論文93-30A-7-2

軟判定에 의한 線形 블록 符號의 최소 거리 復號法

(Minimum-Distance Decoding of Linear Block Codes with Soft-Decision)

沈 龍 杰*, 李 忠 雄**

(Yong Geol Shim and Choong Woong Lee)

要 約

本 論文에서는 블럭 符號에 대한 軟判定 復號 방법을 提案하였다. 최초의 硬判定 復號 결과를 면밀히 관찰하여 후보 符號語들을 효율적으로 탐색할 수 있는 방법을 개발하였다. 이로 인하여, 復號의 複雜度(硬判定 復號 回數)를 줄이면서도 블럭 에러 確率을 낮출 수 있다. (23,12) Golay 符號에 대한 컴퓨터 시뮬레이션 결과를 제시하였다. 復號의 複雜度가 대단히 감소되었으면서도, 블럭 에러 確率은 最尤 復號法과 거의 동일한 결과를 얻을 수 있었다.

Abstract

We have proposed a soft-decision decoding method for block codes. With careful examinations of the first hard-decision decoded results, the candidate codewords are efficiently searched for. Thus, we can reduce the decoding complexity (the number of hard-decision decodings) and lower the block error probability. Computer simulation results are presented for the (23,12) Golay code. They show that the decoding complexity is considerably reduced and the block error probability is close to that of the maximum likelihood decoder.

Ⅰ. 서론

디지탈 통신 시스템에서 통신로 측정 정보(軟判定 정보)를 이용하여 線形 블럭 符號를 復號하는 軟判定 復號法의 연구가 활발히 전개되고 있다. 軟判定 復號를 위해서는 硬判定 復號를 행하는 부분 외에도 軟判定 정보를 추출하고 처리하는 부분이 추가되어야 하므로 하드웨어의 규모가 증가한다. 그러나 추정된 경판정 값의 정확성에 관한 정보를 복호 과정에 이용하므로 성능을 향상시킬 수 있다. 블럭 符號의 軟判定 復號 방법은 크게 두가지 부류로 나누어진다. 그 중 하나는 수신 계열로부터 최소 거리에 있는 符號語를 선택하여 블럭 에러를 최소로 하는 방법이다.[1-7] 다른 하나의 방법은 한 符號語 내의 각 심볼을 平均 심볼 에러 確率이 최소가 되도록 復號하는 것으로, 復號된 계열은 符號語가 되지 않을 수도 있다.[8-10] 本 論文에서는 블럭 에러 確率을 최소로 하는 復號法을 연구한다.

블럭 符號에 대하여 블럭 에러 確率을 최소로 하는

*正會員, 檀國大學校 電子工學科
(Dept. of Elec. Eng., Dankook Univ)
**正會員, 서울大學校 金屬工學科
(Dept. of Metallurgical Eng., Seoul Nat'l Univ.)
接受日字: 1992年 3月 3日

最尤 復號法(maximum likelihood decoding)은 가능한 모든 符號語들을 전부 탐색하는 방법이다. 따라서, 이 방법은 符號語의 수가 적은 符號 외에는 사용할 수 없다. 즉, 符號化率이 낮으면서 符號의 길이가 짧은 符號에 대해서만 사용이 가능하다. 이러한 이유로, 약간의 성능 열화를 감수하면서, 復號의 複雜度를 감소시킬 수 있는 방법이 필요하다.

復號의 複雜度를 줄이기 위하여 몇개의 후보 符號語를 원소로 갖는 집합을 구성한다. 물론, 수신 계열로부터 최소 거리에 존재하는 符號語가 이 집합에 들어있을 確率이 높아지도록 해야한다. 각각의 후보 符號語까지의 거리를 계산하여 가장 가까운 符號語를 復號 결과로 선택한다. 이러한 생각을 기초로 하여 여러 가지 軟判定 復號法들이 연구되어왔다.[1-7] 대부분의 방법들은 수신 계열을 硬判定 復號하여 얻어진 符號語를 첫번째 후보 符號語로 하며, 다른 符號語들도 역시 硬判定 復號 과정을 반복 수행하여 얻는다. 이 때 소요되는 硬判定 復號의 回數가 軟判定 復號 알고리듬의 複雜度를 결정한다.

