特輯 · 技術解說

부호 시스템과 응용

李 在 弘
(正 會 員)
서울大學校 工科大學 電子工學科 助敎授

Ⅰ. 서 론

사회구조 및 산업구조가 발달하고 경제가 성장함에 따라서 통신에 대한 필요성과 욕구가 증대되었다. 이에 부응하여 지난 수년 동안 통신망은 괄목할 정도로 확장되었고 통신량도 급속히 증가하였다. 이와 같은 통신의 양적 팽창과 함께 높은 신뢰도도 함께 요청되고 있다.

통신은 정보를 한 곳에서 다른 곳으로 전달한다. 컴퓨터 기억장치는 정보를 한 시점에서 다른 시점으로 전달한다. 어느 경우에나 잡음은 수신된 데이타를 원래의 데이타와 다소 다르게 만든다. 그러나 Shannon이 1948년에 발표한 통신로 부호화(channel coding)에 관한 정리에서 잡음이 통신의 신뢰도를 떨어지지 않게 할 수 있음을 보였다.[1] 즉, 잡음이 전달되는 정보율의 수용능력에 한계를 가하게 하는 대신 신뢰도는 유지를 할 수가 있다. 이러한 역할을 담당하는 것이 통신로 부호 또는 에러정정 부호(error correcting code)이다.

1950년대와 60년대에는 부호에 사용되는 부호기와 복호기를 구성하는데 많은 양의 디지탈 hardware를 필요로 하였던 까닭으로 부호를 사용하는 것이 가격 및 중량의 측면에서 곤란하였다. 부호를 사용하지 않고 신뢰도를 높이는 가장 간단한 대안은 송신신호의 출력을 증가시키는 것이다. 그러나 송신신호의 출력은 전파관리법에 의하여 규제가 되고 있어서 증가시키는 데는 제약이 따른다. 또한 이 방법은 이동통신, 위성통신, 군사통신 등과 같이 에너지의 가격이 비싼 통신 시스템에서는 사용하기가 어렵다.

1960년대 이래로 반도체 기술의 급격한 발달로 특히 VLSI 기술과 마이크로프로세서 기술의 눈부신 발달로 디지탈 회로의 가격이 급속히 내렸다. 또한 부호의 복호 알고리즘과 그것을 실현하는 디지탈 hardware 기술도 괄목할 정도로 발전하였다. 반면 전력공급장치, 안테나 등과 같은 장치의 가격은 별로 내리지가 않았다. 따라서 경제적인 측면에서 부호 시스템을 사용하는 점이 점점 더 유리하게 되었고 이러한 추세는 앞으로도 계속될 전망이다.

본 고에서는 여러 유형의 부호들을 개략적으로 설명하고 그 성능을 비교한 후 부호들을 응용한 시스템들을 살펴보고 실제로 사용되는 부호에 대해서도 알아본다.

Ⅱ. 이산적 통신로와 부호

에러정정부호(error correcting code)를 사용한 디지탈 통신시스템의 모델은 그림 1과 같다.[2] 파형전송로(waveform channel)는 정보가 담긴 전기적 신호나 전자기파가 통과하는 매질로써 초고주파 링크, 동축케이블, 광섬유, 전화회선 등이 있다. 전기적 신호와 전자기파는 파형 전송로를 통과하는 과정에서 불가피하게 잡음과 간섭 등의 영향을 받는다. 파형전송로와 변조기, 복조기를 묶어서 하나의 구성블록으로 보면 그 입력과 출력은 각각 이산적 데이타이고 입력된 데이타에 에러가 확률적으로 발생하여 출력에 전달된다. 이 구성블록을 離散的 데이타 통신로(discrete data channel)이라 하고 간략히 통신로(channel)라 부른다. 이산적 데이타 통신로의 보편적인 예로서 2元 대칭 통신로(binary symmetric channel), 2元 소거 통신로(binary erasure channel), 2元 소거-에러 통신로

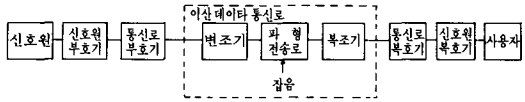
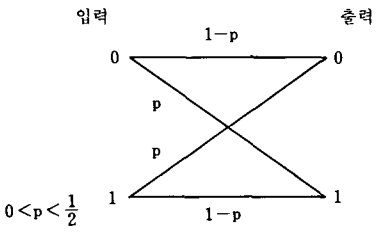
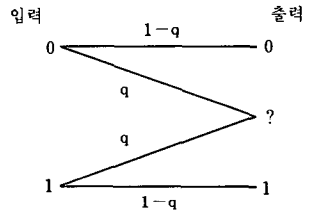


그림 1. 디지탈 통신 시스템의 모델

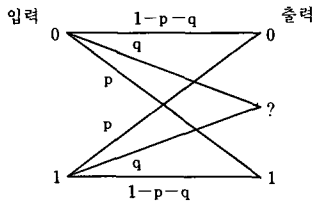
(binary erasure-error channel)을 그림2의 (a), (b), (c)에 각각 보였다. 그림2의 (b)와 (c)에서 소거(erasure)는 복조과정에서 軟性판정(soft decision)을 함으로써 "0"과 "1"의 경계영역에서 발생한다.



(a) 2元 대칭 통신로



(b) 2元 소거 통신로



(c) 2元 소거-에러 통신로

그림 2. 이산적 데이타 통신로의 보기

이와 같은 통신시스템의 모델은 정보저장 시스템을 표현하는 데에도 사용될 수 있다. 정보저장 시스템에서 이산적인 데이타가 정보저장 장치를 통하여 기록되고 검색되는 과정에서 에러가 확률적으로 발생하므로 정보저장 장치는 이산적 데이타 통신로로 간주될 수 있다. 정보저장 장치에는 자기 테이프 기록/검색 장치, 광학적 데이타 기록/검색장치, RAM(random access memory) 등이 있다. 표1에 통신로와 정보 저장장치를 비교하였다.

