선형 블록 부호의 연판정 복호를 위한 효율적인 알고리듬

심 용 걸†

요 약

본 논문에서는 선형 블록 부호에 대한 효율적인 연판정 복호법을 제안하였다. 제안된 연판정 복호법은 경판정 복호 과정을 반복하여 실현하는 방식이다. 경판정 복호 결과로부터 후보 부호어들을 효율적으로 탐색할 수 있는 방법을 개발하였다. 이 과정에서 후보 부호어가 선출되지 않는 경우의 발생을 억제할 수 있는 새로운 복호법을 제안하였다. 또한, 복잡도를 줄이는 방안도 개발하여 알고리듬 개선으로 인한 복잡도 증가가 거의 나타나지 않도록 하였다. 2진(63, 36) BCH 부호에 대한 시뮬레이션 결과로 이러한 사실들을 확인할 수 있었다.

An Efficient Algorithm for Soft-Decision Decoding of Linear Block Codes

Yong-Geol Shim†

ABSTRACT

An efficient soft-decision decoding algorithm for binary block codes is proposed. The proposed soft-decision decoding algorithm is implemented by a series of hard-decision decoding process. By the hard-decision decoding result, the candidate codewords are efficiently searched for. A new decoding method, which prevents the missing of the candidate codeword, is proposed. 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 binary (63, 36) BCH code.

키워드 : 연판정 복호(soft-decision decoding), 에러 정정 부호(error correcting codes)

1. 서 론

에러 정정 부호는 잡음이 존재하는 디지탈 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. 이러한 연판정 복호법의 개념과 방법은 등화기를 비롯한 통신 시스템의 여러 분야에 응용되어 그 사용 범위를 넓혀가고 있다[1]. 연판정 복호법은 에러 정정 성능이 우수할수록 복호기의 복잡도가 증가한다. 따라서 복호의 복잡도를 줄이면서도 우수한 에러 정정 성능을 발휘하는 복호 방법을 개발하는 것이 필요하다. 에러 정정 부호 중 컨벌루셔널 부호는 실용적인 연판정 복호법들이 많이 개발되어 있으며, 이러한 이유로 현재는 컨벌루셔널 부호가 통신 시스템에 널리 사용되고 있다. 한 예로 Nguyen과 Kuchenbecker는 OFDM 시스템에서 컨벌루셔널 부호의 Viterbi 알고리듬을 사용하는 연판정 복호법을 연구하였다[2]. 이 예에서 볼 수 있듯이 컨벌루셔널 부호의 경우 Viterbi 알고리듬을 사용한 연판정 복호법이 주로 사용된다.

반면에 블록 부호의 경우 부호 자체의 성능 면에서는 대단히 우수한 부호들이 많이 있으나, 그에 대한 효율적인 연판정 복호법은 완전히 확립되어 있지 않다. 이러한 이유로, 우수한 성능을 가진 블록 부호들을 연판정 복호에 사용하려는 연구들이 진행 중이다. 최근의 예를 들면, Ponnampalam 등은 연판정 복호법의 성능을 개선하기 위한 새로운 거리 함수를 정의하였고[3], Tokushige 등은 제한된 거리 내에서만 복호를 수행하는 복호법을 사용할 때 후보 부호어를 찾는 방법을 제시하였다[4]. 그러나 아직도 블록 부호의 연판정 복호법들은 정정불능의 확률이 높은 단점이 있고, 동일한 후보 부호어가 중복되어 탐색되는 경우가 많아

※ 이 연구는 2001학년도 단국대학교 대학연구비의 지원으로 연구되었음.
† 정 회 원 : 단국대학교 전자·컴퓨터학부 교수
논문접수 : 2002년 9월 11일, 심사완료 : 2003년 1월 21일

복호의 효율성이 떨어지며, 낮은 에러 확률을 얻기 위해서는 복호의 복잡도가 증가하게 된다. 선형 블록 부호에 대하여 위와 같은 단점을 극복할 수 있는 연판정 복호법으로는 수신된 신호 중심의 후보 부호어들을 얻어내는 방법들이 제안되어 있다. 참고문헌 [5-7]을 비롯한 몇가지 복호법들이 이러한 범주에 속하는 방법들이다. 이러한 복호법에서 후보 부호어들을 얻어내기 위해서는 일련의 경판정 복호 과정을 반복하여 수행해야 한다. 그런데 이 경판정 복호 과정에서 정정 불능의 에러 패턴이 검출되어 후보 부호어를 찾을 수 없는 경우가 발생할 수 있으며, 이로 인해 복호기의 성능이 저하된다.

