신뢰도 값을 이용한 블록 부호의 반복적 연판정 복호 알고리즘

심 용 걸†

요 약

본 논문에서는 블록 부호의 반복적 연판정 복호 알고리즘을 제안하였다. 최초의 경판정 복호 결과에 대한 분석을 바탕으로 후보 부호어들을 효율적으로 탐색할 수 있는 방법을 개발하였다. 복호의 복잡도를 줄이고 에러 확률을 감소시키기 위하여 적은 갯수의 후보 부호어들을 선택한다. 이 때, 수신 신호로부터 가까운 거리에 존재하는 부호어가 포함되어 있을 확률이 크도록 후보 부호어들을 선택한다. 선택된 후보 부호어까지의 거리를 계산하여 가장 가까운 후보 부호어를 복호 결과로 선정한다. 제안된 방법에 의하여 신뢰도 값이 작은 비트들을 에러 패턴에 포함시키게 하는 후보 부호어를 탐색할 수 있으며, 이미 탐색된 후보 부호어가 다시 선정되는 경우를 방지할 수 있다. (23, 12) Golay 부호에 대하여 시뮬레이션을 수행하고 그 결과를 제시하였다. 복호의 복잡도가 현저히 감소되었고, 블록 에러 확률이 저하된 사실을 시뮬레이션 결과에서 확인할 수 있었다.

An Iterative Soft-Decision Decoding Algorithm of Block Codes Using Reliability Values

Yong-Geol Shim†

ABSTRACT

An iterative soft-decision decoding algorithm of block codes is proposed. With careful examinations of the first hard-decision decoding result, the candidate codewords are efficiently searched for. An approach to reducing decoding complexity and lowering error probability is to select a small number of candidate codewords. With high probability, we include the codewords which are at the short distance from the received signal. The decoder then computes the distance to each of the candidate codewords and selects the codeword which is the closest. We can search for the candidate codewords which make the error patterns contain the bits with small reliability values. Also, we can reduce the cases that we select the same candidate codeword already searched for. Computer simulation results are presented for (23, 12) Golay code. They show that decoding complexity is considerably reduced and the block error probability is lowered.

키워드 : 연판정 복호(Soft-Decision Decoding), 에러 정정 부호(Error Correcting Codes)

1. 서 론

연판정 복호법은 디지탈 통신 시스템에서 통신로 측정 정보인 연판정 정보를 이용하여 복호하는 방법이다. 연판정 복호를 위해서는 경판정 복호를 행하는 부분 외에도 연판정 정보를 추출하고 처리하는 부분이 추가되지만, 추정된 경판정 값의 정확성에 관한 정보를 복호 과정에 이용하므로 성능을 향상시킬 수 있다.

에러 정정 부호 중 컨벌루셔널 부호는 실용적인 연판정 복호법들이 많이 개발되어 있으며, 이러한 이유로 현재는 컨벌루셔널 부호가 통신 시스템에 널리 사용되고 있다. 컨벌루셔널 부호의 경우 Viterbi 알고리즘을 사용한 연판정 복호법[1, 2]이 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. Forney가 GMD(generalized minimum distance) 알고리즘[3]을 제안한 이후에 Chase는 Forney의 방법을 더욱 발전시켜서 세가지의 알고리즘[4]를 제안하였다. 특히 Chase의 알고리즘 2는 현재까지 알려진 방법들 중 가장 대표적인 것으로 평가받고 있으며 새로운 방법을 제안할 때 비교의 대상으로 선택되는 경우가 많다. Hacket는 최소 해밍 거리가 짝수인 부호에만 적용되는 방법[5]를 제안하였다. 전체 패리티가 짝수이면 가장 신뢰도가 낮은 비트를 반전시키고 연판정 복호를 수행한다. Tendolkar와 Hartmann은 Chase 알고리즘을 보다 일반화[6]시켰다. 경

※ 이 연구는 2003학년도 단국대학교 대학연구비의 지원으로 연구되었음.
† 정 회 원 : 단국대학교 전자·컴퓨터학부 교수
논문접수 : 2003년 6월 17일, 심사완료 : 2004년 2월 18일

판정 복호기의 에러 정정 능력이 적은 경우에도 적용될 수 있도록 Chase 방법을 일반화한 것이다. Taipale와 Pursley는 Forney의 GMD 알고리즘 중에서 수용 판단 기준을 새로이 바꾸어 개선시킨 방법[7]를 제안하였다. Shim과 Lee는 일반적인 선형 블록 부호에 적용하여 복호 에러 확률을 감소시킬 수 있는 복호법[8]를 제안하였다. 최근에는 Ponnampalam 등이 연판정 복호법의 성능을 개선하기 위한 새로운 거리 함수를 정의[9]하였고, Tokushige등은 제한된 거리 내에서만 복호를 수행하여 후보 부호어를 찾는 방법[10]을 제시하였다. 그러나 이 방법들도 복호의 복잡도와 에러 확률 면에서 동시에 우수한 성능을 나타내지는 않고 있다. 아직도 블록 부호의 연판정 복호법들은 올바른 부호어가 후보 부호어에 포함될 확률을 높이기 어려운 단점이 있고, 동일한 후보 부호어가 중복되어 탐색되는 경우가 많아 복호의 효율성이 떨어진다. 또한, 낮은 에러 확률을 얻기 위해서는 복호의 복잡도가 증가하게 된다.