통신의 목표는 신호원으로부터 사용자까지 정보를 효율적이고 신뢰성 있게 전달하는 것이다. 효율적인 통신을 달성하기 위하여 신호원 부호기(source encoder

표 1. 통신로와 정보 저장장치의 대비

통 신 로	정보 저장장치
전 송	기 록
수 신	검 색
공간적 거리	시간적 간격
시간적 시퀀스	평면상의 배열

는 신호원으로부터의 신호를 양자화(quantization)하고 데이타 압축(data compression)을 하는데, 수신측의 신호원 복호기(source decoder)는 신호원 부호기의 逆으로 작용하여 원래의 신호를 복원하여 사용자에게 전달한다. 이러한 과정을 신호원 부호화 (source coding)라고 한다.

신뢰성이 높은 통신을 달성하기 위하여 통신로 부호기(channel encoder)는 신호원 부호기에서 출력된 정보 심볼의 시퀀스에 redundancy를 더하여 부호어(codeword)를 만들고, 수신측의 통신로 복호기(channel decoder)는 에러가 발생한 수신어를 redundancy를 사용하여 정정하고 추정된 정보 심볼의 시퀀스를 출력한다. 이러한 과정을 통신로 부호화라고 한다. 본 논문에서는 통신로 부호만을 다루고 以下 통신로 부호기를 부호기로, 통신로 복호기를 복호기로, 통신로 부호를 부호로 각각 표기한다.

Ⅲ. 부호의 종류

오늘날 보편적으로 사용되는 부호는 블록부호(block code)와 길쌈부호(convolutional code)의 두가지로 크게 나누어진다.

이 두형의 부호의 구분은 부호화된 블록이 그에 대응되는 정보블록(information block)에만 상관관계를 가지느냐 아니면 그 이전의 정보블록과도 상관관계를 가지느냐에 달려있다.

블록부호의 부호기는 정보블럭이 입력되면 각각 n개의 통신로 심볼(channel symbol)로 구성된 M개의 시퀀스 중의 하나를 출력한다. 이 M개의 길이가 n인 q元 시퀀스의 집합을 부호라고 하고 그 각각을 부호어(codeword), n을 부호장(codelength)이라고 한다. 모든 실제적인 시스템에서 부호어의 갯수는 q의 누승형이다. 즉, $M=q^k$이다. 이 경우 부호기는 k개의 정보심볼로 구성된 블록이 입력되면 이에 고유하게 대응되는 길이가 n인 q元 부호어를 출력한다. 이때 $R=k/n$을 부호율(code rate)이라고 한다.

길쌈부호는 樹枝狀부호(tree code)의 일종이다. 樹枝狀부호는 부호장이 무한대이고 樹枝狀표현도에 의해서 표현될 수 있는 부호이며, 그중 가장 유용하고 보편적인 부호가 길쌈부호이다. 길쌈부호의 부호기는 k개의 정보심볼로 구성된 정보블록이 입력되면 길이가 n인 q元 시퀀스를 출력하는데, 이 n-심볼 시퀀스는 그에 대응되는 정보블록 뿐만 아니라 그에 선행되는 M개의 정보블록에도 종속적이다. 즉, 부호기는 階數가 M인 기억을 가진다.

1. 블록부호

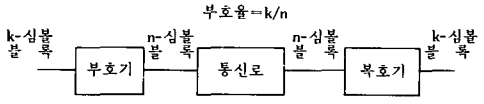
(1) 선형 블록부호(linear block code)

선형 블록부호는 블록부호의 일종으로 부호어의 집합이 선형 벡터공간을 형성한다. q元(n, k) 선형 블록부호는 2^k개의 부호어를 가지며 부호어의 집합은 Galois 體 GF(q) 위의 n-차원 벡터공간의 부분공간을 형성한다. 선형 블록부호는 줄여서 선형부호(linear code)라고 부른다.

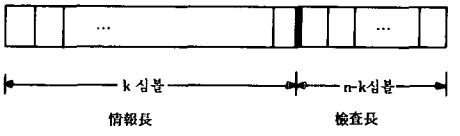
선형부호의 부호기와 복호기의 입출력 관계는 그림 3 (a)와 같다. 부호기는 k개의 정보심볼의 블록 $\boldsymbol{i}$를 받아서 n개의 채널심볼로 구성된 부호어 $\mathbf{c}$를 출력하는데 그 관계는 생성행렬(generator matrix) G를 써서 다음 식으로 표시할 수 있다.

$$\mathbf{c}=\boldsymbol{i}G$$

선형부호 가운데 그림 3 (b)에서와 같이 부호어가 좌측의 k개의 정보심볼과 우측의 n-k개의 검사심볼(parity-check symbol)로 분리될 수 있는 부호를 조직부호(systematic code)라고 한다. 조직부호의 경우 생성행렬은 $G=[I\,|\,A]$의 형태를 가지는데 이때 I는 단위행렬이다. 임의의 부호어 $\mathbf{c}$는 다음의 검사방정식을 만족한다.



(a) 부호기와 복호기



(b) 조직부호

그림 3. 선형부호

$$H\mathbf{c}^T=\mathbf{0}^T$$

이러한 행렬 H를 검사행렬(parity-check matrix)이라고 하고 조직부호의 경우 H는 $H=[-A^T\,|\,I]$의 형태를 가진다.

복호기의 복호원리는 다음과 같다.