본 논문에서는 경판정 복호 과정에서 정정 불능의 에러 패턴이 검출되는 경우에도 새로운 후보 부호어를 도출해 낼 수 있는 알고리듬을 제안한다. 수신 신호 중 연판정 신뢰도가 낮은 위치들을 선택하고 이들의 경판정 값을 여러 가지 조합을 취하여 반전시켜서 후보 부호어를 찾을 수 있도록 한다. 이 때 복잡도가 늘어나는 것을 방지하기 위하여 두 가지 방안을 도입한다. 첫 번째 방안은 한 후보 부호어가 최우복호 결과인지의 여부를 판정하여 복호의 과정을 축소하는 것이다. 두 번째 방안은 수신 신호들의 일부 비트를 반전시켜 얻어진 벡터들 중 새로운 후보 부호어를 얻을 가능성이 있을 조건을 도출하고, 이 조건을 만족하는 경우에만 경판정 복호를 수행하는 것이다. 이러한 방법으로 복호의 복잡도가 증가하지 않으면서도 최우복호 결과에 근접하는 후보 부호어들을 찾아내어 성능을 높이고자 한다.

2. 복호법의 제안

C는 2진 선형 블록 부호이며, 최소 해밍거리는 d이다. C의 부호어를 $\mathbf{c}=(c_1, c_2, \cdots, c_n)$으로 표시하며, $c_i \in \{0, 1\}$이다. 각각의 비트를 BPSK로 변조하여 전송한다. 정보 비트 당 에너지를 E_b로 표시한다. 채널에서 양측 전력 스펙트럼 밀도가 $N_0/2$인 가산성 백색 가우시안 잡음이 부가되고 $\mathbf{r}=(r_1, r_2, \cdots, r_n)$이 수신된다. 수신 신호 $\mathbf{r}$로부터 경판정 $\mathbf{y}=(y_1, y_2, \cdots, y_n)$과 신뢰도 벡터 $\mathbf{b}=(b_1, b_2, \cdots, b_n)$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. 연판정 복호기는 $\mathbf{y}$와 $\mathbf{b}$를 이용하여 전송된 부호어 $\mathbf{c}$를 추정한다. 부호어 $\mathbf{c}$에 대한 에러패턴은 $\mathbf{e}=\mathbf{y} \oplus \mathbf{c}$로 주어지며, $\oplus$는 2진 덧셈을 나타낸다. 에러패턴 $\mathbf{e}=(e_1, e_2, \cdots, e_n)$의 아날로그 무게 $W_a(\mathbf{e})$를 $W_a(\mathbf{e}) = \sum_{i=1}^{n} a_i e_i$로 정의한다. 복호의 목표는 수신 신호 $\mathbf{r}$과의 거리가 가장 가까운 부호어, 즉 $W_a(\mathbf{e})$를 최소로 하는 부호어를 찾는 것이다. 이를 위하여 후보 부호어들을 선정하고 이 중에서 최적의 부호어를 찾아낸다.

최초의 후보 부호어 $\mathbf{c}_1$은 $\mathbf{y}$로부터 얻는다. 이 때 정정 불능의 에러 패턴이 검출되는 경우에도 후보 부호어를 찾아내기 위하여 $\mathbf{y}$의 비트들 중에서 신뢰도가 가장 낮은 $\lfloor d/2 \rfloor$개의 위치를 선택하고($\lfloor x \rfloor$는 x의 정수 부분), 선택된 위치들에 대해서 가능한 모든 조합을 취하여 그 위치를 반전시킨 n차원 벡터들을 구한다. 여기서 $\lfloor d/2 \rfloor$는 경판정 복호의 에러 정정 능력 $\lfloor (d-1)/2 \rfloor$를 넘는 가장 작은 정수이다. 이들 각각의 n차원 벡터를 경판정 복호하여 에러패턴들을 얻는다. 그 중에서 에러패턴의 아날로그 무게가 가장 작은 것을 $\mathbf{c}_1$으로 선택한다. 만약 모든 경판정 복호 결과들이 정정 불능의 에러로 판정되면, 에러의 검출만으로 복호를 종료한다.