本 論文에서는, 최초의 硬判定 復號로 얻어진 符號語에 대한 에러들의 위치와 의심스러운 비트들의 위치를 비교하여, 다른 후보 符號語들을 효율적으로 찾아낼 수 있는 방법을 연구한다. 특히 참고문헌 [7] 의 방법을 더욱 개선하여 最尤 復號法과 거의 동일한 블럭 에러 確率을 얻고자 한다.

Ⅱ. 軟判定 復號法

1. 통신 시스템의 모형

符號 C는 (n,k) 2元 線形 블럭 符號이며, 최소 Hamming 거리는 d이다. 符號化率은 R=k/n이다. C의 符號語를 $c=(c_1,c_2,\cdots,c_n)$으로 표시하며, $c_i \in GF(2)$ 이다.

符號 심볼 c_i는 反極性(antipodal) 信號 $s_i=\sqrt{E_s}(1-2c_i)$로 변환된다. 여기서 E_s는 심볼당 平均 에너지이다. 이 때, 정보 비트당 에너지는 $E_b=E_s/R$ 이다. 信號 벡터 $s=(s_1,s_2,\cdots,s_n)$은 무기억 통신로(memoryless channel)를 통하여 전송되며, 雜音이 부가되어 $r=(r_1,r_2,\cdots,r_n)$으로 수신된다. 심볼 r_i는 수신기의 정합 필터 출력 전압이며 $r_i=s_i+z_i$ 이다. 여기서 $z_1,z_2,\cdots,z_n$는 모두 相互 獨立이며 平均이 0이고 分散이 $N_0/2$인 相加的 白色 가우시안 不規則 變數이다. N_0는 片側 雜音 電力 密度이다. 수신측의 판정기에서는 r을 수신하여 2개의 출력을 발생시킨다. 그 중 하나가 硬判定 $y=(y_1,y_2,\cdots,y_n)$이며, $r_i \geq 0$ 이면 $y_i=0$ 으로, $r_i < 0$ 이면 $y_i=1$ 로 한다. 다른 하나는 信賴度 벡터 $a=(a_1,a_2,\cdots,a_n)$ 이며, $a_i=|r_i|$ 이다.

軟判定 복호기는 y와 a를 이용하여 전송된 符號語를 추정한다. 추정된 符號語를 c^o로 표시한다. 最尤 복호기는 수신 벡터 r과의 거리가 가장 가까운 符號語 c^o를 추정한다. 추정된 符號語 c^o에 대한 에러 패턴은 $e = y \oplus c^o$ 로 주어진다. 여기서 ⊕는 2진 덧셈을 나타낸다. 에러 패턴 $e=(e_1,e_2,\cdots,e_n)$의 아날로그 重(weight)은

$$W_a(e)=\sum_{i=1}^{n} a_i e_i$$

로 정의한다. $W_a(e)=W_a(y \oplus c^o)$ 가 최소로 되는 c^o를 찾아내면 最尤 復號 결과가 된다.

2. 軟判定 復號法의 提案

符號語 c^o를 추정하기 위하여 몇 개의 후보 符號語를 찾는다. 최초의 후보 符號語는 y를 硬判定 復號한 c_1이다. 完全 符號(perfect code)가 아닌 경우에는 訂正 불능인 에러가 檢出되는 수도 있다. 이 때는 Wagner rule [11] 에 의하여 y의 비트들 중 가장 信賴度가 낮은 것을 반전(complement)시키고 다시 硬判定 復號를 수행하여 c_1을 얻는다. 만약 그래도 訂正 불능인 에러가 檢出되면, 에러의 檢出만으로 復號를 마친다.

c_1이 얻어지면 이에 따른 에러 패턴은 $e_1 = y \oplus c_1 = (e_{11},e_{12},\cdots,e_{1n})$ 이다. 만약 $e_1=0$ (0은 영벡터)이면, $W_a(e_1)=0$ 이며, 이것이 최소 아날로그 重이 된다. 따라서 最尤 復號 결과는 c_1이다. 이 경우에는 $c^o=c_1$으로 하고 復號를 종료한다.

