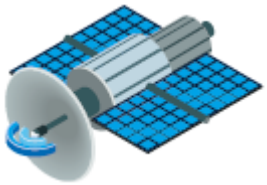
강의교안 이용 안내

- 본 강의교안의 저작권은 **김영길**과 **한빛아카데미㈜**에 있습니다.
- 이 자료를 무단으로 전제하거나 배포할 경우 저작권법 136조에 의거하여 벌금에 처할 수 있고 이를 병과(倂科)할 수도 있습니다.



한빛아카데미 Hanbit Academy, Inc.

CHAPTER 11

정보 이론과 부호 이론

기초

통신이론

디지털 통신 중심으로

한빛아카데미 Hanbit Academy, Inc.

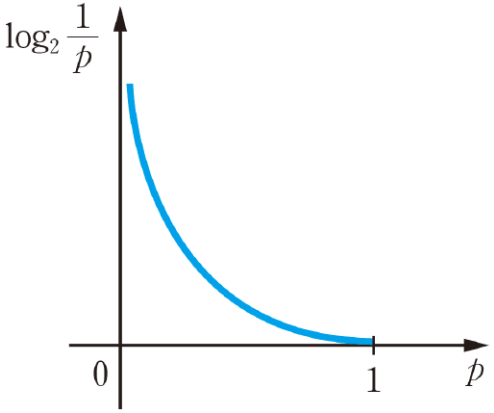
Contents

11.1 엔트로피

11.1 엔트로피

확률변수 X의 **엔트로피** $H(X)$

$$H(X) = -\sum_{i=1}^{m} p(x_i) \cdot \log_2 p(x_i) \qquad (11.1)$$



[그림 11-1] $\log_2 \frac{1}{p}$의 그래프

11.1 엔트로피

예제 11-1

다음과 같은 pmf를 갖는 베르누이 확률변수 X의 엔트로피 $H(X)$를 구하시오.

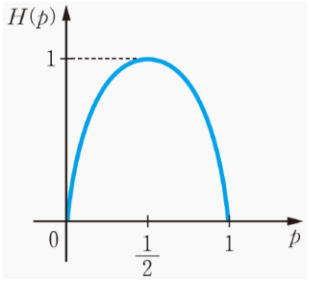
$$X=\begin{cases}1, & P(X=1)=p\\ 0, & P(X=0)=1-p\end{cases}$$

풀이

$H(X)=-\sum_{i=1}^{m}p(x_i)\cdot\log_2 p(x_i)$이므로 $H(X)=-p\log_2 p-(1-p)\log_2(1-p)$가 된다.

베르누이 확률변수의 엔트로피 $H(X)$를 $H(p)$로 쓰고, 이진 엔트로피 함수binary entropy function라고 부른다.

이진 엔트로피 함수 $H(p)$는 [그림 11-2]와 같다.



[그림 11-2] 이진 엔트로피 함수

$H(p)=-p\log_2 p-(1-p)\log_2(1-p)$

11.1 엔트로피

예제 11-2

다음 확률변수 X의 엔트로피 $H(X)$를 구하시오.

$$X=\begin{cases} a,\ P(X=a)=\dfrac{1}{2} \\ b,\ P(X=b)=\dfrac{1}{4} \\ c,\ P(X=c)=\dfrac{1}{4} \end{cases}$$

풀이

$H(X)=\sum_{i=1}^{m} p(x_i)\cdot \log_2 \dfrac{1}{p(x_i)}$ 이므로 $H(X)$는 다음과 같다.

$$H(X)=\frac{1}{2}\log_2 2+\frac{1}{4}\log_2 4+\frac{1}{4}\log_2 4$$

$$=\frac{1}{2}+\frac{1}{2}+\frac{1}{2}=\frac{3}{2}\ \text{bits/symbol}$$

11.2 결합 엔트로피와 조건부 엔트로피

11.2 결합 엔트로피와 조건부 엔트로피

- **결합 엔트로피**

$$H(X, Y) = -\sum_{i=1}^{m}\sum_{j=1}^{n} p(x_i,\ y_j) \cdot \log_2 p(x_i,\ y_j) \tag{11.3}$$