후보 부호어 $\mathbf{c}_1$이 얻어진 경우에는 $\mathbf{c}_1$ 근처의 다른 후보 부호어들을 선정하고 이 중에서 최적의 부호어를 찾아낸다. 이때 복호의 복잡도를 줄이기 위하여 두 가지 방안을 도입한다. 첫 번째 방안은 한 후보 부호어가 최우복호 결과와 일치함이 밝혀지면 즉시 복호를 종료하는 것이다. 후보 부호어가 최우복호 결과와 일치하려면 다음 조건 중 하나를 만족해야 한다. 먼저 $\mathbf{c}_1$의 에러패턴 $\mathbf{e}$가 $\mathbf{0}$(영벡터)이면 그 후보 부호어는 최우복호 결과이다. 그렇지 않은 경우에는 해밍 무게 $W_H(\mathbf{e}) < \mathrm{d}$이면서 아날로그 무게는 $W_a(\mathbf{e}) \leq W_a(\mathbf{e} \oplus \mathbf{u}_d^*(\mathbf{e}))$이어야 한다. 여기서 $\mathbf{u}_d^*(\mathbf{e})$는 해밍 무게가 d인 벡터이며, $\mathbf{u}_d^*(\mathbf{e})$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. 그 이유는 $\mathbf{e}$ 이외의 에러패턴과 $\mathbf{e}$ 사이의 해밍거리가 d이상이 되어야 하기 때문에 $\mathbf{u}_d^*(\mathbf{e})$는 해밍 무게가 d인 벡터로 하였고, $\mathbf{e} \oplus \mathbf{u}_d^*(\mathbf{e})$의 아날로그 무게를 최소로 하기 위하여 위와 같이 $\mathbf{u}_d^*(\mathbf{e})$의 원소가 1과 0이 되는 위치를 정하였다. 결국, $\mathbf{e}$ 이외의 에러패턴이 $W_a(\mathbf{e})$보다 더 작은 아날로그 무게를 갖는 경우라도 그 값은 $W_a(\mathbf{e} \oplus \mathbf{u}_d^*(\mathbf{e}))$ 이상이 될 수 밖에 없는데, 만약 $W_a(\mathbf{e}) \leq W_a(\mathbf{e} \oplus \mathbf{u}_d^*(\mathbf{e}))$이 된다면 더 이상 다른 에러패턴을 찾을 필요가 없기 때문이다.

두 번째 방안은 $\mathbf{y}$의 일부 비트를 반전시켜서 얻어진 n차원 벡터들을 모두 경판정 복호할 것이 아니라, 새로운 후보 부호어를 얻을 수 있을 가능성이 있는 경우에만 그 n차원 벡터를 경판정 복호하는 것이다. 즉, 경판정 복호를 하기 전에 먼저 n차원 벡터와 이미 얻어진 후보 부호어들 사이의 해밍 거리를 계산한다. 만약 한 후보 부호어와의 해밍

거리가 $\lfloor (d-1)/2 \rfloor$ 이하로 된다면 경판정 복호 결과는 동일한 후보 부호어가 될 것이다. 결국 이미 얻어진 모든 후보 부호어들과의 해밍거리가 $\lfloor (d-1)/2 \rfloor$보다 큰 벡터들만을 경판정 복호하는 것으로 충분하다.

이제 $\mathbf{c}_1$ 이외의 다른 후보 부호어들을 찾아야 하는 경우에 사용하는 방법을 설명한다. $\mathbf{c}_1$ 이외의 다른 후보 부호어를 $\mathbf{c}_j$라 하고, $\mathbf{c}_j$에 대한 에러패턴을 $\mathbf{e}_j$로 표시한다. 여기서 j는 여러 가지 값을 가질 수 있다. 이 j값들을 원소로 갖는 집합을 T로 표시한다. 즉, $j \in T$이다. 다시 말하면, 집합 T의 각각의 원소 j에 대하여 후보 부호어 $\mathbf{c}_j$와 그 에러패턴 $\mathbf{e}_j$를 찾아나가는 것이다.