전송된 부호어 $\mathbf{c}$에 에러패턴 $\mathbf{e}$가 발생하여 $\mathbf{r}$이 수신되었다고 하자. 즉,

$$\mathbf{r}=\mathbf{c}+\mathbf{e}\,(\mathrm{mod}\text{-}q)$$

일때, 수신어의 誤症(syndrome) $\mathbf{s}$는 다음과 같이 정의된다.

$$\begin{aligned}\mathbf{s}^T &\triangleq H\mathbf{r}^T\\ &=H(\mathbf{c}+\mathbf{e})^T\\ &=H\mathbf{e}^T\end{aligned}$$

$$\underset{(n-k)\times n}{H}\ \underset{n\times 1}{\mathbf{e}^T}=\underset{(n-k)\times 1}{\mathbf{s}^T}$$

n개의 미지수에 대해 n-k개의 방정식이 주어지므로 하나의 $\mathbf{s}$에 대하여 q^k개의 $\mathbf{e}$의 해가 존재한다. 이러한 q^k개의 $\mathbf{e}$를 coset이라 한다. 복호기는 먼저 수신어 $\mathbf{r}$의 誤症 $\mathbf{s}$를 계산한 후, 최적복호법(maximum likelihood decoding)을 적용하여 $\mathbf{s}$에 대응하는 coset중 발생확률이 가장 큰 $\mathbf{e}$를 찾은 후 다음 식에 의해 복호화된 부호어 $\hat{\mathbf{c}}$를 출력한다.

$$\hat{\mathbf{c}}=\mathbf{r}-\mathbf{e}$$

두 부호어 $\mathbf{c}_1$, $\mathbf{c}_2$ 간의 해밍거리(hamming distance)는 c_1과 c_2의 대응되는 벡터 성분중 같지 않은 성분의 갯수이다. 부호의 최소거리(minimum distance) d_{min}은 임의의 두 부호간의 최소 해밍거리이다. 부호의 최소거리는 부호의 에러 정정능력 및 에러 검출능력을 결정짓는다. 최소거리가 d_{min}인 부호는

$$2t+1\le d_{min}$$

을 만족하는 가장 큰 정수값인 t개의 에러를 정정할 수 있다. 최소거리가 d_{min}인 부호는

$$2t+f+1\le d_{min}$$

을 만족하는 t개의 에러와 f개의 소거를 동시에 정정할 수 있다. 또한 최소거리가 d_{min}인 부호는

$$t+f+1\le d_{min},\quad (t<f)$$

을 만족하는 t개의 에러를 정정하고 동시에 f개의 에러를 검출할 수 있다.

(n, k) 선형부호중 $n=2^m-1$이고 $k=2^m-1-m$인 부호를 해밍부호(hamming code)라고 하는데 가능한 n과 k은 값은 표 2 와 같다.

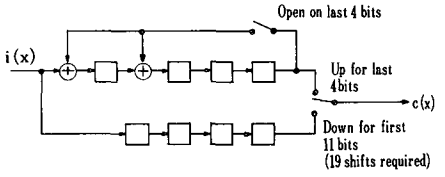
표 2. (n, k) 해밍코드의 n, k의 값

GF(2)	GF(4)	GF(8)	GF(16)	GF(27)
(7, 4)	(5, 3)	(9, 7)	(17, 15)	(28, 26)
(15, 11)	(21, 18)	(73, 70)	(273, 270)	(757, 754)
(31, 26)	(85, 81)	(585, 581)		
(63, 57)	(341, 336)			
(127, 120)				

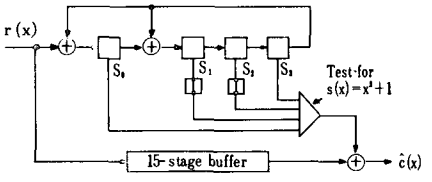
(2) 순회부호(cyclic code)

순회부호는 선형부호의 일종이다. 임의의 부호어를 $\mathbf{c}=(c_0, c_1, c_2, \cdots, c_{n-1})$라 할때 각 심볼을 한 자리씩 순회 치환시킨 $\mathbf{c}'=(c_1, c_2, \cdots c_{n-1}, c_0)$도 또한 부호어인 부호가 순회부호이다. 순회부호의 생성행렬과 검사행렬은 각각 생성다항식과 검사다항식으로 표현할 수 있는데 이 표현방법이 순회부호를 해석하는 기초가 된다. 다항식 표현에는 Galois體, ring과 같은 추상대수의 개념이 사용된다.

순회부호의 부호기와 복호기는 치환 레지스터(shift register)와 2元 가산기(binary adder)를 사용하여 구성한다. 순회부호의 일종인 (15, 11) 해밍부호의 부호기와 복호기는 각각 그림 4 (a)와 (b)와 같다.



(a) 부호기



(b) 복호기

그림 4. (15, 11) 해밍부호의 부호기와 복호기

(3) BCH 부호(Bose-Chandhuri-Hocquenghem code)

BCH 부호는 순회부호의 일종이다. 부호장이 $n=q^m-1$이고 t개의 에러를 정정할 수 있는 Galois體 GF(q) 위의 原始 BCH 부호는 그 생성다항식이 GF(q^m) 위의 $\alpha, \alpha^2, \alpha^3, \cdots, \alpha^{2t}$를 근으로 가진다. BCH 부호는 그 부호장과 부호율을 임의로 쉽게 실현할 수 있다. 1959년과 1960년에 Bose, Chaudhuri, Hocquenghem에 의하여 동시에 발견된 후 BCH 부호가 통신로 부호에 있어서 중요한 위치를 차지한 것은 부호 파라미터의 선택에 융통성이 있기 때문이기도 하지만 부호장이 數百 내외인 BCH 부호는 같은 부호장과 부호율을 가지는 부호들 중 성능이 가장 좋은 편에 속하기 때문이다.