만약 $e_1 \neq 0$이면, 다른 후보 符號語들을 찾는다. 후보 符號語 중 하나를 c_j로 표시하자. C는 線形 符號이므로 c_j를 $c_1 \oplus u_j$ 로 표시할 수 있으며, $u_j=(u_{j1},u_{j2},\cdots,u_{jn})$은 또하나의 符號語이다. 물론, $c_j \neq c_1$이며, $u_j \neq 0$이다. c_j에 대한 에러 패턴은 $e_j = y \oplus c_j = y \oplus c_1 \oplus u_j = e_1 \oplus u_j$ 이다. 결국, 아날로그 重

$$W_a(e_j)=W_a(e_1 \oplus u_j)=\sum_{i=1}^{n} a_i(e_{1i} \oplus u_{ji}) \qquad (1)$$

를 최소로 하는 符號語 u_j를 찾아야 한다. 식 (1)을 최소로 하려면 e_{1i}가 0일때 u_{ji}도 0이 되고 e_{1i}가 1일 때 u_{ji}도 1이 되면 좋을 것이다. 그러나, $W_H(e_1) \leq d/2$이고 $W_H(u_j) \geq d$ ($W_a(\cdot)$는 Hamming 重을 나타낸다) 이므로 모든 심볼이 다 그렇게 될 수는 없다. u_j를 찾기에 앞서서 먼저 2元 벡터 $u_j^*=(u_{j1}^*,u_{j2}^*,\cdots,u_{jn}^*)$를 생각하자. u_j^*의 Hamming 重 $W_H(u_j^*)$는 j (j > $W_H(e_j)$)이다. u_j^*의 원소가 1

이 되는 곳은 e_{1i}=1인 $W_H(e_1)$개의 위치와 e_{1i}=0이면서 信賴度가 가장 작은 [j-$W_H(e_1)$] 개의 위치이다. 물론, u_j^*는 符號語가 아닐 수도 있으므로 나중에 u_j^*를 硬判定 復號하여 符號語 uj를 얻는다.

Hamming 重이 j인 모든 n차원 2元 벡터 중에서 u_j^*가 에러 패턴의 아날로그 重을 최소가 되게 한다. 이것을 定理 1에서 설명한다.

定理 1 : Hamming 重이 j이며 u_j^*가 아닌 임의의 n차원 2元 벡터를 b_j라 하면, 아날로그 重 $W_a(e_1 \oplus u_j^*)$는 $W_a(e_1 \oplus b_j)$보다 작거나 같다.

證明 : 信賴度 벡터 $a=(a_1, a_2, \cdots, a_n)$의 원소들을 다음과 같이 3가지 집합으로 분류한다.

$A_1=\{a_i \mid e_{1i}=1$이고 $u_j^*=1\}=\{\alpha(1), \alpha(2), \cdots, \alpha(L)\}$

$A_2=\{a_i \mid e_{1i}=0$이고 $u_j^*=1\}=$
$\{\beta(1), \beta(2), \cdots, \beta(j-L)\}$

$A_3=\{a_i \mid e_{1i}=0$이고 $u_j^*=0\}=$
$\{\gamma(1), \gamma(2), \cdots, \gamma(n-j)\}$

여기서 $W_H(e_1)$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. u_j^*는 e_{1i}=0이면서 信賴度가 가장 작은 (j-L)개의 위치에 1을 갖기 때문에 A_2의 가장 큰 원소라도 A_3의 가장 작은 원소보다 클 수 없다. 즉,

$$\beta(1) \le \beta(2) \le \cdots \le \beta(j-L) \le \gamma(1) \le \gamma \qquad (2)$$

이다. $e_1 \oplus u_j^*$의 아날로그 重은

$$W_a(e_1 \oplus u_j^*) = \sum_{i=1}^{n} a_i(e_{1i} \oplus u_j i^*) = \sum_{N=1}^{j-L} \beta(N)$$

이다.

n차원 2元 벡터 b_j와 u_j^*가 서로 다른 위치의 수를 e_{1i}=1인 곳에서 f개, e_{1i}=0이고 u_j^*=1인 곳에서 g개로 가정하면, $W_H(b_j)=W_H(u_j^*)$이므로 e_{1i}=0이고 u_j^*=0인 곳에서는 (f+g)개의 위치에서 서로 다르다. 결국, b_j와 u_j^*는 총 2(f+g)개의 위치에서 서로 다르다. e_{1i}=1인 f개의 相異한 위치에 해당하는 信賴度 값들을 $\alpha(m_1)$, $\alpha(m_2), \cdots, \alpha(m_f)$로 표시하자. 같은 방법으로, e_{1i}=0이고 u2*=1인 g개의 相異한 위치의 信賴度 값들을 $\beta(h_1)$, $\beta(h_2), \cdots, \beta(h_g)$로, e_{1i}=0이고 u_j^*=0인 (f+g)개의 相異한 위치의 信賴度 값들을 $\gamma(p_1)$, $\gamma(p_2), \cdots, \gamma(p_{f+g})$로 표시하자. 그러면,

$$\begin{aligned} & W_a(e_1 \oplus b_j) - W_a(e_1 \oplus u_j^*) \\ &= \left[\alpha(m_1)+\alpha(m_2)+\cdots+\alpha(m_f)\right] + \left[\gamma(p_1)+\gamma(p_2)+\cdots+\gamma(p_{f+g})\right] \\ &\quad - \left[\beta(h_1)+\beta(h_2)+\cdots+\beta(h_g)\right] \end{aligned}$$