아날로그 무게가 작은 $\mathbf{e}_j$를 얻기 위하여 앞에서와 비슷한 방법으로 벡터 $\mathbf{u}_j^*(\mathbf{e})$를 생각한다. 즉, $\mathbf{u}_j^*(\mathbf{e})$는 해밍 무게가 j인 벡터이며, $\mathbf{u}_j^*(\mathbf{e})$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. 부호 C는 선형 부호이므로, $W_a(\mathbf{e} \oplus \mathbf{u}_j^*(\mathbf{e}))$가 $W_a(\mathbf{e})$보다 작더라도 $\mathbf{u}_j^*(\mathbf{e})$가 부호어가 아니라면 $\mathbf{e} \oplus \mathbf{u}_j^*(\mathbf{e})$는 에러패턴이 될 수 없다. 그래서 $\mathbf{u}_j^*(\mathbf{e})$에 가장 가까운 부호어를 찾아야하는데 그 방법으로 경판정 복호법을 사용한다. $\mathbf{u}_j^*(\mathbf{e})$를 경판정 복호하여 얻어진 부호어를 $\mathbf{u}_j(\mathbf{e})$라 하고 $\mathbf{e} \oplus \mathbf{u}_j(\mathbf{e})$를 $\mathbf{e}_j$로 놓는다. 물론 후보 부호어 $\mathbf{c}_j$는 $\mathbf{y} \oplus \mathbf{e}_j$가 된다. $\mathbf{e}_j$의 아날로그 무게 $W_a(\mathbf{e}_j)$를 다른 에러패턴들의 아날로그 무게와 비교하여 더 나은 후보 부호어를 찾는 것이다. 새로운 후보 부호어와 그의 에러패턴을 생각할 때마다 앞에서 설명한 복호 간소화 방안을 적용한다. 즉, 현재 고려 중인 후보 부호어가 최우복호 결과인지를 확인하여 복호 과정의 중단 혹은 계속 여부를 결정한다.

더 많은 후보 부호어를 찾을 필요가 있는 경우에는 $\mathbf{c}_j$를 중심으로 그 근방의 후보 부호어 $\mathbf{c}_j'$을 생각할 수도 있다. 모든 $\mathbf{c}_j$에 대하여 그 근방의 후보 부호어 $\mathbf{c}_j'$을 찾을 수도 있지만, 복호의 간소화가 필요한 경우에는 T의 부분집합인 S를 정하고, $j \in S$일때만 후보 부호어 $\mathbf{c}_j'$을 찾는다. $\mathbf{c}_j'$의 에러패턴은 $\mathbf{e}_j' = \mathbf{e}_j \oplus \mathbf{u}_q(\mathbf{e}_j)$이며, $\mathbf{u}_q(\mathbf{e}_j)$는 $\mathbf{u}_q^*(\mathbf{e}_j)$를 경판정 복호하여 얻는다. $\mathbf{u}_q^*(\mathbf{e}_j)$는 해밍 무게가 q인 벡터이며, $\mathbf{u}_q^*(\mathbf{e}_j)$의 원소가 1이 되는 곳은 $e_j = 1$ 인 $W_H(\mathbf{e}_j)$개의 위치와 $e_j = 0$이면서 신뢰도가 가장 작은 $[q - W_H(\mathbf{e}_j)]$개의 위치이다. 여기서 q는 $W_H(\mathbf{e}_j)$보다 커야한다. 또한, q가 $\lfloor d/2 \rfloor$ 이하인 경우에는 경판정 복호 결과가 $\mathbf{0}$이 되어 의미가 없다. 결국 $q = \max\{W_H(\mathbf{e}_j), \lfloor d/2 \rfloor\} + 1$로 해야 한다.

본 논문에서 제안하는 연판정 복호 알고리듬은 다음과 같다. 단, 알고리듬을 시작하기 전에 에러패턴 $\mathbf{e}_j$ 찾기를 제한하는 집합 $T = \{t_1, t_2, \cdots, t_{|T|}\}$와 파생된 에러패턴 $\mathbf{e}_j'$ 찾기를 제한하는 집합 $S = \{s_1, s_2, \cdots, s_{|S|}\}$를 결정해야 한다. 물론 S는 T의 부분집합이다.