(4) 리드-솔로몬 부호(Reed-Solomon code)

리드-솔로몬 부호는 BCH 부호의 일종이다. BCH 부호는 이론적으로 잘 정의된 부호이고 임의의 부호장과 부호율도 쉽게 실현할 수 있지만 실제의 2元 통신로에 적용하는 데는 문제가 있다. GF(q)위의 리드-솔로몬 부호는 부호장 n이 $n=q-1$이다. $q=2^m$인 경우에는 그림 5 에서와 같이 각각의 통신로 심볼은 m개의 2元 비트들로 표시할 수 있다. 즉, q元 (n, k) 리드-솔로몬 부호는 2元 (mn, mk) 부호로 간주될 수 있다. 리드-솔로몬 부호는 2元 통신로에 쉽게 적용할 수 있고 連集에러(burst error)를 정정할 수 있어서 많이 사용된다. 또한 리드-솔로몬 부호는 고정된 n과 k값에 대하여 부호의 최소거리가 모든 부호들 중에서 가장 큰 최대거리 분리기호이다.

이상의 블록부호들의 포함관계를 도시하면 그림 6 과 같다.

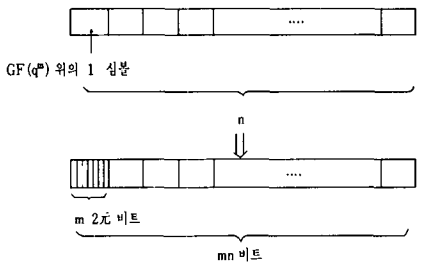


그림 5. $q=2^m$인 경우의 리드-솔로몬 부호

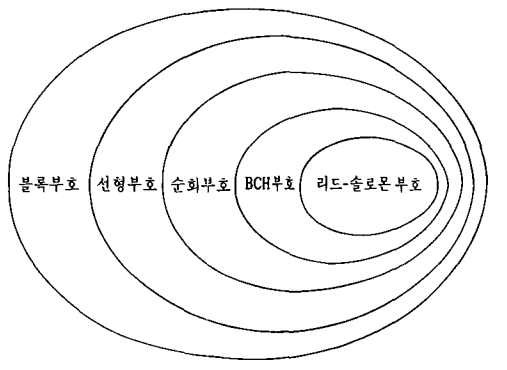


그림 6. 블록부호

(5) 선형부호의 수정

주어진 선형부호를 약간 수정함으로써 부호장이나 부호어의 갯수를 변화시켜 새로운 선형부호를 만들 수 있다. 기본적인 변형방법에는 다음 여섯 가지가 있다.

① 擴大(expanding) : 검사심볼을 추가함으로써 부호장을 증대시킨다.

② 延長(lengthening) : 정보심볼을 추가함으로써 부호장을 증대시킨다.

③ 簡略(puncturing) : 검사심볼을 버림으로써 부호장을 감소시킨다.

④ 短縮(shortening) : 정보심볼을 버림으로써 부호장을 감소시킨다.

⑤ 擴張(augmenting) : 부호장을 변화시키지 않고 정보심볼의 갯수 만을 증가시킨다.

⑥ 削除(expurgating) : 부호장을 변화시키지 않고 정보심볼의 갯수만을 감소시킨다.

예로써 (7, 4) 해밍부호의 수정과 그에 따른 새로운 부호의 구성을 그림7에 보였다.

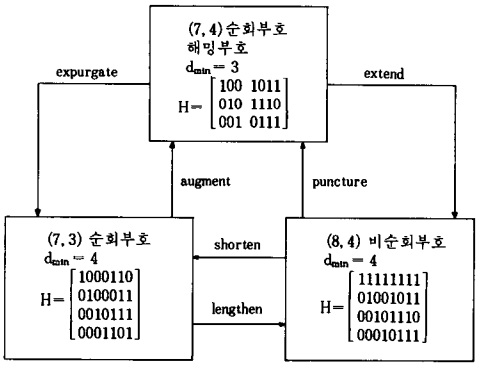


그림 7. (7, 14) 해밍부호의 수정

2. 길쌈부호

길쌈부호에서는 k개의 정보심볼로 구성된 정보블록을 길이가 n인 부호어로 부호화하는데 있어서 그 정보블록 뿐만 아니라 선행된 M개의 정보블록이 부호어를 결정짓는다. 이때 M을 記憶長(memory)이라 하고, M+1을 拘束長(constraint length)이라 하며 이러한 부호(n, k, M)를 길쌈부호라고 한다.

예로써 (2, 1, 3) 길쌈부호의 부호기를 그림8에 보였다.