- **조건부 엔트로피**

$$\begin{aligned} H(Y|X) &= \sum_{i=1}^{m} p(x_i) \cdot H(Y|X=x_i) \\ &= -\sum_{i=1}^{m} p(x_i) \sum_{j=1}^{n} p(y_j|x_i) \cdot \log_2 p(y_j|x_i) \\ &= -\sum_{i=1}^{m}\sum_{j=1}^{n} p(x_i,\ y_j) \cdot \log_2 p(y_j|x_i) \\ &= -E[\log_2 p(Y|X)] \end{aligned} \tag{11.4}$$

11.2 결합 엔트로피와 조건부 엔트로피

$$
\begin{aligned}
H(X,\ Y) &= -\sum_{i=1}^{m}\sum_{j=1}^{n} p(x_i,\ y_j)\cdot \log_2 p(x_i,\ y_j) \\
&= -\sum_{i=1}^{m}\sum_{j=1}^{n} p(x_i,\ y_j)\cdot \log_2 \left[p(x_i)p(y_j\,|\,x_i)\right] \\
&= -\sum_{i=1}^{m}\sum_{j=1}^{n} p(x_i,\ y_j)\cdot \log_2 p(x_i) - \sum_{i=1}^{m}\sum_{j=1}^{n} p(x_i,\ y_j)\cdot \log_2 p(y_j\,|\,x_i) \\
&= -\sum_{i=1}^{m} p(x_i)\cdot \log_2 p(x_i) - \sum_{i=1}^{m}\sum_{j=1}^{n} p(x_i,\ y_j)\cdot \log_2 p(y_j\,|\,x_i) \\
&= H(X) + H(Y\,|\,X)
\end{aligned}
$$

11.2 결합 엔트로피와 조건부 엔트로피

예제 11-3

[표 11−1]과 같이 확률변수 X, Y의 joint pmf가 주어질 때, 다음을 구하시오.

[표 11−1]

Y \ X	1	2	3
1	$\frac{1}{8}$	$\frac{3}{16}$	$\frac{1}{16}$
2	$\frac{1}{16}$	$\frac{1}{8}$	$\frac{1}{16}$
3	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{4}$

(a) $H(X)$, $H(Y)$ (b) $H(X|Y)$ (c) $H(X, Y)$

11.2 결합 엔트로피와 조건부 엔트로피

풀이

(a) 확률변수 X의 pmf는 $\left(\frac{1}{4}, \frac{3}{8}, \frac{3}{8}\right)$이고, 확률변수 Y의 pmf는 $\left(\frac{3}{8}, \frac{1}{4}, \frac{3}{8}\right)$이다. 그러므로 $H(X)$는 다음과 같다.

$$H(X) = -\frac{1}{4}\log_2\frac{1}{4} - \frac{3}{8}\log_2\frac{3}{8} - \frac{3}{8}\log_2\frac{3}{8} = \frac{11}{4} - \frac{3}{4}\log_2 3$$

확률변수 Y는 확률변수 X와 같은 형태의 pmf를 가지므로 $H(Y) = \frac{11}{4} - \frac{3}{4}\log_2 3$ 이 된다.

(b) $$H(X|Y) = \sum_{i=1}^{3} p(Y=i)H(X|Y=i)$$

$$= \frac{3}{8}H\left(\frac{1}{3}, \frac{1}{2}, \frac{1}{6}\right) + \frac{1}{4}H\left(\frac{1}{4}, \frac{1}{2}, \frac{1}{4}\right) + \frac{3}{8}H\left(\frac{1}{6}, \frac{1}{6}, \frac{2}{3}\right)$$

11.2 결합 엔트로피와 조건부 엔트로피

풀이

$$H(X|Y)=\frac{3}{8}\left(\frac{2}{3}+\frac{1}{2}\log_2 3\right)+\frac{1}{4}\left(\frac{3}{2}\right)+\frac{3}{8}\left(\log_2 3-\frac{1}{3}\right)=\frac{1}{2}+\frac{9}{16}\log_2 3$$

(c) $$H(X,Y)=H(Y)+H(X|Y)=\frac{11}{4}-\frac{3}{4}\log_2 3+\frac{1}{2}+\frac{9}{16}\log_2 3=\frac{13}{4}-\frac{3}{16}\log_2 3$$

