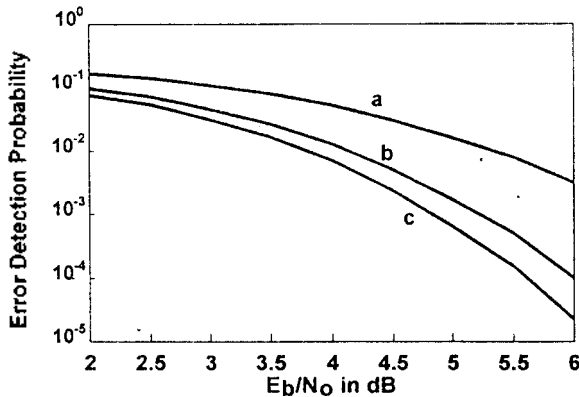
1. D. Chase, "A class of algorithms for decoding block codes with channel measurement information," IEEE Trans. Inform. Theory, vol. IT-18, pp. 170-182, Jan. 1972.
2. K. H. Farrell, L. D. Rudolph, C. R. P. Hartmann and L. D. Nielsen, "Decoding by local optimization," IEEE Trans. Inform. Theory, vol. IT-29, pp. 740-743, Sept. 1983.
3. D. J. Taipale and M. B. Pursley, "An improvement to generalized-minimum-distance decoding," IEEE Trans. Inform. Theory, vol. IT-37, pp. 167-172, Jan. 1991.
4. Y. G. Shim and C. W. Lee, "Soft-decision decoding algorithm for binary linear block codes", IEICE Trans. on Fundamentals of Electronics vol. E76-A, no. 11, pp.2016-2021, november 1993.
5. 심용길, "디지털 이동 통신 시스템에서 선형 블록 부호의 연판정 복호법," 한국음향학회지, vol. 16, no. 8, pp. 127-130, 1997년 11월.

▲심 용 길(Yong Geol Shim)
 현재: 단국대학교 전자공학과 부교수
 한국음향학회지 제16권 8호 참조



a : 경판정 복호법 b : 개선되지 않은 알고리즘
 c : 제안된 알고리즘

그림 1. (31,16) BCH 부호에 대한 복호 오류 확률
 Fig. 1 Incorrect decoding probability for (31,16) BCH code.



a : 경판정 복호법 b : 개선되지 않은 알고리즘
 c : 제안된 알고리즘

그림 2. (31,16) BCH 부호에 대한 오류 검출 확률
 Fig. 2 Error detection probability for (31,16) BCH code.