본 논문에서는 복호의 복잡도를 줄이고 에러 확률을 감소시키기 위하여 몇 개의 후보 부호어를 원소로 갖는 집합을 구성한다. 물론, 수신 계열로부터 최소 거리에 존재하는 부호어가 이 집합에 들어있을 확률이 크도록 집합을 구성해야 한다. 집합에 속한 후보 부호어까지의 거리를 계산하여 가장 가까운 부호어를 복호 결과로 선택한다. 첫 번째 부호어는 수신 계열을 경판정 복호하여 얻어진 부호어로 하며, 다른 부호어들도 역시 경판정 복호 과정을 반복 수행하여 얻는다. 이 때 소요되는 경판정 복호의 횟수가 연판정 복호법의 복잡도를 결정한다. 최초의 경판정 복호로 얻어진 부호어에 대한 에러들의 위치와 의심스러운 비트들의 위치를 비교하여, 다른 후보 부호어들을 효율적으로 찾아낼 수 있는 방법을 연구한다. 이 방법을 사용하여 복호의 복잡도를 줄이면서 블록 에러 확률을 감소시키는 연판정 복호법을 제안하고자 한다.

2. 연판정 복호법

2.1 시스템의 구성

부호 C는 (n, k) 2진 선형 블록 부호이며, 최소 해밍거리는 d이다. 부호화율은 $R=k/n$이다. C의 부호어를 $\mathbf{c}=(c_1, c_2, \cdots, c_n)$으로 표시하며, $c_i \in \{0,1\}$이다. 부호 심볼 c_i는 반극성(antipodal) 신호 $s_i=\sqrt{E_s}(1-2c_i)$로 변환된다. 여기서 E_s는 심볼당 평균 에너지이다. 이 때, 정보 비트당 에너지는 $E_b=E_s/R$이다. 신호벡터 $\mathbf{s}=(s_1, s_2, \cdots, s_n)$은 무기억 통신로를 통하여 전송되며, 잡음이 부가되어 $\mathbf{r}=(r_1, r_2, \cdots, r_n)$으로 수신된다. 수신 심볼 r_i는 수신기의 정합 필터 출력 전압이며 $r_i=s_i+z_i$이다. 여기서 $z_1, z_2, \cdots, z_n$은 모두 상호 독립이며 평균이 0이고 분산이 $N_0/2$인 가산성 백색 가우시안 불규칙 변수이다. N_0는 편측 잡음 전력 밀도이다. 수신측의 판정기에서는 $\mathbf{r}$을 수신하여 2개의 출력을 발생시킨다. 그 중 하나가 경판정 $\mathbf{y}=(y_1, y_2, \cdots, y_n)$인데, $r_i \geq 0$이면 $y_i=0$으로, $r_i<0$이면 $y_i=1$로 한다. 다른 하나는 신뢰도 벡터 $\mathbf{a}=(a_1, a_2, \cdots, a_n)$이며, $a_i=|r_i|$이다. 연판정 복호기는 $\mathbf{y}$와 $\mathbf{a}$를 이용하여 전송된 부호어를 추정한다. 추정된 부호어를 $\hat{\mathbf{c}}$로 표시한다. 부호어 $\mathbf{c}$에 대한 에러패턴은 $\mathbf{e}=\mathbf{y}\oplus\mathbf{c}$로 주어진다. 여기서 $\oplus$는 2진 덧셈을 나타낸다. 복호의 목표는 에러패턴 $\mathbf{e}=(e_1, e_2, \cdots, e_n)$의 아날로그 무게 $W_a(\mathbf{e})=\sum_{i=1}^{n} a_i e_i$를 최소로 하는 최적의 부호어 $\hat{\mathbf{c}}$를 찾는 것이다. $\mathbf{e}$는 2진 벡터이므로 $\mathbf{e}$의 원소는 0 또는 1로 구성된다. 이러한 원소들 중에서 1의 갯수를 그 2진 벡터의 해밍 무게라 한다. 에러 패턴 $\mathbf{e}$의 해밍 무게를 $W_H(\mathbf{e})$로 표시한다.

2.2 후보 부호어 결정 방법

최초의 후보 부호어는 $\mathbf{y}$를 경판정 복호한 $\mathbf{c}_1$이다. 완전 부호가 아닌 경우에는 정정 불능인 에러가 검출되는 수도 있다. 이 때는 $\mathbf{y}$의 비트들 중 가장 신뢰도가 낮은 것을 반전시키고 다시 경판정 복호를 수행하여 $\mathbf{c}_1$을 얻는다. 만약 그래도 정정 불능인 에러가 검출되면, 에러의 검출만으로 복호를 마친다. $\mathbf{c}_1$이 얻어지면 이에 따른 에러패턴은 $\mathbf{e}_1=\mathbf{y}\oplus\mathbf{c}_1(e_{11}, e_{12}, \cdots, e_{1n})$이다. 만약 $\mathbf{e}_1=\mathbf{0}$($\mathbf{0}$은 영벡터)이면, 아날로그 무게는 0으로 최소가 된다. 따라서 $\mathbf{c}_1$이 최우 복호 결과이므로, 이 경우에는 $\hat{\mathbf{c}}=\mathbf{c}_1$으로 하고 복호를 종료한다.