11.2 결합 엔트로피와 조건부 엔트로피

- **상호 정보량**

$$
\begin{aligned}
I(X;Y) &= \sum_{i=1}^{m}\sum_{j=1}^{n} p(x_i,\ y_j)\cdot \log_2 \frac{p(x_i|y_j)}{p(x_i)} \\
&= -\sum_{i=1}^{m}\sum_{j=1}^{n} p(x_i,\ y_j)\cdot \log_2 p(x_i) + \sum_{i=1}^{m}\sum_{j=1}^{n} p(x_i,\ y_j)\cdot \log_2 p(x_i|y_j) \\
&= -\sum_{i=1}^{m} p(x_i)\cdot \log_2 p(x_i) - \left(-\sum_{i=1}^{m}\sum_{j=1}^{n} p(x_i,\ y_j)\cdot \log_2 p(x_i|y_j)\right) \\
&= H(X) - H(X|Y) \qquad (11.9)
\end{aligned}
$$

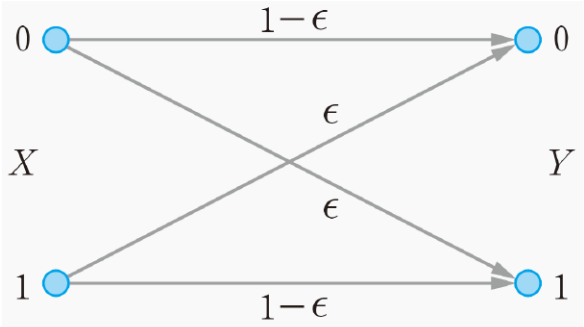
11.3 채널 용량

11.3 채널 용량

$$C = \max_{p(x)} I(X;Y) \qquad (11.10)$$

예제 11-4

[그림 11-4]의 이진 대칭 채널binary symmetric channel에서 채널 용량 C를 구하시오. 단, $P(X=0)=1-p$이고 $P(X=1)=p$이다.



[그림 11-4] 이진 대칭 채널($P(Y=1|X=0)=P(Y=0|X=1)=\epsilon$)

11.3 채널 용량

풀이

$$
\begin{aligned}
H(Y|X) &= \sum_{i=1}^{m} p(x_i) \cdot H(Y|X=x_i) \\
&= (1-p) \cdot H(Y|X=0) + p \cdot H(Y|X=1) \\
&= (1-p) \cdot H(\epsilon) + p \cdot H(\epsilon) \\
&= H(\epsilon) = -\epsilon \log_2 \epsilon - (1-\epsilon) \log_2 (1-\epsilon)
\end{aligned}
$$

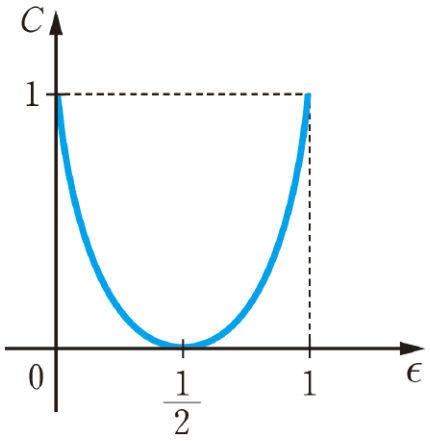
따라서 [그림 11-4]에서 이진 대칭 채널의 상호 정보량 $I(X;Y)$는 다음과 같다.

$$
\begin{aligned}
I(X;Y) &= H(Y) - H(Y|X) \\
&= H(Y) + \epsilon \log_2 \epsilon + (1-\epsilon) \log_2 (1-\epsilon)
\end{aligned}
\qquad (11.11)
$$

채널 용량 C는 p를 바꿔 가면서 식 (11.11)의 최댓값을 구한 것이다. 식 (11.11)에서 $H(Y)$만 p의 함수이고 $H(Y)$는 $p=\frac{1}{2}$일 때 최댓값 1을 갖는다. 따라서 [그림 11-4]의 이진 대칭 채널의 채널 용량 C는 식 (11.12)와 같다.

$$
C = 1 + \epsilon \log_2 \epsilon + (1-\epsilon) \log_2 (1-\epsilon) \qquad (11.12)
$$

11.3 채널 용량



[그림 11–5] 이진 대칭 채널의 채널 용량 C

★ 핵심 포인트 ★

- **채널 용량** : $C = \max_{p(x)} I(X;Y)$
- **채널 용량의 의미** : 어떤 채널을 한 번 사용할 때 최대 몇 비트를 보낼 수 있는가
- **이진 대칭 채널의 채널 용량** : $C = 1 + \epsilon \log_2 \epsilon + (1-\epsilon)\log_2(1-\epsilon)$