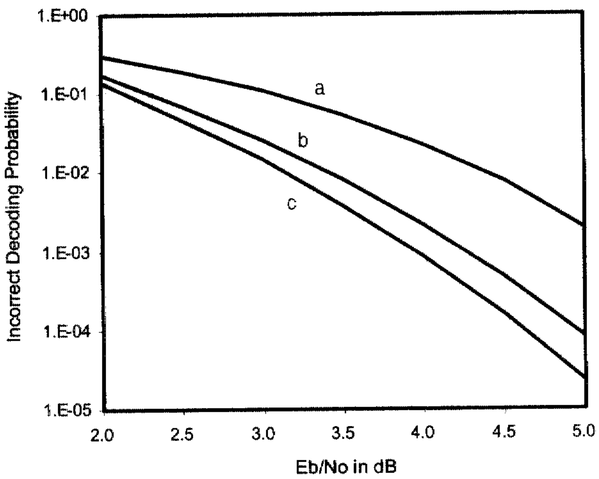
- $\mathbf{y}$의 비트들 중에서 신뢰도가 가장 낮은 $\lfloor d/2 \rfloor$개의 위치에 대해서 가능한 모든 조합을 취하여 그 위치를 반전시킨 n차원 벡터들을 경판정 복호하여 $\mathbf{c}$와 $\mathbf{e}$들을 구한다. 만약 $\mathbf{e} = \mathbf{0}$인 경우 또는 만약 $W_H(\mathbf{e}) < d$ 이면서 $W_a(\mathbf{e}) \le W_a(\mathbf{e} \oplus \mathbf{u}_d^*(\mathbf{e}))$인 경우이면 $\hat{\mathbf{c}} = \mathbf{c}$로 하고 종료한다. 그 외의 경우에는 후보 부호어들 중 에러패턴의 아날로그 무게가 가장 작은 것을 $\mathbf{c}_1$으로 선택하고 에러 패턴을 $\mathbf{e}_1$이라 한다.
- 변수 j를 t_1에서 $t_{|T|}$까지 증가시키며 각각의 j에 대하여 단계 ①에서 ⑤까지 수행한다.
  - ① $\mathbf{u}_j^*(\mathbf{e}_1)$을 경판정 복호하여 $\mathbf{u}_j(\mathbf{e}_1)$을 얻는다. 만약 $\mathbf{u}_j^*(\mathbf{e}_1)$의 경판정 복호가 불가능하면 j를 다음 값으로 한 후 다시 시도한다.
  - ② $\mathbf{e}_j = \mathbf{e}_1 \oplus \mathbf{u}_j(\mathbf{e}_1)$으로 한다. 이 때, 만약 $W_H(\mathbf{e}_j) < d$이고 $W_a(\mathbf{e}_j) \le W_a(\mathbf{e}_j \oplus \mathbf{u}_d^*(\mathbf{e}_j))$이면, $\hat{\mathbf{c}} = \mathbf{y} \oplus \mathbf{e}_j$로 하고 종료한다.
  - ③ 만약 $j \in S$이면 다음 단계로 진행하고, 그렇지 않으면 j를 다음 값으로 한 후 단계 ①로 간다.
  - ④ $q = \max\{W_H(\mathbf{e}_j), \lfloor d/2 \rfloor\} + 1$로 하고 $\mathbf{u}_q^*(\mathbf{e}_j)$를 경판정 복호하여 $\mathbf{u}_q(\mathbf{e}_j)$를 얻는다.
  - ⑤ $\mathbf{e}_j' = \mathbf{e}_j \oplus \mathbf{u}_q(\mathbf{e}_j)$로한다. 만약 $W_H(\mathbf{e}_j') < d$이고 $W_a(\mathbf{e}_j') \le W_a(\mathbf{e}_j' \oplus \mathbf{u}_d^*(\mathbf{e}_j'))$이면, $\hat{\mathbf{c}} = \mathbf{y} \oplus \mathbf{e}_j'$으로 하고 종료한다.
- 탐색된 에러패턴들 ($\mathbf{e}_1$과 여러 가지 $\mathbf{e}_j$, $\mathbf{e}_j'$) 중에서 아날로그 무게가 가장 작은 것을 $\hat{\mathbf{e}}$로 선택한다. $\hat{\mathbf{c}} = \mathbf{y} \oplus \hat{\mathbf{e}}$로 하고 종료한다.