길쌈부호의 생성을 행렬로 표시하면 정보 시퀀스가 $\boldsymbol{i}=(i_0, i_1, i_2, \cdots)$일때

$$\boldsymbol{c}=\boldsymbol{i}G$$

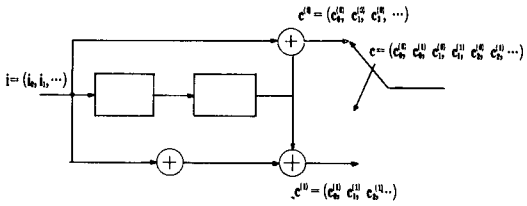


그림 8. (2, 1, 3) 길쌈부호의 부호기

이다. 생성행렬 G는 그림9와 같고 여기서 G_0, G_1, G_M은 각각 k×n 행렬이다. 길쌈부호의 부호기의 동작은 상태도(state diagram)로 나타낼 수 있다. 그림10은 그림8의 (2, 1, 3) 길쌈부호의 생성을 나타내는데 네 개의 사각형은 네 상태를 표시하는데 치환 레지스터에 저장된 비트의 값들을 표시한다. 실선은 입력 "0"에 따른 한 상태에서 다른 상태로의 전이를 나타내고 점선은 입력 "1"에 따른 한 상태에서 다른 상태로의 전이를 나타낸다. 전이선 옆의 괄호 속에 표시된 숫자는 전이에 대응하는 부호기의 출력을 나타낸다. 시간적 진행에 따른 길쌈부호의 생성은 格子狀표현도(trellis diagram)로 더 잘 나타낼 수 있다. 그림11은 그림8의 (2, 1, 3) 길쌈부호의 생성을 나타내는데 각 세로열의 네 점은 네 상태를 나타낸다. 실선과 점선이 입력 "0"과 "1"에 따른 전이를 나타내고 전이선 위에 적힌 숫자가 부호기의 출력을 표시한다.

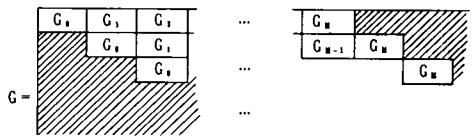


그림 9. 길쌈부호의 생성행렬

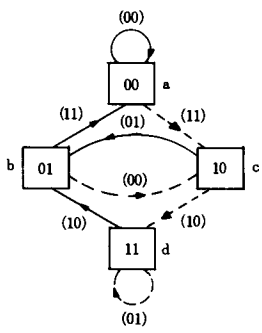


그림10. (2, 1, 3) 길쌈부호의 상태도

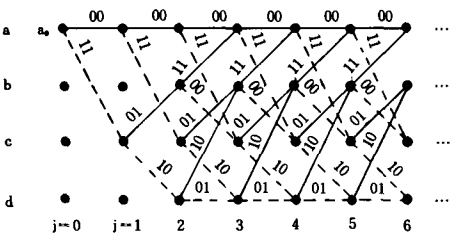


그림11. (2, 1, 3) 길쌈부호의 格子狀표현도

길쌈부호의 복호는 복호 알고리즘을 사용하여 樹枝狀표현도 위에서 경로를 찾는 것이다. 길쌈부호의 복호 알고리즘 가운데 Viterbi에 의하여 제안된 Viterbi 알고리즘은 최적복호기법을 사용한 것이므로 이 보다 더 성능이 좋은 복호 알고리즘은 없다. 그러나 Viterbi 알고리즘은 부호의 기억장 M이 증가함에 따라 알고리즘의 복잡도가 지수적으로 증가한다는 결점이 있다. 이러한 문제점은 順次복호 알고리즘을 사용함으로써 해결될 수 있는데 순차복호 알고리즘에는 Fano 알고리즘과 스택(stack) 알고리즘 등이 있다. 순차 복호 알고리즘은 Viterbi 알고리즘이 사용될 수 없는 기억장이 큰 길쌈부호에 적용하였을 때 좋은 성능을 나타내지마는, 한편으로는 복호에 필요한 계산의 양이 잡음의 정도에 따라 변한다는 점이 문제점으로 지적된다.

3. 블록부호와 길쌈부호의 비교

블록부호는 길쌈부호에 비해 오랜 연구의 역사를 가지고 있고 이론적으로 잘 정립이 되어 있다. 이 두 종류의 부호를 相加性 白色 Gaussian잡음(additive white Gaussian noise) 통신로에 응용했을 때의 성능을 비교한다.

성능은 부호를 사용하지 않은 BPSK(binary phase shift keying) 또는 QPSK(quarternary phase shift keying) 변조를 기준으로 하여 비교하는데, 한가지 특기할 사항은 부호를 사용한 시스템은 사용하지 않은 시스템 보다 넓은 RF주파수 대역폭을 필요로 한다는 점이다. 비트 에러확률이 각각 10^{-5}과 10^{-8}일때, 여러 부호의 부호화 이득(coding gain)을 표3에 비교하였다.[3] "데이타율"의 난에 적힌 것의 의미는 다음과 같다 : 낮음(10Kbps 이하), 중간(10Kbps 이상, 1Mbps 미만), 높음(1Mbps 이상, 20Mbps 미만), 매우 높음(20Mbps 이상).

중간 및 매우 높은 데이타율에서는 Viterbi 복호 알고리즘을 사용하는 길쌈부호가 덜 복잡해서 제일 유리해 보인다. 이것은 Viterbi 복호 알고리즘은 비교적 쉽게 軟性판정에 사용될 수 있는 반면, 블록부호는 硬性판정(hard decision)에만 사용할 수 있기 때문이다. 만약 부호장이 긴 블록부호를 복호화하는 효율적인 軟性 알고리즘이 개발된다면 아마도 그 부호화 이득이 Viterbi 복호 알고리즘을 사용한 길쌈부호에 필적할 것이다.

매우 높은 부호율에서는 外부호와 內부호에 리드-솔로몬 부호와 짧은 부호장의 블록부호를 각각 사용한 鎖狀부호(Ⅳ. 1절에서 설명됨)와 Viterbi 복호 알고리즘을 사용한 길쌈부호가 비슷한 부호화 이득을 가지는데 前者가 덜 복잡하다.

높은 부호율에서 보다 큰 부호화 이득을 얻자면 硬性판정에 順次 복호법을 사용하는 것이 가장 유리해 보인다. 중간 정도의 데이타율에서는 軟性판정에 順次복호법을 사용하는 것이 더 좋은 경우도 있다.