11.4 데이터 압축

11.4 데이터 압축

[그림 11-6] 출력이 코드워드 $C(x_i)$인 소스 부호화 블록

11.4 데이터 압축

예제 11-5

확률변수 X가 다음과 같이 정의되어 있다.

$$X=\begin{cases} a, & P(X=a)=\dfrac{1}{2} \\ b, & P(X=b)=\dfrac{1}{4} \\ c, & P(X=c)=\dfrac{1}{4} \end{cases}$$

코드워드를 다음과 같이 할당했을 때, 코드워드 길이의 평균값 $L(C)$를 구하고 이것을 확률변수 X의 엔트로피와 비교하시오.

$$C(a)=0,\quad C(b)=10,\quad C(c)=11$$

풀이

코드워드 길이의 평균값은 $L(C)=\frac{1}{2}\cdot 1+\frac{1}{4}\cdot 2+\frac{1}{4}\cdot 2=\frac{3}{2}$이 된다. 확률변수 X의 엔트로피는 $H(X)=-\frac{1}{2}\log_2\frac{1}{2}-\frac{1}{4}\log_2\frac{1}{4}-\frac{1}{4}\log_2\frac{1}{4}=\frac{3}{2}$이므로, 이 예제의 경우 $H(X)=L(C)$가 됨을 알 수 있다.

11.4 데이터 압축

예제 11-6

확률변수 X가 다음과 같이 정의되어 있다.

$$X=\begin{cases} a, & P(X=a)=\dfrac{1}{3} \\ b, & P(X=b)=\dfrac{1}{3} \\ c, & P(X=c)=\dfrac{1}{3} \end{cases}$$

코드워드를 다음과 같이 할당했을 때, 코드워드 길이의 평균값 $L(C)$를 구하고 이것을 확률변수 X의 엔트로피와 비교하시오.

$$C(a)=0,\quad C(b)=10,\quad C(c)=11$$

풀이

코드워드 길이의 평균값은 $L(C)=\frac{1}{3}\cdot 1+\frac{1}{3}\cdot 2+\frac{1}{3}\cdot 2=\frac{5}{3}$이다. 확률변수 X의 엔트로피는 $H(X)=\log_2 3$이므로, 이 예제의 경우 $H(X)<L(C)$가 된다.

허프만 부호

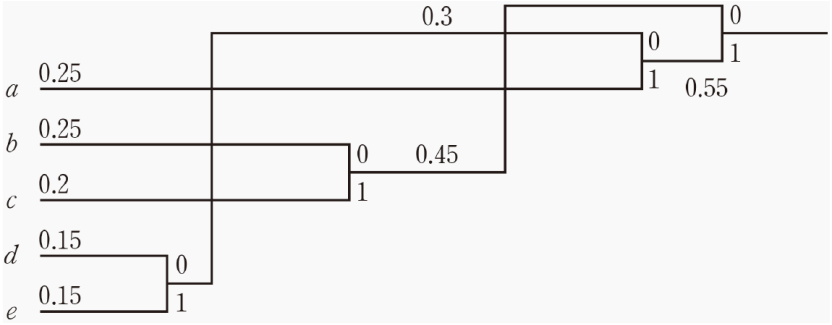
예제 11-7

아래와 같은 pmf를 갖는 확률변수 X가 있다.

$$X=\begin{cases} a, & P(X=a)=0.25 \\ b, & P(X=b)=0.25 \\ c, & P(X=c)=0.2 \\ d, & P(X=d)=0.15 \\ e, & P(X=e)=0.15 \end{cases}$$

이 확률변수를 정보 소스라고 가정할 때, 허프만 코드를 만드시오.