만약 $\mathbf{e}_1 \neq \mathbf{0}$이면, 다른 후보 부호어들을 찾는다. $\mathbf{c}_1$이 아닌 후보 부호어들 중 하나를 $\mathbf{c}_j$로 표시하자. C는 선형 부호이므로 $\mathbf{c}_j$를 $\mathbf{c}_1\oplus\mathbf{u}_j$로 표시할 수 있으며, 여기서 $\mathbf{u}_j=(u_{j1}, u_{j2}, \cdots, u_{jn})$ 은 또 다른 부호어이다. 물론, $\mathbf{c}_j \neq \mathbf{c}_i$이며, $\mathbf{u}_j \neq \mathbf{0}$이다. $\mathbf{c}_j$에 대한 에러패턴은 $\mathbf{e}_j=\mathbf{y}\oplus\mathbf{c}_j=\mathbf{y}\oplus\mathbf{c}_i\oplus\mathbf{u}_j=\mathbf{e}_1\oplus\mathbf{u}_j$이다. 결국, $\mathbf{e}_j$의 아날로그 무게는

$$W_a(\mathbf{e}_j)=W_a(\mathbf{e}_i\oplus\mathbf{u}_j)=\sum_{i=1}^{n} a_i(e_{1i}\oplus u_{ji}) \qquad (1)$$

로 되므로 이것을 최소로 하는 부호어 $\mathbf{u}_j$를 찾아야 한다. 식 (1)을 최소로 하려면 e_{1i}가 0일때 u_{ji}도 0이 되고 e_{1i}가 1일때 u_{ji}도 1이 되면 좋을 것이다. 그러나, $\mathbf{e}_1$의 해밍 무게는 에러의 갯수이므로 $d/2$ 이하인 반면에, $\mathbf{u}_j$는 부호어이므로 $\mathbf{u}_j$의 해밍 무게는 d 이상이어야 한다. 그러므로 e_{1i}와 u_{ji}가 항상 일치할 수만은 없다. 부호어 $\mathbf{u}_j$를 찾기에 앞서서 먼저 2진 벡터 $\mathbf{u}_j^*=(u_{j1}^*, u_{j2}^*, \cdots, u_{jn}^*)$를 생각한다. $\mathbf{u}_j^*$의 원소가 1이 되는 곳은 $e_{1i}=1$인 $W_H(\mathbf{e}_1)$개의 위치와 $e_{1i}=0$이면서 신뢰도가 가장 작은 $[j-W_H(\mathbf{e}_1)]$개의 위치이며 그 외의 위치에서는 모두 0으로 한다. $\mathbf{u}_j^*$의 해밍 무게 $W_H(\mathbf{u}_j^*)$는 j이며, $j>W_H(\mathbf{e}_j)$이다. $\mathbf{u}_j^*$를 경판정 복호하여 얻어지는

부호어가 $\mathbf{u}_j$로 된다. 해밍 무게가 j인 모든 n차원 2진 벡터 중에서 $\mathbf{u}_j^*$가 에러 패턴의 아날로그 무게를 최소가 되게 한다. 이것을 [정리 1]에서 설명한다.

[정리 1] 해밍 무게가 j이며 $\mathbf{u}_j^*$가 아닌 임의의 n차원 2진 벡터를 $\mathbf{b}_j$라 하면, 아날로그 무게 $W_a(\mathbf{e}_1 \oplus \mathbf{u}_j^*)$는 $W_a(\mathbf{e}_1 \oplus \mathbf{b}_j)$보다 작거나 같다.

[증명] 신뢰도 벡터 $\mathbf{a}=(a_1, a_2, \cdots, a_n)$의 원소들을 다음과 같이 3가지 집합으로 분류한다.

$$A_1 = \{ a_i \mid e_{1i}=1\text{이고 } u_{ji}^*=1\} = \{\alpha(1), \alpha(2), \cdots, \alpha(L)\}$$
$$A_2 = \{ a_i \mid e_{1i}=0\text{이고 } u_{ji}^*=1\} = \{\beta(1), \beta(2), \cdots, \beta(j-L)\}$$
$$A_2 = \{ a_i \mid e_{1i}=0\text{이고 } u_{ji}^*=0\} = \{\gamma(1), \gamma(2), \cdots, \gamma(n-j)\}$$

여기서 $W_H(\mathbf{e}_1)$을 L로 표시하였고, $\beta(1) \le \beta(2) \le \cdots \le \beta(j-L)$과 $\gamma(1) \le \gamma(2) \le \cdots \le \gamma(n-j)$로 가정하였다. $\mathbf{u}_j^*$는 $e_{1i}=0$이면서 신뢰도가 가장 작은 $(j-L)$개의 위치에 1을 갖기 때문에 A_2의 가장 큰 원소라도 A_3의 가장 작은 원소보다 클 수 없다. 즉,

$$\begin{aligned}&\beta(1) \le \beta(2) \le \cdots \le \beta(j-L) \le \\ &\gamma(1) \le \gamma(2) \le \cdots \le \gamma(n-j)\end{aligned} \tag{2}$$

이다. 따라서 $W_a(\mathbf{e}_1 \oplus \mathbf{u}_j^*) = \sum_{i=1}^{n} a_i(e_{1i} \oplus u_{ji}^*) = \sum_{N=1}^{j-L} \beta(N)$이다.

n차원 2진 벡터 $\mathbf{b}_j$와 $\mathbf{u}_j^*$의 원소가 서로 다른 위치의 수를 $e_{1i}=1$인 곳에서 f개, $e_{1i}=0$이고 $u_{ji}^*=1$인 곳에서 g개로 가정하면, $W_H(\mathbf{b}_j) = W_H(\mathbf{u}_j^*)$이므로 $e_{1i}=0$이고 $u_{ji}^*=0$인 곳에서는 $(f+g)$개의 위치에서 서로 다르다. 결국, $\mathbf{b}_j$와 $\mathbf{u}_j^*$는 총 $2(f+g)$개의 위치에서 서로 다르다. $e_{1i}=1$인 f개의 상이한 위치에 해당하는 신뢰도 값들을 $\alpha(m_1), \alpha(m_2), \cdots, \alpha(m_f)$로 표시하자. 같은 방법으로, $e_{1i}=0$이고 $u_{ji}^*=1$인 g개의 상이한 위치의 신뢰도 값들을 $\beta(h_1), \beta(h_2), \cdots, \beta(h_g)$, $e_{1i}=0$이고 $u_{ji}^*=0$인 $(f+g)$개의 상이한 위치의 신뢰도 값들을 $\gamma(p_1), \gamma(p_2), \cdots, \gamma(p_{f+g})$로 표시하자. 그러면,

$$\begin{aligned}&W_a(\mathbf{e}_1 \oplus \mathbf{b}_j) - W_a(\mathbf{e}_1 \oplus \mathbf{u}_j^*) \\ &= [\alpha(m_1) + \alpha(m_2) + \cdots + \alpha(m_f)] \\ &+ [\gamma(p_1) + \gamma(p_2) + \cdots + \gamma(p_{f+g})] \\ &- \beta(h_1) + \beta(h_2) + \cdots + \beta(h_g)]\end{aligned}$$