표3. Gaussian 통신로에 BPSK 또는 QPSK 변조와 함께 사용한 부호의 성능비교

부 호	부호화 이득(dB) ber=10^{-5}	부호화 이득(dB) ber=10^{-8}	데이타율
鎖狀부호(RS부호, Viterbi복호)	6.5-7.5	8.5-9.5	중 간
길쌈부호(順次복호, 軟性판정)	6.0-7.0	8.0-9.0	중 간
鎖狀부호(RS부호와 biorthogonal부호)	6.0-7.0	7.0-9.0	중 간
블록부호(軟性판정)	5.0-6.0	6.5-7.5	중 간
鎖狀부호(RS부호와 짧은 블록부호)	4.5-5.5	6.5-7.5	매우 높음
길쌈부호(Viterbi복호)	4.0-5.5	5.0-6.5	높 음
길쌈부호(硬性판정)	4.0-5.0	6.0-7.0	높 음
블록부호(硬性판정)	3.0-4.0	4.5-5.5	높 음
블록부호(임계복호)	2.0-4.0	3.5-5.5	높 음
길쌈부호(임계복호)	1.5-3.0	2.5-4.0	매우 높음
길쌈부호(목록이용 복호)	1.0-2.0	1.5-2.5	높 음

TDMA(time division multiple access)에서와 같이 블록단위의 데이타를 전송해야 하는 시스템 프로토콜에서는 길쌈부호의 부호기와 복호기는 한 블록을 처리한 후 반드시 all-zero의 상태로 돌아가서 다음 블록을 처리해야 한다. 이와 같은 시스템에서는 블록부호가 더 유리하다고 생각된다.

Ⅳ. 부호의 응용

부호장이 긴 부호를 덜 복잡한 hardware로 실현하기 위하여 鎖狀부호가 사용되고, 連集에러를 정정하기 위하여 interleaving/deinterleaving가 사용된다. 이들을 살펴본 후 실제로 응용되는 부호에 대해서 알아본다.

1. 鎖狀부호(Concatenated Code)

鎖狀부호는 Forney에 의해 긴 부호장과 큰 에러 정정능력을 가진 부호를 실현하는 방법으로 제안되었다. 鎖狀부호는 여러 단계의 부호로 구성할 수 있는데 보통 2단계의 부호가 많이 사용된다. 2단계 鎖狀부호의 기본도는 그림12와 같다. 통신로는 보통 2元 통신로이다. 즉, q=2. 內부호인 q元 (n, k) 부호는 q^k 개의 부호어를 가진다. 內부호의 부호기에 k개의 정보심볼이 입력되면 內부호의 복호기에서 에러가 발생하였을지도 모르는 복호화된 k개의 심볼을 출력된다. 內부호의 q^k개의 부호어는 각각 外부호의 하나의 부호심볼로 사용된다. 이러한 의미에서 內부호의 부호기, 통신로, 복호기를 묶어서 하나의 q^k元 통신로로 간주하고 수퍼통신로라고 부른다. 같은 방법으로 外부호의 부호기와 內부호의 부호기를 묶어서 수퍼부호기라고 하고, 內부호의 복호기와 外부호의 복호기를 묶어서 수퍼복호기라고 한다. 결과로 생기는 鎖狀부호는 Kk개의 q元 정보심볼로부터 생성된 부호장이 Nn인 부호 즉, q元(Nn, Kk) 부호로 간주될 수 있다. 鎖狀부호의 부호율은 $R_c = Rr = K/N \cdot k/n$로 外부호와 內부호의 부호율의 곱이다. 外부호에는 리드-솔로몬 부호가 많이 사용되는데 이것은 리드-솔로몬 부호가 최대 거리 분리기호이기도 하고 또한 실현하기가 용이하기 때문이다. 內부호에는 블록부호와 길쌈부호가 다 쓰인다. 적절한 外부호와 內부호를 선택함으로써 鎖狀이 아닌 부호에 비해서 복잡도가 또한 복호기와 높은 부호화 이득(coding gain)을 실현할 수 있다.

2. Interleaving/Deinterleaving

일반적으로 통신시스템의 성능을 분석할 때 통신로는 無記憶통신로라고 가정하고 통신로에 발생하는 에러는 그 발생확률이 시간에 따라 변하지 않는 散發에러(random error)라고 가정한다. 그러나 連集에러가 발생하는 통신로에서는 에러가 발생하면 연속해서 발생할 확률이 크므로 이 가정은 성립되지 않는다.

연집에러가 발생해서 한 부호어 내에 부호의 에러정정능력 보다 많은 갯수의 에러가 발생하면 부호는 에러를 정정할 수 없게 된다. 이러한 문제점의 해결방법 가운데 하나는 산발에러 정정부호를 interleaving/deinterleaving과 함께 사용하는 것이다. 이 방법에서는 부호기의 출력이 전송되기 전에 interleaving 되고 수신측에서 복호화되기 전에 deinterleaving된다. 이 시스템의 계통도는 그림13과 같다.

Interleaver는 미리 정해진 방법으로 심볼 시퀀스의 순서를 재배열하여 새로운 시퀀스를 구성한다. Deinterleaver는 interleaver의 逆으로 작용하여 원래의 순서대로 시퀀스를 복원한다. Interleaver의 일종인 블록 interleaver는 부호화된 심볼을 N×B 行列에 한 列씩 기록을 한 후 한 行씩 읽어서 전송을 한다. Deinterleaver는 수신된 심볼의 시퀀스를 行列에 한 行씩 기록을 한후 한 列씩 읽어서 내놓는다. 이러한 interleaver/deinterleaver는 디지탈 회로로 쉽게 구성할 수 있다. 길이가 B보다 작은 연집에러는 interleaver를 통과하면 적어도 N심볼만큼 떨어져 있는 산발에러로 바뀐다. 이때 한 부호어 내의 산발에러의 갯수가 부호의 에러정정 능력 이내이면 복호기에 의해 정정된다. 즉, interleaving/deinterleaving을 사용하면 連集에러를 사실상 산발에러로 바꿈으로써 連集에러를 정정할 수 있게 된다.