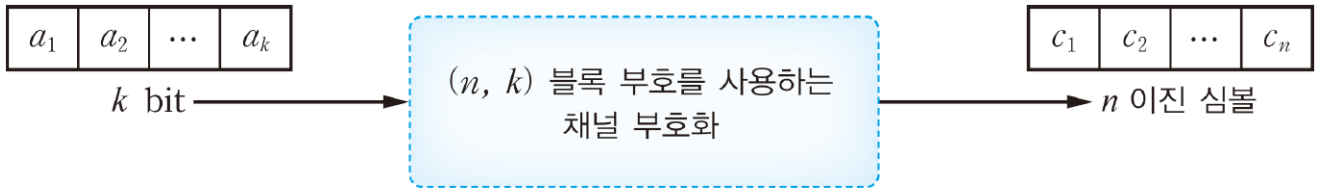
풀이



[그림 11-8] 허프만 코드를 만드는 과정

11.5 블록 부호

11.5 블록 부호



[그림 11-9] (n, k) 이진 블록 오류 정정 부호를 사용하는 채널 부호화 과정

- **최소 해밍 거리**

$$d_{\min} = \min_{v_1 \neq v_2} d_H(v_1, v_2) \tag{11.13}$$

선형 부호 C에서는 $v_1, v_2 \in C$이면 $v_1 + v_2 \in C$이므로 식 (11.14)가 성립한다.

$$d_{\min} = \min_{v \neq 0} w_H(v) \tag{11.14}$$

11.5 블록 부호

예제 11-8

다음 코드워드들로 구성된 선형 부호 C의 최소 해밍 거리 $d_{\min}$을 구하시오.

$$C = \{00000,\ 11111,\ 11000,\ 00111,\ 10000,\ 01111,\ 10111,\ 01000\}$$

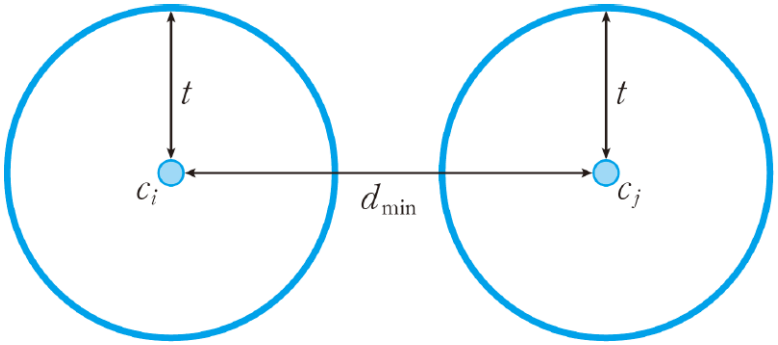
풀이

$$d_{\min} = \min_{v_1 \neq v_2} d_H(v_1,\ v_2) = 1$$

11.5 블록 부호

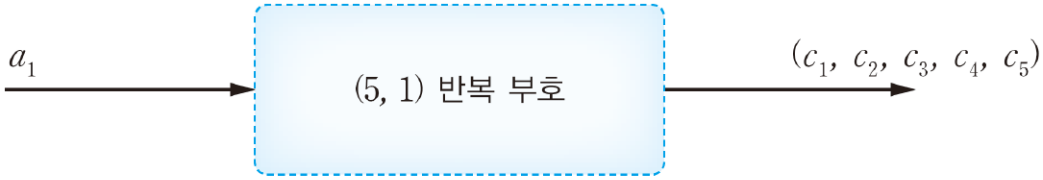
- **블록 부호의 오류정정능력**

$$t = \left\lfloor \frac{d_{\min} - 1}{2} \right\rfloor$$



[그림 11–10] $d_{\min}$ 만큼 떨어져 있는 코드워드 c_i와 c_j

11.5.1 (n,1) 반복부호

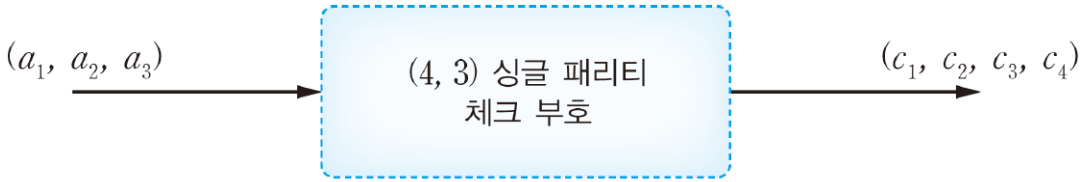


[그림 11-11] (5, 1) 반복 부호의 부호화기

$$c_1 = a_1 \qquad c_2 = a_1 \qquad c_3 = a_1$$
$$c_4 = a_1 \qquad c_5 = a_1 \tag{11.15}$$