가 된다. 신뢰도 값들은 음이 아니므로 $[\alpha(m_1)+\alpha(m_2)+\cdots+\alpha(m_f)]$는 음이 아니다. 또한, 식 (2)으로부터 $[\gamma(p_1)+\gamma(p_2)+\cdots+\gamma(p_{f+g})]-[\beta(h_1)+\beta(h_2)+\cdots+\beta(h_g)]$도 음이 아니다. 이것은 $W_a(\mathbf{e}_1 \oplus \mathbf{u}_j^*) \le W_a(\mathbf{e}_1 \oplus \mathbf{b}_j)$임을 의미하며, 이것으로 정리 1이 증명되었다. (증명 끝)

이제 $\mathbf{u}_d^*$를 생각한다. $\mathbf{u}_d^*$의 해밍 무게는 부호의 최소 해밍 거리 d이다. 어떠한 에러 패턴의 아날로그 무게도 $W_a(\mathbf{e}_1 \oplus \mathbf{u}_d^*)$보다 작을 수 없다. 이것을 [정리 2]에서 설명한다.

[정리 2] $\mathbf{0}$이 아닌 임의의 부호어를 $\mathbf{x}$라 하면, 아날로그 무게 $W_a(\mathbf{e}_1 \oplus \mathbf{u}_d^*)$는 $W_a(\mathbf{e}_1 \oplus \mathbf{x})$보다 작거나 같다.

[증명] $W_H(\mathbf{x})$를 j라 하자. $\mathbf{x}$는 부호어이므로 $j \ge d$이다. 그러면, [정리 1]에 의하여 $W_a(\mathbf{e}_1 \oplus \mathbf{u}_j^*) \le W_a(\mathbf{e}_1 \oplus \mathbf{x})$이다. $\mathbf{u}_d^*$와 $\mathbf{u}_j^*$의 원소가 공통으로 1이 되는 곳은 $e_{1i}=1$인 $W_H(\mathbf{e}_1)$개의 위치와 $e_{1i}=0$이면서 신뢰도가 가장 작은 $[d-W_H(\mathbf{e}_1)]$개의 위치이다. $\mathbf{u}_j^*$는 이외에도 $e_{1i}=0$이면서 신뢰도가 다음으로 작은 $(j-d)$개의 위치에 1을 갖는다. 따라서 $W_a(\mathbf{e}_1 \oplus \mathbf{u}_j^*) - W_a(\mathbf{e}_1 \oplus \mathbf{u}_d^*)$는 $(j-d)$개의 신뢰도 값들의 합이 되며, 이것은 음이 아니다. 그러므로 $W_a(\mathbf{e}_1 \oplus \mathbf{u}_d^*) \le W_a(\mathbf{e}_1 \oplus \mathbf{u}_j^*)$이다. 결국, $W_a(\mathbf{e}_1 \oplus \mathbf{u}_j^*) \le W_a(\mathbf{e}_1 \oplus \mathbf{x})$이며, 이것으로 [정리 2]가 증명되었다. (증명 끝)

[정리 2]로부터, 만약 $W_a(\mathbf{e}_1) \le W_a(\mathbf{e}_1 \oplus \mathbf{u}_d^*)$이면, $W_a(\mathbf{e}_1)$이 에러패턴의 최소 아날로그 무게가 되어 최대 우도 복호 결과는 $\mathbf{c}_1$임을 알 수 있다. 이 경우에는 $\hat{\mathbf{c}} = \mathbf{c}_1$으로 하고 복호를 종료한다. 이에 따라 복호의 복잡도는 줄어든다.

만약 $W_a(\mathbf{e}_1) > W_a(\mathbf{e}_1 \oplus \mathbf{u}_d^*)$이면, $\mathbf{c}_1$ 근처의 후보 부호어들을 찾는다. 앞에서 언급했듯이 $\mathbf{u}_j^*$를 형성시키고 $\mathbf{u}_j^*$를 경판정 복호하여 $\mathbf{u}_j$를 얻는다. 이 과정을 상세히 설명한다. $\mathbf{u}_j^*$의 해밍 무게들을 원소로 갖는 집합 T를 생각하자. $|T|$는 집합 T의 크기를 의미한다. T를 $\{t_1, t_2, \cdots, t_{|T|}\}$로 표시하고, $t_1 < t_2 < \cdots < t_{|T|}$로 가정한다. 변수 j는 $t_1, t_2, \cdots, t_{|T|}$의 값을 순서대로 갖는다. 각각의 j에 대하여 $\mathbf{u}_j^*$를 형성시킨다. 복호의 복잡도를 감소시키기 위하여, 임계값 Φ를 정하고 신뢰도 값과 비교한다. $e_{1i} \oplus u_{ji}^*=1$ 인 $[j-W_H(\mathbf{e}_1)]$개의 위치에 해당하는 신뢰도 값들이 모두 Φ보다 작거나 같은 경우에만 $\mathbf{u}_j^*$를 형성시킨다. (만약 임계값을 사용하지 않으려면 $\Phi=\infty$로 한다.)