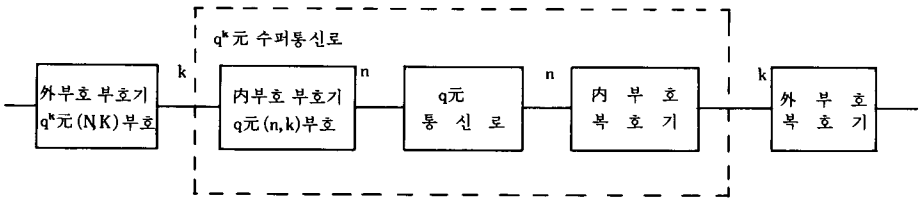


그림12. 鎖狀부호

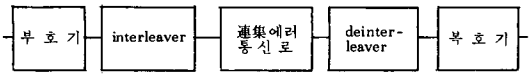


그림13. Interleaver와 deinterleaver

3. 부호 응용의 실제

부호의 실제적 응용은 이산적 데이타 통신로를 위한 부호와 정보저장 장치를 위한 부호의 두가지로 크게 나누어진다.

첫째로, 이산적 데이타 통신로에 발생한 에러를 검출 및 정정하는데는 블록부호와 길쌈부호가 모두 사용된다. 먼저 블록부호의 예로서는 AWACS를 포함하는 미국의 연합전략정보 분배시스템(JTIDS)에 사용된 (31, 15) 리드-솔로몬 부호, 통신위성 INTELSAT V에 사용된 (127, 112) BCH부호, 미국 공군위성통신(AFSATCOM)에 사용된 (7, 2) 리드-솔로몬 부호등과 같은 BCH부호 계열의 부호를 들 수 있다.[3]

이산적 데이타 통신로에는 길쌈부호도 사용되는데 우주 및 위성통신에 널리 사용되고 있다. 먼저 Viterbi 복호법을 사용한 길쌈부호의 한 예로 미국 항공우주국이 1977년 화성, 목성 및 토성 탐사를 목적으로 한 Voyager계획에 JPL연구소가 설계한 (2, 1, 6) 길쌈부호 및 (3, 1, 6) 길쌈부호用 codec(encoder/decoder)을 사용하였다. 行星표준부호로 알려진 이 길쌈부호들은 Viterbi 복호기에 3-비트 軟性판정을 사용하였는데 전송속도는 최고 100Kbps이었다.[4] 이 길쌈부호들 중 (2, 1, 6) 길쌈부호는 지금까지 미국의 방어위성통신망(DSCS)에 사용되고 있다.[5] 이 (2, 1, 6) 길쌈부호에 16개의 고속 Viterbi 복호기를 병렬로 사용하여 최고 160Mbps의 속도로 복호화 할 수 있는 시스템이 미국항공우주국의 데이타 중계위성(TDRSS)에 사용되고 있다.

順次복호법을 사용한 길쌈부호의 嚆矢는 1968년 미국항공우주국이 Pioneer 9호에 사용한 전송속도가 512bps인 (2, 1, 20) 길쌈부호이다.[6] 1970년 Linkabit社가 개발한 전송속도 50Mbps의 硬性판정 Fano 順次복호기를 사용한 길쌈부호가 미국항공우주국에 의하여 위성과 지상간의 자동계측기 전송장치에 사용되고 있다. 이 복호기는 지금까지 개발된 順次복호기 가운데 가장 빠르다.

連集에러 정정을 위한 길쌈부호의 예로써 1973년 Linkabit社가 미국 육군위성통신국을 위하여 개발한 interleaver/부호기와 Viterbi 복호기를 사용한 (2, 1, 6) 길쌈부호가 있다. 이 interleaver는 최고 1,024 비트의 連集에러를 분산시켜 에러 비트간의 간격이 64비트 이상이 되게 할 수 있다. 1970년대 초에 Harris社는 함상의 위성통신 단말장치를 레이다의 무선주파수 간섭으로부터 보호하기 위하여 2Mbps의 부호시스템을 개발하였는데 (2, 1, 5) 길쌈부호에 Viterbi 복호법이 사용되었다.[7]

둘째로, 정보저장 장치에 발생한 에러를 검출 및 정정하는데는 길쌈부호 보다는 블록부호가 주로 사용된다. 먼저, 주기억장치에 부호를 사용한 정보저장 시스템의 嚆矢는 磁氣 코어 기억장치에 단일에러정정, 2중에러검출(SEC-DED) Hamming 부호를 사용한 1961년형 IBM시스템 7030 전자계산기이다. 그 후 IBM 시스템 360도 코어기억장치의 신뢰도를 높이기 위하여 단일에러정정, 2중에러검출 부호를 채택하였다. 1970년대에 들어와서 반도체 기억소자가 코어기억장치를 대체하게 되었는데 前者는 後者에 비하여 속도는 빠르나 신뢰도가 떨어지는 단점이 있다. 이 때문에 정확한 정보처리를 위하여 부호의 사용은 불가피하게 되었다. 비트 중심의 기억장치에서 발생되는 대부분의 에러는 단일에러이므로 IBM 시스템 370을 비롯한 많은 전자계산기가 SEC-DED 부호를 사용한다. IBM 시스템 370은 (72, 64) SED-DED 부호를 사용하는데 8 바이트 단위로 부호화와 복호화를 한다.