- 최소 해밍 거리 = n
- 차원 = 1
- 부호율 = $1/n$

11.5.2 (n,n-1) 싱글 패리티 체크 부호

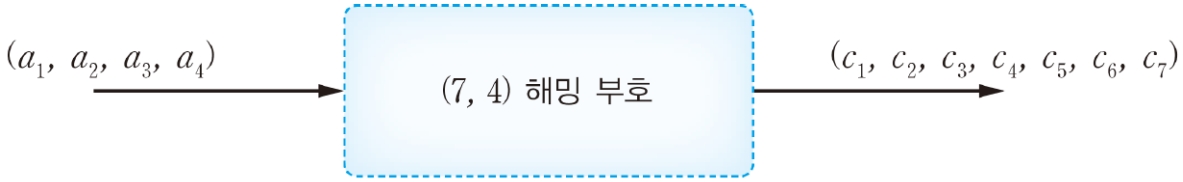


[그림 11-12] (4, 3) 싱글 패리티 체크 부호의 부호화기

$$c_1 = a_1 \qquad c_2 = a_2$$
$$c_3 = a_3 \qquad c_4 = a_1 + a_2 + a_3 \tag{11.16}$$

- 최소 해밍 거리 = 2
- 차원 = $n - 1$
- 부호율 = $(n-1)/n$

11.5.3 (7,4) 해밍 부호

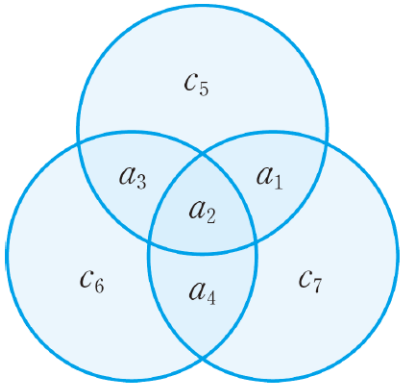


[그림 11-13] (7, 4) 해밍 부호의 부호화기

$$c_1 = a_1 \qquad c_2 = a_2 \qquad c_3 = a_3 \qquad c_4 = a_4$$
$$c_5 = a_1 + a_2 + a_3 \qquad c_6 = a_2 + a_3 + a_4 \qquad c_7 = a_1 + a_2 + a_4 \tag{11.17}$$

- 최소 해밍 거리 = 3
- 차원 = 4
- 부호율 = 4/7

11.5.3 (7,4) 해밍 부호



$$a_1 + a_2 + a_3 + c_5 = 0$$
$$a_2 + a_3 + a_4 + c_6 = 0$$
$$a_1 + a_2 + a_4 + c_7 = 0$$

[그림 11-14] $(7,\ 4)$ 해밍 부호 부호화 식들의 그림 표현

11.6 생성 행렬과 패리티 체크 행렬

11.6 생성 행렬과 패리티 체크 행렬

- **생성 행렬**

$$c = aG \qquad (11.18)$$

예제 11-14

(5, 1) 반복부호의 생성 행렬 G를 구하시오.

풀이

$$G = [11111]$$

$$[c_1 c_2 c_3 c_4 c_5] = [a_1][11111]$$

11.6 생성 행렬과 패리티 체크 행렬

예제 11-10

(4, 3) 싱글 패리티 체크 부호의 생성 행렬 G를 구하시오.

풀이

$$G = \begin{bmatrix} 1\,0\,0\,1 \\ 0\,1\,0\,1 \\ 0\,0\,1\,1 \end{bmatrix}$$

$$[c_1\,c_2\,c_3\,c_4] = [a_1\,a_2\,a_3] \begin{bmatrix} 1\,0\,0\,1 \\ 0\,1\,0\,1 \\ 0\,0\,1\,1 \end{bmatrix}$$

11.6 생성 행렬과 패리티 체크 행렬

예제 11-11

(7, 4) 해밍 부호의 생성 행렬 G를 구하시오.

풀이

$$G = \begin{bmatrix} 1\,0\,0\,0\,1\,0\,1 \\ 0\,1\,0\,0\,1\,1\,1 \\ 0\,0\,1\,0\,1\,1\,0 \\ 0\,0\,0\,1\,0\,1\,1 \end{bmatrix}$$

$$[c_1\,c_2\,c_3\,c_4\,c_5\,c_6\,c_7] = [a_1\,a_2\,a_3\,a_4] \begin{bmatrix} 1\,0\,0\,0\,1\,0\,1 \\ 0\,1\,0\,0\,1\,1\,1 \\ 0\,0\,1\,0\,1\,1\,0 \\ 0\,0\,0\,1\,0\,1\,1 \end{bmatrix}$$

11.6 생성 행렬과 패리티 체크 행렬

예제 11-12

(5, 1) 반복부호의 패리티 체크 행렬 H를 구하시오.