가 된다. 信賴度 값들은 음이 아니므로 [$\alpha(m_1)+\alpha(m_2)+\cdots+\alpha(m_f)$] 는 음이 아니다. 또한, (2)식으로부터 [$\gamma(p_1)+\gamma(p_2)+\cdots+\gamma(p_{f+g})$] - [$\beta(h_1)+\beta(h_2)+\cdots+\beta(h_g)$] 도 음이 아니다. 이것은 $W_a(e_1 u_j^*) \le W_a(e_1 \oplus b_j)$ 임을 의미하며, 이것으로 定理 1이 證明되었다.

이제 u_d^*를 생각한다.(u_d^*의 Hamming 重은 符號의 최소 Hamming 거리 d이다.) 어떠한 에러 패턴의 아날로그 重 $W_a(e_j)=W_a(e_1 \oplus u_j)$도 $W_a(e_1 \oplus u_d^*)$보다 작을 수 없다. 이것을 定理 2에서 설명한다.

定理 2 : 0이 아닌 임의의 符號語를 x라 하면, 아날로그 重 $W_a(e_1 \oplus u_d^*)$는 $W_a(e_1 \oplus x)$보다 작거나 같다.

證明 : $W_H(x)$를 j라 하자. (x는 符號語이므로 $j \ge d$이다.) 그러면, 定理 1에 의하여 $W_a(e_1 \oplus u_j^*) \le W_a(e_1 \oplus x)$이다. u_d^*와 u_j^*의 원소가 공통으로 1이 되는 곳은 e_{1i}=1인 $W_H(e_1)$개의 위치와 e_{1i}=0이면서 信賴度가 가장 작은 [d-$W_H(e_1)$] 개의 위치이다. u_j^*는 이외에도 e_{1i}=0이면서 信賴度가 다음으로 작은 (j-d)개의 위치에 1을 갖는다. 따라서 $W_a(e_1 \oplus u_j^*)$-$W_a(e_1 \oplus u_d^*)$는 (j-d)개의 信賴度 값들의 합이 되며, 이것은 음이 아니다. 그러므로 $W_a(e_1 \oplus u_d^*) \le W_a(e_1 \oplus u_j^*)$ 이다. 결국, $W_a(e_1 \oplus u_j^*) \le W_a(e_1 \oplus x)$이며, 이것으로 定理 2가 證明되었다.

定理 2로부터, 만약 $W_a(e_1) \le W_a(e_1 \oplus u_d^*)$ 이면, $W_a(e_1)$이 에러 패턴의 최소 아날로그 重이 되어 最尤 復號 결과는 c_1임을 알 수 있다. 이 경우에는 $c^o=c_1$으로 하고 復號를 종료한다. 이에 따라 復號의 複雜度는 줄어든다.

만약 $W_a(e_1) > W_a(e_1 \oplus u_d^*)$ 이면, c_1 근처의 후보 符號語들을 찾는다. 앞에서 언급했듯이 u_j^*를 형성시키고 u_j^*를 硬判定 復號하여 u_j를 얻는다. 이 과정을 상세히 설명한다.

u_j^*의 Hamming 重들을 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 u_j^*를 형성시킨다. 3절에서 T의 원소들의 범위를 설명한다.