$\mathbf{u}_j^*$는 부호어가 아닐 수도 있기 때문에, $\mathbf{u}_j^*$를 경판정 복호하여 $\mathbf{u}_j$를 얻는다. $\mathbf{u}_j$는 $\mathbf{u}_j^*$로부터 가장 가까운 부호어이다. 어떤 j값에 대해서는, $\mathbf{u}_j^*$의 경판정 복호가 불가능한 경우도 있다. 이러한 경우에는 다음 j값으로 넘어간다. 각각의 $\mathbf{u}_j$에 대한 후보 부호어는 $\mathbf{c}_j = \mathbf{c}_1 \oplus \mathbf{u}_j$이고, $\mathbf{c}_j$에 대한 에러패턴은 $\mathbf{e}_j = \mathbf{e}_1 \oplus \mathbf{u}_j$이다.

$\mathbf{c}_1$ 근처의 후보 부호어 $\mathbf{c}_i$를 찾은 것과 비슷한 방법으로 $\mathbf{c}_i$ 근처의 후보 부호어 $\mathbf{c}_i'$을 찾을 수 있다. $\mathbf{u}_j^*$를 생각한 것과 같은 이유로 2진 벡터 $\mathbf{v}_q^*$를 생각한다. $\mathbf{v}_q^*$의 해밍무게 $W_H(\mathbf{v}_q^*)$는 $q(q > W_H(\mathbf{e}_j))$이다. $\mathbf{v}_q^*$의 원소가 1이 되는 곳은 $e_{ji}=1$인 $W_H(\mathbf{e}_j)$개의 위치와 $e_{ji}=0$이면서 신뢰도가 가장 작은 $[q-W_H(\mathbf{e}_j)]$개의 위치이다. $\mathbf{u}_d^*$를 이용했던 것

과 동일한 방법으로 $\mathbf{v}_d^*$를 이용한다. 만약 $W_H(\mathbf{e}_j) < d$이고 $W_a(\mathbf{e}_j) \le W_a(\mathbf{e}_j \oplus \mathbf{v}_d^*)$이면 $W_a(\mathbf{e}_j)$가 에러 패턴의 최소 아날로그 무게가 되어 최대 우도 복호 결과는 $\mathbf{c}_j$이다. 이 경우에는 $\hat{\mathbf{c}} = \mathbf{c}_j$로 하고 복호를 종료한다. 이에 따라 복호의 복잡도는 줄어든다.

만약 $W_a(\mathbf{e}_j) > W_a(\mathbf{e}_j \oplus \mathbf{v}_d^*)$이면 $\mathbf{c}_j$ 근처의 부호어 $\mathbf{c}_j'$를 찾는다. 그러나, 복호 복잡도의 간소화를 위하여 $\mathbf{c}_j'$ 찾기를 제한하는 집합 S를 도입한다. S는 T의 부분집합이며, $j \in S$일 때에만 $\mathbf{c}_j'$를 찾는다. $\mathbf{c}_j'$를 찾는 방법은 다음과 같다. $q = \max\{W_H(\mathbf{e}_j), \lfloor d/2 \rfloor\} + 1$로 하고, 2진 벡터 $\mathbf{v}_q^*$를 형성시킨다. ($\lfloor z \rfloor$)는 z의 정수 부분을 표시한다.) $\mathbf{v}_q^*$를 경판정 복호하여 얻은 부호어를 $\mathbf{v}$라 하면, 후보 부호어 $\mathbf{c}_j'$는 $\mathbf{c}_j \oplus \mathbf{v}$이며 $\mathbf{c}_j'$에 대한 에러패턴은 $\mathbf{e}_j' = \mathbf{e}_j \oplus \mathbf{v}$이다. 만약 $W_H(\mathbf{e}_j') < d$이면, $\mathbf{u}_d^*$나 $\mathbf{v}_d^*$를 생각했던 것과 같은 방법으로 2진 벡터 $\mathbf{w}_d^*$를 생각한다. $\mathbf{w}_d^*$의 원소가 1이 되는 곳은 $e_{ji}' = 1$인 $W_H(\mathbf{e}_j')$개의 위치와 $e_{ji}' = 0$이면서 신뢰도가 가장 작은 $[d - W_H(\mathbf{e}_j')]$개의 위치이다. 만약 $W_a(\mathbf{e}_j') \le W_a(\mathbf{e}_j' \oplus \mathbf{w}_d^*)$이면 $W_a(\mathbf{e}_j')$가 에러 패턴의 최소 아날로그 무게가 되어 최우 복호 결과는 $\mathbf{c}_j'$이다. 이 경우에는 $\hat{\mathbf{c}} = \mathbf{c}_j'$으로 하고 복호를 종료한다. 후보 부호어들($\mathbf{c}_1$과 여러가지 $\mathbf{c}_j$, $\mathbf{c}_j'$) 중에서 에러 패턴의 아날로그 무게를 최소로 하는 것을 $\hat{\mathbf{c}}$로 선택한다.

2.3 연판정 복호 과정

제안된 연판정 복호 알고리즘을 설명한다. 알고리즘을 시작하기 전에, 집합 T와 그 부분집합 S, 그리고 임계값 ϕ가 결정되어야 한다. 복호 결과는 $\hat{\mathbf{c}}$이다.