3. 성능 평가 및 검토

가산성 백색 가우스 잡음이 존재하는 채널에서 BPSK 변조를 사용하는 (63, 36) BCH 부호에 대하여 컴퓨터 시뮬레이션을 수행하였다. 이때 T와 S는 모두 $\{6, 7, \cdots, 27\}$로 하였다. T와 S의 원소가 5 이하인 경우에는 경판정 복호결

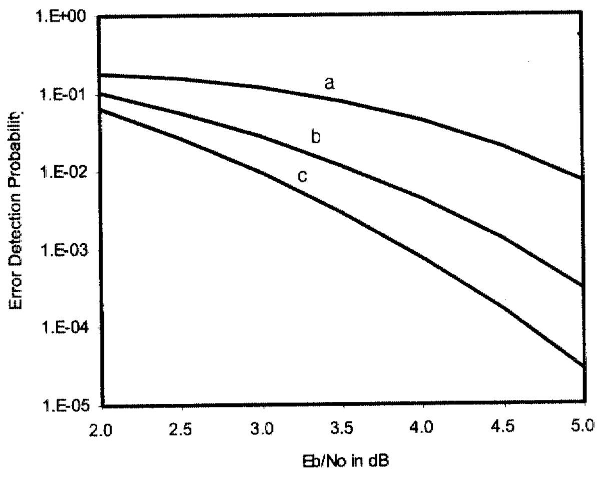
과가 영벡터가 되어 새로운 후보 부호어를 찾을 수 없다. 또한, 28 이상으로 하여도 에러 확률 성능이 거의 개선되지 않음을 시뮬레이션 과정에서 알게되어 T와 S를 $\{6, 7, \cdots, 27\}$로 정하였다.

정보 비트 당 에너지 대 잡음 전력 스펙트럼 밀도 E_b/N_o 값을 여러 가지로 변화시키면서 결과치를 얻었다. 제안된 방법과의 비교를 위하여 후보 부호어 선출 불능 문제를 개선하지 않은 방법[7]과 연판정 정보를 이용하지 않은 경판정 복호법에 대해서도 함께 시뮬레이션을 수행하였다. (그림 1)은 옳지 않은 복호 결과를 얻게되는 확률이고, (그림 2)는 정정이 불가능하여 복호 결과를 얻을 수 없게되는 확



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

(그림 1) (63, 36) BCH 부호에 대한 복호 에러 확률



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

(그림 2) (63, 36) BCH 부호에 대한 에러 검출 확률

률이다. 제안된 알고리듬에서는 경판정 복호에서 정정 불능이 되는 경우에도 후보부호어를 찾아내므로 에러 검출 확률이 현저하게 개선되는 것을 (그림 2)에서 볼 수 있다. 또한, 이 과정에서 더욱 가능성이 높은 후보부호어들이 탐색되기 때문에 제안된 알고리듬에서 복호 에러 확률 성능도 개선된다는 사실을 (그림 1)에서 확인할 수 있다. 복호 과정의 복잡도와 복호 수행에 소요되는 시간은 여러 가지 요인에 의하여 결정된다. 그러나 이 요인들 중 가장 복잡도가 높으며 긴 시간이 소요되는 것은 경판정 복호 과정이다. 따라서 본 논문에서는 경판정 복호 회수로 복호의 복잡도를 표시하기로 한다.

(63, 36) BCH 부호에 대하여 한 번의 연판정 복호과정 내에서 수행해야할 경판정 복호 회수를 수학적으로 정확하게 해석하려면 수신 신호 벡터 $\mathbf{r} = (r_1, r_2, \cdots, r_{63})$에 포함된 63개의 확률 변수로 이루어진 함수를 다루어야 한다. 물론, 이 함수식 표현 속에는 각각의 경판정 복호 과정들이 여러 가지 경우마다 다양하게 조합되어 있는 형태들을 포함하고 있어야 한다. 이러한 이유로 경판정 복호 회수의 정확한 수학적 표현은 대단히 복잡하게 된다. 따라서 본 논문에서는 경판정 복호 회수의 근사식을 유도하고, 시뮬레이션 결과를 이용하여 식을 완성시키는 방법을 사용한다.