復號의 複雜度를 감소시키기 위하여, 임계값 Φ를 설정하여 信賴度 값 a_i와 비교한다. $e_{1i} \oplus u_j^*$=1인 [j-$W_H(e_1)$] 개의 위치에 해당하는 信賴度 값들이 모두 Φ보다 작거나 같은 경우에만 u_j^*를 형성시킨다. (만약 임계값을 사용하지 않으려면 $\Phi = \infty$로 한다.)

u_j^*는 符號語가 아닐 수도 있기 때문에, u_j^*를 硬判定 復號하여 u_j를 얻는다. u_j는 u_j^*로부터 가장 가까운 符號語이다. 어떤 j 값에 대해서는, u_j^*의 硬判定 復號가 불가능하여 u_j를 얻을 수 없는 경우도 있다. 이러한 경우에는 현재의 j 값을 포기하고 다음 j 값으로 넘어간다. 각각의 u_j에 대한 후보 符號語는 $c_j = c_1 \oplus u_j$ 이고, c_j에 대한 에러 패턴은 $e_j = e_1 \oplus u_j$ 이다.

c_1 근처의 후보 符號語 c_j를 찾은 것과 비슷한 방법으로 c_j 근처의 후보 符號語 c_j'를 찾을 수 있다. u_j^*를 생각한 것과 같은 이유로 2元 n차원 벡터 v_q^*를 생각한다. v_q^*의 Hamming 重 $W_H(v_q^*)$는 $q\ (q \rangle W_H(e_j)\ )$이다. v_q^*의 원소가 1이 되는 곳은 $e_{ji}=1$인 $W_H(ej)$개의 위치와 $e_{ji}=0$이면서 信賴度가 가장 작은 $[q-WH(e_j)]$ 개의 위치이다.

u_d^*를 이용했던 것과 동일한 방법으로 v_d^*를 이용한다. 만약 $W_H(e_j) \langle d$이고 $W_a(e_j) \le W_a(e_j \oplus v_d^*)$이면 $W_a(e_j)$가 에러 패턴의 최소 아날로그 重이 되어 最尤 復號 결과는 c_j이다. 이 경우에는 $c^o=c_j$로 하고 復號를 종료한다. 이에 따라 復號의 複雜度는 줄어든다.

만약 $W_a(e_j) \rangle W_a(e_j \oplus v_d^*)$이면 c_j 근처의 符號語 c_j'를 찾는다. 그러나, 復號 複雜度의 간소화를 위하여 c_j' 찾기를 제한하는 집합 S를 도입한다. S는 T의 부분집합이며, $j \in S$일 때에만 c_j'를 찾는다. c_j'를 찾는 방법은 다음과 같다. $q = \max\{ W_H(e_j), [d/2] \}+1$ 로 하고, 2元 n차원 벡터 v_q^*를 형성시킨다. ($[x]$ 는 x의 정수 부분을 표시한다.) v_q^*를 硬判定 復號하여 符號語 v_q를 얻는다. (이것이 불가능하면 v_q 얻기를 포기한다.) 후보 符號語 c_j'는 $c_j \oplus v_q$이며 c_j'에 대한 에러 패턴은 $e_j' = e_j \oplus v_q$ 이다. 만약 $W_H(e_j') \langle d$ 이면, u_d^*나 v_d^*를 생각했던 것과 같은 방법으로 2元 n차원 벡터 w_d^*를 생각한다. w_d^*의 원소가 1이 되는 곳은 $e_{ji}'=1$인 $W_H(e_j')$개의 위치와 $e_{ji}'=0$이면서 信賴度가 가장 작은 $[d-W_H(e_j')]$ 개의 위치이다. 만약 $W_a(ej') \le W_a(e_j' \oplus w_d^*)$이면 $W_a(e_j')$가 에러 패턴의 최소 아날로그 重이 되어 最尤 復號 결과는 c_j'이다. 이 경우에는 $c^o=c_j$ 로 하고 復號를 종료한다.

후보 符號語들(c_1과 여러가지 c_j, c_j') 중에서 에러 패턴의 아날로그 重을 최소로 하는 것을 c^o로 선택한다.

3. 집합 T의 원소들의 범위

집합 T의 원소가 (d-1)/2 보다 작거나 같은 것은 의미가 없다. 만약 $j \le (d-1)/2$ 이면, u_j^*는 0으로 硬判定 復號되는데, 이것은 u_j가 될 수 없다. 따라서 T는 { (d-1)/2 +1, (d-1)/2 +2, ,n }의 부분집합이다.