1) $\mathbf{y}$를 경판정 복호하여 $\mathbf{c}_1$과 $\mathbf{e}_1$을 얻는다. 만약 $\mathbf{y}$의 경판정 복호가 불가능하면, $\mathbf{y}$의 비트들 중 가장 신뢰도가 낮은 것을 반전시키고 다시 경판정 복호를 수행한다. 만약 그렇게 하여도 경판정 복호가 불가능하면 정정 불가능한 에러임을 표시하고 종료한다.
2) 만약 $\mathbf{e}_1 = \mathbf{0}$이거나 $W_a(\mathbf{e}_1) \le W_a(\mathbf{e}_1 \oplus \mathbf{u}_d^*)$이면, $\hat{\mathbf{c}} = \mathbf{c}_1$으로 하고 종료한다.
3) 변수 j를 t_1에서 $t_{|T|}$까지 증가시키며 각각의 j에 대하여 단계 i)에서 단계 vi)까지 수행한다.
   i) 임계값 비교에 의하여 $\mathbf{u}_j^*$를 형성시킬 필요가 없으면 단계 4)로 간다.
   ii) $\mathbf{u}_j^*$를 형성시킨다. $\mathbf{u}_j^*$를 경판정 복호하여 $\mathbf{u}_j$를 얻는다. 만약 $\mathbf{u}_j^*$의 경판정 복호가 불가능하면, $\mathbf{u}_j^*$를 버리고 j를 다음 값으로 한 후 단계 i)로 간다.
   iii) $\mathbf{e}_j = \mathbf{e}_1 \oplus \mathbf{u}_j$로 한다. 이 때, 만약 $W_H(\mathbf{e}_j) < d$이고 $W_a(\mathbf{e}_j) \le W_a(\mathbf{e}_j \oplus \mathbf{v}_d^*)$이면, $\hat{\mathbf{c}} = \mathbf{y} \oplus \mathbf{e}_j$=로 하고 종료한다.
   iv) 만약 $j \in S$이면 다음 단계로 진행하고, 그렇지 않으면 j를 다음 값으로 한 후 단계 i)로 간다.
   v) $q = \max\{W_H(\mathbf{e}_j), \lfloor d/2 \rfloor\} + 1$로 하고 $\mathbf{v}_q^*$를 형성시킨다. $\mathbf{v}_q^*$를 경판정 복호하여 $\mathbf{v}$를 얻는다. 만약 $\mathbf{v}_q^*$의 경판정 복호가 불가능하면, $\mathbf{v}_q^*$를 버리고 j를 다음 값으로 한 후 단계 i)로 간다.
   vi) $\mathbf{e}_j' = \mathbf{e}_j \oplus \mathbf{v}$로 한다. 만약 $W_H(\mathbf{e}_j') < d$이고 $W_a(\mathbf{e}_j') \le W_a(\mathbf{e}_j' \oplus \mathbf{w}_d^*)$이면, $\hat{\mathbf{c}} = \mathbf{y} \oplus \mathbf{e}_j'$으로 하고 종료한다.
4) 탐색된 에러 패턴들($\mathbf{e}_1$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

본 논문에서는 (23, 12) Golay 부호를 대상으로 컴퓨터 시뮬레이션을 수행하였다. (23, 12) Golay 부호는 선형 부호이고 순회 부호이며, 특히 완전 부호(perfect code)의 성질을 만족하고 있다. 따라서 부호화 및 복호화가 편리하고, 에러 정정 능력이 우수하기 때문에 일반적으로 널리 사용되고 있다. 이러한 이유로 본 논문에서는 (23, 12) Golay 부호를 실험 대상으로 채택하였다.

통신 채널에서 여러 가지 다양한 원인으로 발생한 교란 요소들이 중첩되어 있는 잡음은 중앙 극한 정리(central limit theorem)에 의하여 가우시안 확률 밀도를 갖는 확률 변수가 된다. 따라서 가산성 백색 가우시안 잡음(additive white Gaussian noise, AWGN) 채널은 통신 채널의 가장 일반적인 형태로 받아들여지고 있다. 본 논문에서도 가산성 백색 가우시안 잡음 채널 환경에서 시뮬레이션을 수행하였다. 본 논문에서 사용하는 변조 방식은 BPSK로 선정하였다. BPSK 방식은 2진 반극성 신호를 전송하며, 2진 디지탈 통신 시스템에서 보편적으로 사용되는 변조 방식이다.

후보 부호어의 탐색 범위를 정하기 위하여 집합 T와 S의 여러 가지 경우에 대하여 시뮬레이션을 수행하였으며, 그 중에서 2가지 경우를 선택하였다. T와 S가 모두 {4, 5, …, 19}인 경우를 case 1이라 한다. case 1은 가장 낮은 블록 에러 확률을 갖는다. 복호의 복잡도는 경판정 복호의 회수로 결정되는데, 경판정 복호의 최대 회수는 $1 + |T| + |S|$이며, 시스템에 따라서는 이것이 제한을 받을 수도 있다. 이러한 이유로 최대 8회의 경판정 복호 회수를 갖는 경우 중에서 블록 에러 확률이 가장 낮은 경우를 선택하여 case 2라 한다. case 2에서는 T가 {4, 5, 8, 9}이고, S가 {4, 5, 8}이다.

복호 과정의 복잡도와 복호 수행에 소요되는 시간은 여러 가지 요인에 의하여 결정된다. 그런데 이 요인들 중 현저하게 복잡도가 높으며 많은 시간이 소요되는 것은 경판정 복호 과정이므로, 복호의 복잡도는 경판정 복호 회수와

같다고 볼 수 있다[4].