풀이

$$H=[P^T|I_{n-k}]=\begin{bmatrix}1&1&0&0&0\\1&0&1&0&0\\1&0&0&1&0\\1&0&0&0&1\end{bmatrix}$$

예제 11-13

(4, 3) 싱글 패리티 체크 부호의 패리티 체크 행렬 H를 구하시오.

풀이

$$H=[P^T|I_{n-k}]=[1111]$$

11.7 표준배열 복호화와 신드롬

11.7 표준배열 복호화와 신드롬

- **수신벡터**

$$r = c + e \qquad (11.20)$$

- **최소 해밍거리 복호화 기법**

$$\hat{c} = \arg\min_{c' \in C} d_H(r, c') \qquad (11.21)$$

11.7 표준배열 복호화와 신드롬

예제 11-14

(5, 2) 블록 부호이고 코드워드가 00000, 01011, 10101, 11110이다. 수신 벡터가 $r=11011$ 일 때, 최소 해밍 거리 복호화를 이용하여 복호하시오.

풀이

모든 코드워드로부터 수신 벡터 $r=11011$까지의 해밍 거리를 구한다.

$$d_H(11011,00000)=4,\ d_H(11011,01011)=1,$$
$$d_H(11011,10101)=3,\ d_H(11011,11110)=2$$

$d_H(11011,01011)=1$로 해밍 거리가 가장 작으므로 $\hat{c}=01011$로 복호화한다.

11.7 표준배열 복호화와 신드롬

[표 11-2] (3, 1) 반복 부호의 표준 배열

000	111
001	110
010	101
001	110

11.7 표준배열 복호화와 신드롬

예제 11-15

생성 행렬 $G=\begin{bmatrix}1&0&1&0&1\\0&1&0&1&1\end{bmatrix}$ 인 $(5,\ 2)$ 선형 블록 부호의 표준 배열을 그리고, 이것을 이용하여 수신 벡터가 11011일 때 복호화하시오.

풀이

[표 11-3] [예제 11-15] $(5,\ 2)$ 부호의 표준 배열

00000	01011	10101	11110
00001	01010	10100	11111
00010	01001	10111	11100
00100	01111	10001	11010
01000	00011	11101	10110
10000	11011	00101	01110
11000	10011	01101	00110
10010	11001	00111	01100

11.7 표준배열 복호화와 신드롬

- **신드롬**

$$s = Hr \tag{11.22}$$

예제 11-16

생성 행렬 $G = \begin{bmatrix} 1\,0\,1\,0\,1 \\ 0\,1\,0\,1\,1 \end{bmatrix}$ 인 $(5,\ 2)$ 선형 블록 부호를 사용한다. 수신 벡터가 11011일 때 신드롬 s 를 구하시오.

풀이

$$s = Hr = \begin{bmatrix} 1\,0\,1\,0\,0 \\ 0\,1\,0\,1\,0 \\ 1\,1\,0\,0\,1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$$