더구나, 원소가 모두 1인 n차원 벡터 (1, 1, ,1)이 符號語이고 $k \rangle$ (d-1)/2 인 경우에는 T가 { (d-1)/2 +1, (d-1)/2 +2, ,n- (d-1)/2 -1 }의 부분집합인 것으로도 충분하다. 만약 $j \ge n-$ (d-1)/2 이면, u_j는 원소가 모두 1인 符號語로 硬判定 復號된다. 즉, $u_F=(1, 1, \cdots, 1)$이고 $W_H(u_j)=n$이 된다. $W_H(e_1) \le (d-1)/2$ 이고 $k \rangle$ (d-1)/2 이므로 $W_H(e_j) = W_H(e_1 \oplus u_j) = n-W_H(e_1) \ge n-$ (d-1)/2 $\rangle$ n-k 이다. 이제, Hamming 重이 (n-k)보다 큰 에러 패턴은 고려할 필요가 없음을 설명한다. 檢査 行列(parity check matrix) H는 (n-k) x n 행렬이다. H의 線形 獨立인 열의 수는 (n-k)를 넘지 않는다. 따라서, $W_H(e_j)$가 (n-k)보다 크면, 적어도 하나의 符號語 $c'' = (c_1'', c_2'', \cdots, c_n'')$가 존재하여 $\{i \mid c_i'' = 1\}$이 $\{i \mid e_{ji}=1\}$의 부분집합이 된다. e_j를 $c'' \oplus e''$로 표시하면 $W_a(e_j) = W_a(c'')+W_a(e'')$가 된다. $e'' = e_j \oplus c''$이므로 e''는 또하나의 에러 패턴이다. (e''에 지정된 符號語는 $y \oplus e'' = y \oplus ej \oplus c'' = y \oplus e_1 \oplus u_j \oplus c'' = c_1 \oplus u_j \oplus c''$이다.) $W_a(e_j)$는 $W_a(e'')$보다 작을 수가 없으므로, 最尤 復號의 관점에서 e_j는 고려할 필요가 없다.

4. 알고리듬의 요약

提案된 軟判定 復號 알고리듬을 요약한다. 알고리듬을 시작하기 전에, 집합 T와 그 부분집합 S, 그리고 임계값 Φ가 결정되어야 한다. 復號 결과는 c^o이다.

1) y를 硬判定 復號하여 c_1과 e_1을 얻는다. 만약 y의 硬判定 復號가 불가능하면, y의 비트들 중 가장 信賴度가 낮은 것을 반전시키고 다시 硬判定 復號를 수행한다. 만약 그래도 불가능하면 종료한다.

2) 만약 $e_1=0$이거나 $W_a(e_1) \le W_a(e_1 \oplus u_d^*)$이면, $c^o=c_1$으로 하고 종료한다.

3) 변수 j를 t_1에서 $t^{|T|}$까지 증가시키며 각각의 j에 대하여 단계 i)에서 vi)까지 수행한다.

i) 임계값 비교에 의하여 u_j^*를 형성시킬 필요가 없으면 바로 단계 4)로 간다.

ii) u_j^*를 형성시킨다. u_j^*를 硬判定 復號하여 u_j를 얻는다. 만약 u_j^*의 硬判定 復號가 불가능하면, u_j^*를 버리고 j를 다음 값으로 한 후 단계 i)로 간다.

iii) $e_j = e_1 \oplus u_j$로 한다. 만약 $W_H(e_j) \langle d$ 이고 $W_a(e_j) \le W_a(e_j \oplus v_d^*)$이면, $c^o = y \oplus e_j$로 하고 종료한다.

iv) 만약 $j \in S$이면 다음 단계로 진행하고, 그렇지 않으면 j를 다음 값으로 한 후 단계 i)로 간다.

v) $q = \max\{ W_H(e_j), d/2 \}+1$로 하고 v_q^*를 형성시킨다. v_q^*를 硬判定 復號하여 v_q를 얻는다. 만약 v_q^*의 硬判定 復號가 불가능하면, v_q^*를 버리고

j를 다음 값으로 한 후 단계 i)로 간다.

vi) $e_j' = e_j \oplus v_q$ 로 한다. 만약 $W_H(e_j') < d$ 이고 $W_a(e_j') \; W_a(e_j' \oplus w_d^*)$이면, $c^o = y \oplus e_j$ 로 하고 종료한다.

4) 탐색된 에러 패턴들(e_1과 여러가지 e_j, e_j') 중에서 아날로그 重이 가장 작은 것을 e^o 로 선택한다. $c^o = y \oplus e^o$로 하고 종료한다.