(23, 12) Golay 부호에 대하여 한 번의 연판정 복호과정 내에서 수행해야할 경판정 복호 회수를 수학적으로 정확하게 해석하려면 수신 신호 벡터 $\mathbf{r}=(r_1, r_2, \cdots, r_{23})$에 포함된 23개의 확률 변수로 이루어진 함수를 다루어야 한다. 물론, 이 23개 확률 변수들의 조합에 따라 경판정 복호 과정과 회수는 다양하게 변화한다. 이러한 이유로 경판정 복호 회수의 정확한 수학적 표현은 매우 곤란하다. 따라서 본 논문에서는 컴퓨터 시뮬레이션을 통하여 경판정 복호 회수를 산출하였다. 즉, 대단히 많은 갯수의 수신 신호 벡터들에 대한 연판정 복호 과정을 직접 수행하고, 그 과정에서 소요된 경판정 복호 회수들을 통계적으로 처리하였다. 이러한 방법으로 한 번의 연판정 복호에 수반되는 경판정 복호 회수의 평균값과 표준편차를 얻을 수 있었다. $E_b/N_0=5.0$dB에서 제안된 알고리즘(case 1)에 대한 블록 에러 확률과 경판정 복호 회수를 <표 1>에 나타내었다. 정규화된 임계값 Φ를 $\Phi/\sqrt{E_s}$로 정의한다. $\Phi=1.5$일 때의 블록 에러 확률은 $\Phi=\infty$일 때와 거의 같지만, 경판정 복호 회수의 평균과 표준편차의 측면에서 유리함을 알 수 있다. (그림 1)은 제안된 알고리즘(case 1)에서 여러 가지 Φ값을 파라미터로 하여 E_b/N_0에 따른 평균 경판정 복호 회수를 나타낸 것이다. E_b/N_0가 충분히 클 때, 경판정 복호 회수의 평균은 1에 접근함을 알 수 있다. case 2의 결과도 같은 경향을 보이므로 제시하지 않았다.

블록 부호에 대한 기존의 연판정 복호 알고리즘 중에서는 Chase의 알고리즘 2와 Tokushige 등의 알고리즘이 가장 잘 알려져 있고, 본 논문에서 제안된 방법과의 관련이 깊다. 이 알고리즘들을 제안된 알고리즘과 함께 시뮬레이션을 수행하여 그 결과를 비교한다. <표 2>는 $E_b/N_0=5.0$dB에서 제안된 알고리즘과 Chase 알고리즘 2, Tokushige등의 알고리즘을 비교한 것이다. 제안된 알고리즘이 다른 알고리즘들에 비하여 에러 확률 저하와 복잡도 감소를 실현하였음을 확인할 수 있다.

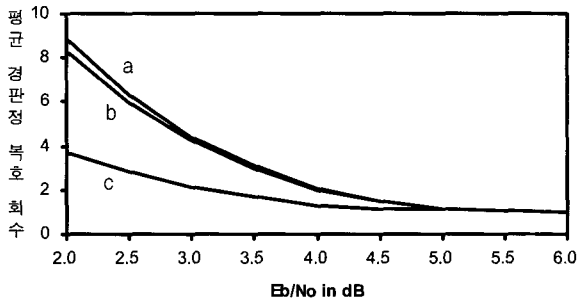
여러 가지 알고리즘들의 평균 경판정 복호 회수를 비교하여 (그림 2)에 나타내었다. 제안된 알고리즘의 case 1과 case 2는 $\Phi=1.5$일 때의 결과이다. 제안된 알고리즘이 다른 알고리즘들에 비하여 평균 경판정 복호 회수가 현저히 감소되는 것을 알 수 있다. E_b/N_0에 따른 블록 에러 확률을 비교하여 (그림 3)에 나타내었다. 제안된 알고리즘이 Chase 알고리즘 2이나 Tokushige등의 알고리즘보다 낮은 블록 에러 확률을 갖는다. 제안된 알고리즘의 case 1과 case 2을 비교하면 (그림 2)에서 복호의 복잡도 면에서는 case 2가 우수하고, (그림 3)에서 블록 에러 확률은 case 1이 우수함을 알 수 있다.

Chase 알고리즘 2는 수신된 신호 중 신뢰도 값이 가장 작은 3개의 비트를 선택한다. 선택한 비트들을 가능한 모든 경우로 조합하여 반전시킨다. 이렇게 반전된 각각의 결과를 경판정 복호하여 후보 부호어들을 얻는다. 따라서 Chase 알고리즘 2는 2^3인 8번의 경판정 복호를 수행해야 한다.

Tokushige 등은 경판정 복호 회수를 감소시키기 위하여 후보 부호어 탐색 영역을 제한하는 방법을 연구하였다. 이 방법은 전송 채널의 신호대잡음비에 따라 탐색 영역의 범위를 변화시켜야 하며, 신호대잡음비를 추정하여 찾아내야 하는 단점을 갖는다. 탐색 영역을 제한하였으므로 Chase

<표 1> $E_b/N_0=5.0$dB에서 제안된 알고리즘(case 1)의 블록 에러 확률과 경판정 복호 회수

정규화된 임계값 Φ	블록에러 확률	경판정복호회수	
		평 균	표준편차
0.5	2.46×10^{-4}	1.0790	0.9659
1.0	2.30×10^{-4}	1.1533	1.8734
1.5	2.28×10^{-4}	1.2077	2.5202
2.0	2.28×10^{-4}	1.2116	2.5655
∞	2.28×10^{-4}	1.2116	2.5656