BPSK 변조 방식에서 한 수신 심볼의 에너지는 $E_s = RE_b$로 표시할 수 있다. 여기서 E_b는 2장에서 설명한 정보 비트 당 에너지이며, R은 부호율이다. (63, 36) BCH 부호의 경우 $R = 36/63$이다. BPSK 변조 방식에서 수신 심볼 하나에 경판정 에러가 발생할 확률은 $p = Q[\sqrt{2E_s/N_o}] = Q[\sqrt{72E_b/63N_o}]$로 표시된다. 여기서 $Q(x)$는 Q-함수라 부르며 $Q(x) = \int_x^\infty (1/\sqrt{2\pi}) \exp[-\beta^2/2]\, d\beta$로 계산할 수 있다.

연판정 복호과정에서 수행해야할 경판정 복호 회수를 결정하는 가장 주된 요인은 하나의 부호에 내에 포함된 63개의 비트 중에서 발생한 경판정 에러의 수이다. (63, 36) BCH 부호에서 경판정 복호의 에러 정정 능력은 5이므로 경판정 에러의 수가 0인 경우, 1에서 5인 경우, 6이상인 경우의 세 가지로 분류하여 생각한다. 경판정 에러의 수가 0일 확률을 P_1이라 표시하며, 이 경우에는 1번의 경판정 복호만으로 연판정 복호가 완료된다. 경판정 에러의 수가 1에서 5일 확률을 P_2이라 표시하며, 이 경우에 경판정 복호 회수의 평균을 A_2로 표시한다. 경판정 에러의 수가 6 이상일 확률을 P_3이라 표시하며, 이 경우에 경판정 복호 회수의 평균을 A_3로 표시한다. 그러면, 하나의 연판정 복호 과정에서 수행되는 평균 경판정 복호 회수 A의 근사식은

$$A = P_1 + A_2P_2 + A_3P_3 \tag{1}$$

이 된다. 이 때 확률 P_1, P_2, P_3는 다음과 같이 계산할 수 있다.

$$P_1 = (1-p)^{63} \tag{2}$$

$$P_2 = \binom{63}{1} p(1-p)^{62} + \binom{63}{2} p^2(1-p)^{61} + \cdots + \binom{63}{5} p^5(1-p)^{58} \tag{3}$$

$$P_3 = 1 - P_1 - P_2 \tag{4}$$

식 (2), 식 (3), 식 (4)식으로부터 여러 가지 E_b/N_o에 대하여 P_1, P_2, P_3 값들을 계산할 수 있다. E_b/N_o가 4.0dB일 때 $P_1 = 0.0532, P_2 = 0.8803, P_3 = 0.0665$로 계산되며, E_b/N_o가 6.0dB일 때는 $P_1 = 0.3486, P_2 = 0.6508, P_3 = 0.0006$으로 계산된다. A_2와 A_3는 시뮬레이션 결과를 이용하여 값을 추정한다. 시뮬레이션에서 평균 경판정 복호 회수 A는 E_b/N_o가 4.0dB일 때 1.337번이고, E_b/N_o가 6.0dB일 때는 1.021번이 되었다. 이 두 경우의 P_1, P_2, P_3와 A값들을 식 (1)에 대입하여 A_2와 A_3를 추정하면 $A_2 = 1.028$, $A_3 = 5.693$을 얻는다. 따라서 하나의 연판정 복호 과정에서 수행되는 평균 경판정 복호 회수 A의 근사식은 $A = P_1 + 1.028\,P_2 + 5.693\,P_3$가 된다. 예를들어 E_b/N_o가 6.0dB일 때 그 의미를 살펴보면, 경판정 복호를 $A_3 = 5.693$ 즉 5내지 6번 정도 할 확률은 불과 $P_3 = 0.0006$에 지나지 않고, $P_1 + P_2 = 0.9994$의 확률로 경판정 복호를 거의 1회 정도 수행함을 알 수 있다. 물론 이로부터 한번의 연판정 복호를 수행하는데 소요되는 대략적인 시간을 파악할 수 있다.