Ⅲ. 시뮬레이션 결과

完全 符號로 널리 알려진 (23,12) Golay 符號를 사용하여, 相加的 白色 가우시안 雜音 채널을 통한 2元 反極性 信號에 대하여 컴퓨터 시뮬레이션을 수행하였다. (23,12) Golay 符號는 최소 Hamming 거리 d가 7이고, 符號語 중에 원소가 모두 1인 23차원 벡터가 있다. 따라서 집합 T는 {4,5,…,19}의 부분집합이다.

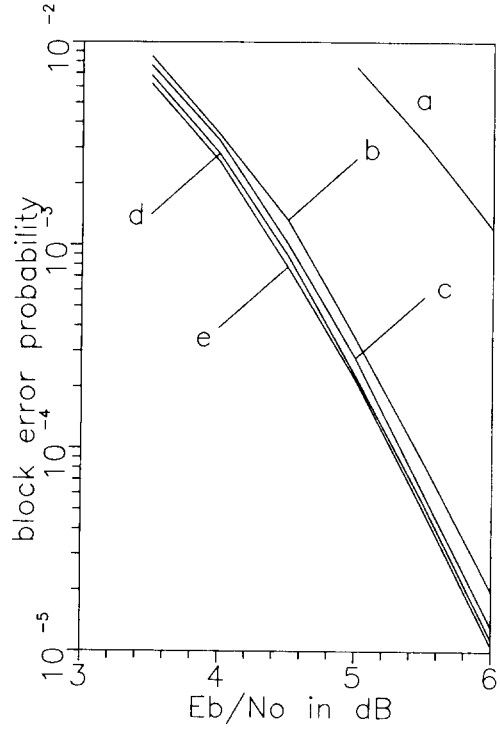
여러가지의 T와 S에 대하여 수행을 하였으며, 그 중에서 2가지 경우를 선택하여 그 결과를 제시한다. T와 S가 모두 {4,5,…,19}인 경우를 case 1 이라 하였다. case 1 은 모든 경우들 중에서 가장 낮은 블럭 에러 確率을 갖는다. 復號의 複雜度는 硬判定 復號의 回數로 결정된다. 硬判定 復號의 최대 回數는 1+|T|+|S| 이며, 시스템에 따라서는 이것이 제한을 받을 수도 있다. 이러한 이유로 최대 8회의 硬判定 復號 回數를 갖는 경우 중에서 블럭 에러 確率이 가장 낮은 경우를 선택하여 case 2 라 하였다. case 2에서는 T가 {4,5,8,9}이고, S가 {4,5,8}이다.

표 1. E_b/N_o = 5.0 dB 에서 提案된 알고리듬 (case 1) 의 블럭 에러 確率과 硬判定 復號 回數

Table 1. Block error probability and the number of hard-decision decodings of proposed algorithm (case 1) for E_b/N_o = 5.0 dB.

Normalized threshold ø	Block error probability	Number of hard-decision decodings	
		Average	Standard deviation
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

E_b/N_o = 5.0 dB 에서 case 1에 대한 블럭 에러 確率과 硬判定 復號 回數를 표 1에 나타내었다. 정규화된 임계값 ø를 $\phi/\sqrt{E_s}$ 로 정의한다. ø=1.5일때의 블럭 에러 確率은 ø=∞일때와 거의 같지만, 硬判定 復號 回數의 平均과 표준편차의 측면에서 유리함을 알 수 있다. case 2의 결과도 같은 경향을 보이므로 제시하지 않았다.



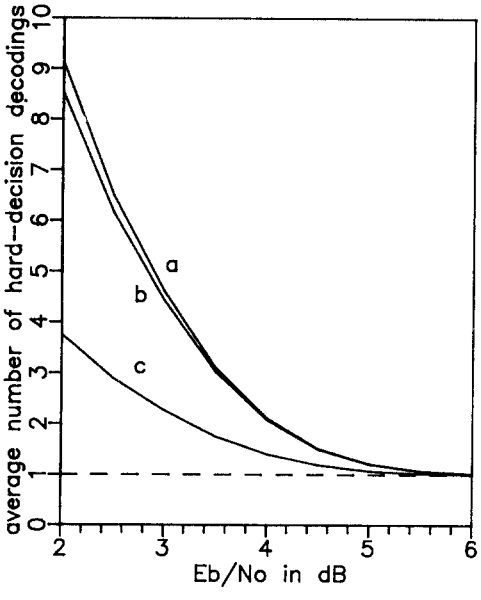
a Hard-decision decoding
b Chase's algorithm 2
c Proposed algorithm (case 2)
d Proposed algorithm (case 1)
e Maximum likelihood decoding

그림 1. 블럭 에러 確率 對 E_b/N_o

Fig. 1. Block error probability versus E_b/N_o.