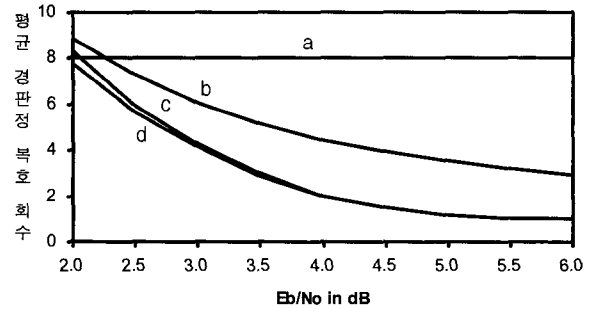


a $\Phi=\infty$, b $\Phi=1.5$, c $\Phi=0.5$

(그림 1) 제안된 알고리즘(case 1)의 평균 경판정 복호 회수

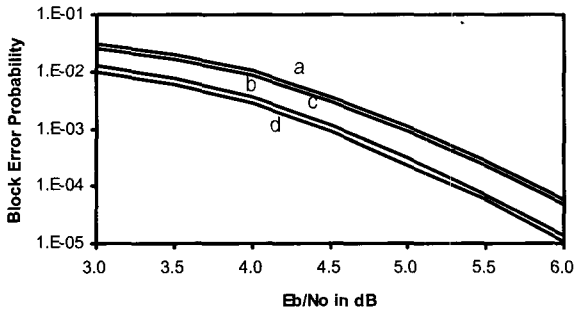
<표 2> $E_b/N_0=5.0$dB에서 제안된 알고리즘, Chase 알고리즘 2, Tokushige등의 알고리즘의 성능 비교

연판정복호법	블록에러 확률	평균경판정 복호회수
제안된 알고리즘(case 1, Φ=1.5)	2.28×10^{-4}	1.2077
제안된 알고리즘(case 2, Φ=1.5)	3.24×10^{-4}	1.1846
Chase 알고리즘 2	9.33×10^{-4}	8.0000
Tokushige등의 알고리즘	1.12×10^{-3}	3.5549



a. Chase 알고리즘 2, b. Tokushige등의 알고리즘
c. 제안된 알고리즘(case 1, Φ=1.5), d. 제안된 알고리즘(case 2, Φ=1.5)

(그림 2) 제안된 알고리즘, Chase 알고리즘 2, Tokushige등의 알고리즘의 평균 경판정 복호 회수 비교



a. Tokushige등의 알고리즘, b. Chase 알고리즘 2
c. 제안된 알고리즘(case 2, Φ=1.5), d. 제안된 알고리즘(case 1, Φ=1.5)

(그림 3) 제안된 알고리즘, Chase 알고리즘 2, Tokushige등의 알고리즘의 블록 에러 확률 비교

알고리즘 2보다는 평균 경판정 복호 회수를 감소시킬 수 있으나, 탐색 영역 내에서 가능한 모든 경우의 조합으로 수신 신호 벡터를 변형시키는 단순한 방법을 사용하기 때문에 본 논문에서 제안하는 알고리즘에 비하여 복잡도와 에러 확률이 높은 결과를 보인다.

본 논문에서는 최초의 경판정 복호로 얻어진 부호어에 대한 에러들의 위치와 신뢰도 값이 작은 비트들의 위치를 비교하여 수신 신호 벡터로부터 최소 거리에 존재하는 부호어가 후보 부호어로 선정될 확률을 높일 수 있는 방법을 연구하였다. 본 논문에서 제안된 알고리즘이 Chase 알고리즘 2나 Tokushige 등의 알고리즘에 비하여 에러 확률이 낮고 복잡도가 감소된 우수한 성능을 보이는 이유는 두 가지가 있다. 첫 번째는 신뢰도가 낮은 비트들을 에러 패턴에 포함시키게 하는 후보 부호어를 탐색하였기 때문이다. 이렇게 하면 올바른 복호 결과가 얻어질 가능성을 효과적으로 향상시킬 수 있으며, 탐색해야 할 후보 부호어의 수를 줄일 수 있다. 두 번째는 이미 탐색된 후보 부호어가 중복하여 다시 선정되는 경우를 방지하였기 때문이다. 하나의 새로운 후보 부호어를 선정할 때마다 한 번의 경판정 복호 과정이 소요된다. 이렇게 경판정 복호과정을 거치면서 찾아낸 후보 부호어가 이미 탐색되어 알고 있는 후보 부호어와 동일한 것이라면 그 과정은 의미가 없어진다. 이상의 두 가지 이유로 본 논문에서 제안된 알고리즘은 에러 확률 저하와 복잡도 감소를 실현할 수 있다.

4. 결 론

선형 블록 부호에 대한 연판정 복호법을 제안하였다. 후보 부호어들을 효율적으로 찾아낼 수 있는 방법을 연구하였고, 이를 통하여 복호의 복잡도를 줄이면서 블록 에러 확률을 낮출 수 있었다. 본 논문에서 제안된 알고리즘은 신뢰도가 낮은 비트들을 에러 패턴에 포함시키게 하는 후보 부호어를 찾아내고, 이미 탐색된 후보 부호어가 중복하여 다시 선정되는 경우를 방지하여 에러 확률 저하와 복잡도 감소를 실현할 수 있다. 제안된 복호법을 실행하는데 필요한 경판정 복호의 평균 회수는 1에 접근하며, 낮은 블록 에러 확률을 얻을 수 있음을 확인하였다.

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

참 고 문 헌

[1] G. C. Clark, Jr. and J. B. Cain, *Error-Correction Coding for Digital Communications*, Plenum Press, New York, 1981.

[2] S. Lin and D. J. Costello, Jr., *Error Control Coding*, Prentice-Hall, Englewood Cliffs, N. J., 1983.

[3] G. D. Forney, Jr., *Concatenated codes*, MIT Press, Cambridge, Mass., 1966.

[4] 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.

[5] C. M. Hacket, "An efficient algorithm for decoding of the (23,12) extended Golay code," *IEEE Trans. Commun.*, vol. COM-29, pp.909-911, June, 1981.

[6] N. N. Tendolkar and C. R. P. Hartmann, "Generalization of Chase algorithms for soft-decision decoding of binary linear codes," *IEEE Trans. Inform. Theory*, Vol.IT-30, pp.714-721, Sept., 1984.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

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 전자·컴퓨터학부 교수

관심분야 : 통신공학, 부호이론, 정보이론