본 논문에서 제안하는 알고리듬과 참고문헌 [7]의 방법에 대하여 경판정 복호 과정 수의 평균값을 비교해 보면, E_b/N_o가 4.0dB일 때 제안된 알고리듬은 1.337번이고 개선되지 않은 알고리듬은 1.284번이다. E_b/N_o가 6.0dB일 때는 제안된 알고리듬은 1.021번이고 개선되지 않은 알고리듬은 1.016번이다. 제안된 알고리듬이 에러 확률 성능 면에서 현저하게 개선되었으면서도 복잡도 증가량은 거의 무시할 수 있는 수준으로 된 것을 확인할 수 있다. 그 이유는 제안된 방법에서 복잡도를 줄이기 위한 방안들을 도입했기 때문이다. 이상의 결과로부터 블록 에러 확률과 정정 불능의 확률이 낮아지면서도 복잡도는 거의 증가되지 않는 제안된 복호 방법의 성능 개선 효과를 확인할 수 있다.

4. 결 론

선형 블록 부호에 대한 효율적인 연판정 복호법을 제안하였다. 일련의 경판정 복호 과정을 반복하여 연판정 복호를 실현한다. 이 때, 최초로 수행된 경판정 복호 결과로부터 후보 부호어들을 효율적으로 탐색할 수 있는 방법을 개발하였다. 이 과정에서 후보 부호어가 선출되지 않는 경우의 발생을 억제할 수 있는 새로운 복호법을 제안하였다. 또한, 복잡도를 줄이는 방안도 개발하여 알고리듬 개선으로 인한 복잡도 증가가 거의 나타나지 않도록 하였다.

연판정 복호법은 에러 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 후보 부호어를 찾을 수 있도록 하였다. 또한, 후보 부호어를 실제로 탐색하기 전에 이 탐색으로 최우복호에 가까운 결과를 얻을 수 있는가의 여부를 미리 알 수 있는 조건을 확립하여 복잡도 증가를 방지할 수 있었다.

선형 블록 부호는 성능이 우수하고 경판정 복호법이 잘 확립되어 있고, 에러 정정 능력이 우수한 부호이다. 본 논문에서 제안한 방법으로 선형 블록 부호에 대한 효율적인 연판정 복호법을 확립하면 디지탈 통신 시스템의 신뢰도와 성능을 향상시킬 수 있다.

참 고 문 헌

[1] J. Egle, C. Sgraja and J. Lindner, "Iterative Soft Cholesky Block Decision Feedback Equalizer - a Promising Approach to Combat Interference," Proceeings of the 53rd IEEE Vehicular Technology Confernece, pp.1604-1608, May, 2001.

[2] V. D. Nguyen and H. Kuchenbecker, "Block Interleaving for Soft Decision Viterbi Decoding in OFDM Systems," Proceeings of the 54th IEEE Vehicular Technology Confernece, pp.470-474, Oct., 2001.

[3] V. Ponnampalam, A. Grant and B. Vucetic, "A Class of Soft Decoding Algorithms," Proceedings of the 2001 IEEE International Symposium on Information Theory, pp.258-258, June, 2001.

[4] H. Tokushige, K. Nakamaye, T. Koumoto, Y. S. Tang and T. Kasami, "Selection of Search Centers in Iterative Soft-Decision Decoding Algorithms," IEICE Trans. on Fundamentals of Electronics, Communications & Computer Sciences, Vol.E84-A, No.10, pp.2397-2403, Oct., 2001.

[5] 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.

[6] 심용걸, 이충웅, "선형 2원 블록 부호를 위한 연판정 복호 알고리듬", 전자공학회논문지, 제27권 제2호, pp.9-15, 1990.

[7] Y. G. Shim and C. W. Lee, "Soft-decision decoding algorithm for binary linear block codes," IEICE Trans. on Fundamentals of Electronics, Communications & Computer Sciences, Vol.E76-A, No.11, pp.2016-2021, Nov., 1993.

심 용 걸

e-mail : ygshim@dku.edu

1982년 서울대학교 전자공학과(공학사)

1984년 서울대학교 대학원 전자공학과 (공학석사)

1982년 서울대학교 대학원 전자공학과 (공학박사)

1988년~현재 단국대학교 교수

관심분야 : 통신공학, 부호이론, 정보이론