E_b/N_o에 따른 블럭 에러 確率을 그림 1에 나타내었다. case 1과 case 2는 ø=∞일때의 결과이다. 블럭 符號에 대한 기존의 軟判定 復號 알고리듬 중에서는 Chase의 알고리듬[2] 이 가장 잘 알려져 있고, 본 논문에서 提案된 방법과의 관련이 깊다. 提案된 방법과의 비교를 위하여 Chase의 알고리듬 2와 最尤 復號法, 그리고 硬判定 復號法에 대한 컴퓨터 시뮬레이션을 수행하여 그 결과를 함께 제시하였다. case 1의

블럭 에러 確率은 最尤 復號法과 거의 동일하다. case 2는 Chase의 알고리듬 2보다 낮은 블럭 에러 確率을 갖는다. Chase의 알고리듬 2에 필요한 硬判定 復號 回數는 8회이다. 그러나, case 2는 硬判定 復號 回數가 8회를 넘지 않으면서, E_b/N_o = 5.0 dB에서 平均이 1.0499이고 표준편차가 0.5658이다.



a　ø = ∞
b　ø = 1.5
c　ø = 0.5

그림 2. 提案된 알고리듬(case 1) 의 硬判定 復號 回數의 平均 對 E_bN_o

Fig. 2. Average number of hard-decision decodings of proposed algorithm (case 1) versus E_b/N_o.

그림 2에 case 1의 여러가지 ø값을 파라미터로 하여 E_b/N_o에 따른 平均 硬判定 復號 回數를 나타내었다. E_b/N_o가 충분히 클때, 硬判定 復號 回數의 平均은 1(점선)에 접근함을 알 수 있다.

Ⅳ. 결론

本 論文에서는 후보 符號語들을 효율적으로 찾아낼 수 있는 軟判定 復號法을 提案하였다. 提案된 復號法에 필요한 硬判定 復號의 平均 回數는 1에 접근하며, 最尤 復號法과 거의 동일한 블럭 에러 確率을 얻을 수 있음을 컴퓨터 시뮬레이션을 통하여 확인하였다.

본 알고리듬을 특정한 2元 블럭 符號에 적용하려면, 시스템이 요구하는 조건과 상황에 적합하도록 임계값과 T, S를 결정해야 한다. 이 과정에서 예비 실험이나 컴퓨터 시뮬레이션이 요구될 수도 있다.

參 考 文 獻

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

[2] 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.

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

[4] M.A.El-Agamy and E.Munday, "Reduced search soft-decision minimum- distance decoding for binary block codes," *IEE Proc.*F, vol.133, pp.34-39, 1986.

[5] D.J.Taipale and M.B.Pursey, "An improvement to generalized- minimum-distance decoding," *IEEE Trans. Inform.* Theory, vol.IT-37, pp.167-172, Jan. 1991.

[6] Y.G.Shim and C.W.Lee, "An efficient algorithm for soft-decision decoding of linear binary block codes," *Proc. of JTC-CSCC '89*, pp.198-203, June 1989.

[7] 沈龍杰, 李忠雄, "線形 2元 블럭 符號를 위한 軟判定 復號 알고리듬," 電子工學會論文誌, 제27권 제2호, pp. 9-15, 1990년 2월.

[8] J.L.Massey, Threshold decoding, Cambridge, Mass. MIT Press, 1963.

[9] C.R.P.Hartmann and L.D.Rudolph, "An optimum symbol-by-symbol decoding rule for linear codes," *IEEE Trans. Inform.* Theory, vol.IT-22, pp.514-517, Sept. 1976.

[10] E.J.Weldon,Jr., "Decoding binary block codes on Q-ary output channels," *IEEE Trans.* Inform. Theory, vol.IT-17, pp. 514-517, Nov. 1971.

[11] R.A.Silverman and M.Balser, "Coding for a constant data rate source," *IRE Trans.* Inform. Theory, vol.4, pp.50-63, 1954.

著 者 紹 介

沈 龍 杰(正會員) 第 27卷 第 2號 參照
현재 단국대학교 전자공학과 조교수

李 忠 雄(正會員) 第 26卷 第 5號 參照
현재 서울대학교 전자공학과 교수