磁氣테이프, 磁氣디스크 등과 같은 전자계산기의 보조기억장치에는 표면의 결함, head의 기계적 결함, 먼지 등에 의하여 에러가 발생하는데 보통 連集 또는 소거의 形態로 발생한다. IBM 3420과 3850 테이프 시스템은 2중에러정정 부호를 사용한다.[8] 磁氣디스크에 저장된 파일은 여러 개의 트랙(track)으로 구성되고 각 트랙은 따로따로 access된다. 따라서 부호는 길고 연속된 기록을 포함하는 긴 트랙에 사용되고 고속처리가 가능해야 한다. 예로서 IBM 3330 디스크 시스템에는 길이가 11비트 미만인 단일 連集에러를 정정하고 길이가 22비트 미만인 단일 連集에러를 검출할 수 있는 (585422, 585366) Fire 부호가 사용된다. IBM3370 디스크 시스템에는 GF(2^8) 위의 단축 리드-솔로몬 부호가 사용된다. 보조기억장치의 일종인 photodigital 데이타 저장시스템에도 블록부호가 사용되는데 예로서 IBM Digital Cypress 대량 저장시스템에는 GF(2^6) 위의 (61, 50) 단축 리드-솔로몬 부호가 사용된다.[9]

디지탈 음향기기에도 에러정정부호가 사용되고있다. 콤팩트 디스크(CD : ccmpact disc)에는 內부호가 (32, 28) 리드-솔로몬이고 外부호가 (28, 24) 리드-솔로몬 부호인 鎖狀부호가 사용된다.[10] 디지탈 음향녹음기

(DAT : digital audio tape recorder)에는 內부호가 (32, 28) 리드-솔로몬 부호이고 外부호가 (32, 26) 리드-솔로몬 부호인 鎖狀부호가 사용된다.[11]

V. 결 론

본 고에서는 통신로 부호에 관한 전반적이고 개괄적인 설명을 하였다. 부호와 다른 기술을 결합시키는 기술을 소개하였고 현재 사용되고 있는 부호의 응용 예를 보였다.

1990년대의 정보화 통신시대를 앞두고 데이타 통신의 보급이 확대됨에 따라 통신의 신뢰도에 대한 요구가 커지고 있다. 시대적 요청에 호응하여 새로운 부호기술이 개발되고 보다 빠르고 쉽게 실현할 수 있는 복호화 알고리즘이 개발될 것으로 기대된다. 또한 반도체 기술의 발달에 힘입어 부호가 보편적으로 보급되어 통신의 신뢰도를 높이는데 기여할 것으로 예상된다. 그러나 이러한 과정에서 시스템 표준화 등의 정책적인 뒷받침이 있어야 부호분야의 체계적인 연구개발이 이루어 질 것이다.

參 考 文 獻

[1] C.E. Shannon, "A mathematical theory of communications," *Bell Syst. Tech. J.*, vol. 27, pp. 379-423, 623-656, 1948.

[2] G.C. Clark, Jr. and J.B. Cain, Error Correction Coding for Digital Communications, Plenum Press, 1981.

[3] V.K. Bhargava, "Forward error correction schemes for digital communications," *IEEE Commun. Mag.*, vol. 21, pp. 11-19, Jan. 1983.

[4] M.K. Simon and J.G. Smith, "Alternate symbol inversion for improved symbol synchronization in convolutionally coded systems," *IEEE Trans. Commun.*, vol. COM-28, pp. 228-237, Feb. 1980.

[5] J.P. Odenwalder and A.J. Viterbi, "Overview of existing and projected uses of coding in military satellite communications," NTC Conf. Rec., pp. 36.4.1-36.4.2, Los Angeles, California, Dec.1977.

[6] S. Lin and H. Lyne, "Some results on binary convolutional code generators," *IEEE Trans. Infor. Theory*, vol. IT-13, pp. 134-139, Jan. 1967.

[7] G.C. Clark, Jr. and R.C. Davis, "Two recent applications of error-correction coding to communications system design," *IEEE Trans. Commun. Technol.*, vol. COM-19, pp. 856-863, Oct. 1971.

[8] A.M. Patel and S.J. Hong, "Optimal rectangular code for high density magnetic tapes," *IBM J. Res. Dev.*, vol. 18, pp. 579-588, Nov. 1974.

[9] I.B. Oldham, R.T. Chien and D.T. Tang, "Error detection and correction in a photo digital storage system," *IBM J. Res. Dev.*, vol. 12, pp. 423-430, Nov. 1968.

[10] J. Peek, "Communications aspects of the compact disc digital audio system," *IEEE Commun. Mag.*, vol. 23, pp.7-15, Feb. 1985.

[11] T. Arai, T. Noguchi, M. Kobayashi and H. Okamoto, "Digital signal processing technology for R-DAT," *IEEE Trans. Consumer Electron.*, vol. CE-32, pp. 416-424, Aug. 1986. *

♣ 用 語 解 說 ♣

Hierarchical Network(계층망, 계위망)

통신망의 구성법으로, 교환국에 상하의 계층(계위)을 갖게하는 방법과 갖지 못하게 하는 방법이 있는데 전자를 계층망(계위망), 후자를 무계층망이라 한다. 성형망은 전자에 속하고 망형망(網形網)과 벌집형망(蜂巢形網)은 후자에 속한다.

Decoder

1) 여러 개의 입력단자와 출력 단자가 있는 회로에서 입력단자의 어떤 조합에 신호가 가하여졌을 때 그 조합에 대응하는 하나의 출력 단자에 신호가 나타나는 것. 해독기의 기능은 부호기(符號器)의 기능의 역에 해당한다.

2) 부호기로 부호화한 부호계열을 아날로그 양으로 변환하는 것을 말한다.