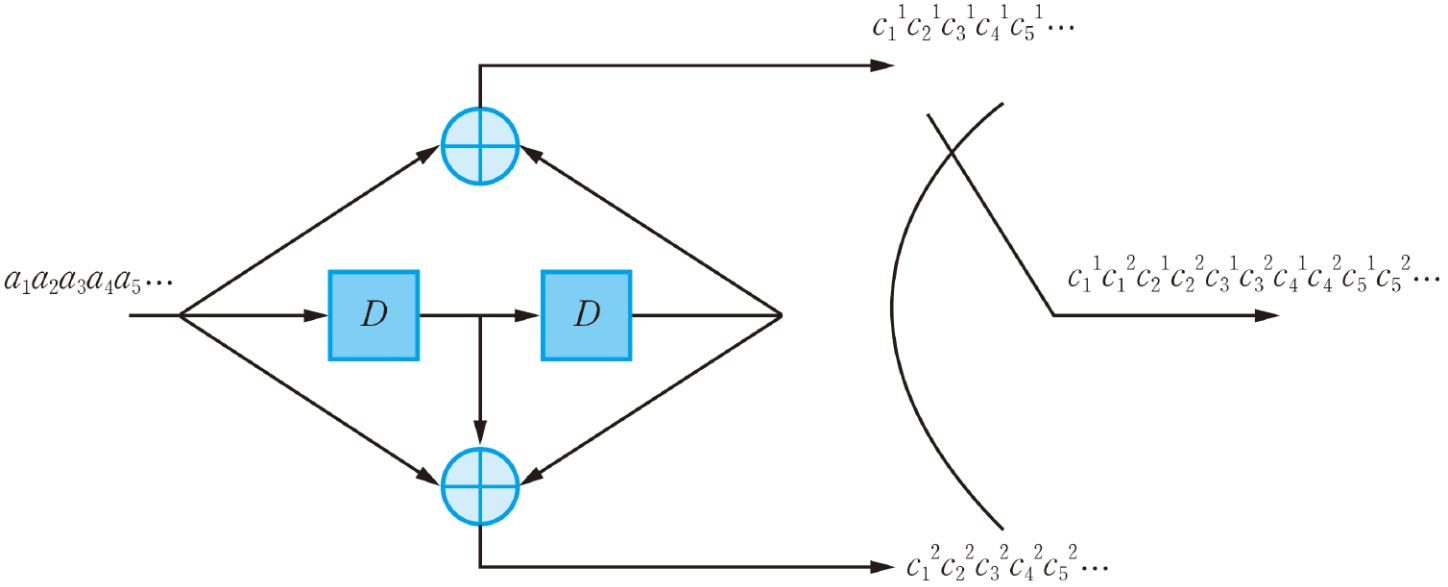
11.7 표준배열 복호화와 신드롬

[표 11-4] 생성 행렬 $G=\begin{bmatrix}1\,0\,1\,0\,1\\0\,1\,0\,1\,1\end{bmatrix}$인 $(5,\ 2)$ 선형 블록 부호의 신드롬 표

신드롬	추정 오류 벡터 $\hat{e}$ (코셋 리더)
000	00000
001	00001
010	00010
100	00100
011	01000
101	10000
110	11000
111	10010

11.8 컨볼루션 부호

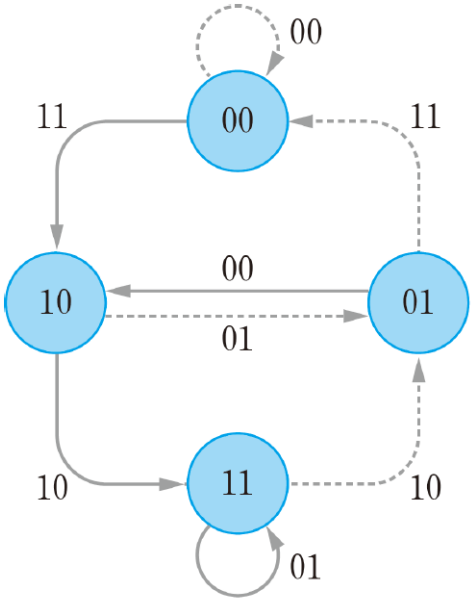
11.8 컨볼루션 부호



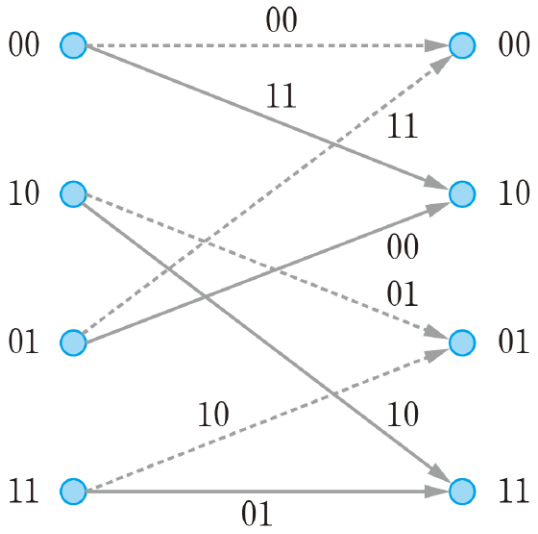
[그림 11–15] $\frac{1}{2}$ 컨볼루션 부호의 부호화기 예

$$c_i^1 = a_i + a_{i-2} = (1 + D^2)[a_i]$$
$$c_i^2 = a_i + a_{i-1} + a_{i-2} = (1 + D + D^2)[a_i] \qquad (11.24)$$

11.8 컨볼루션 부호

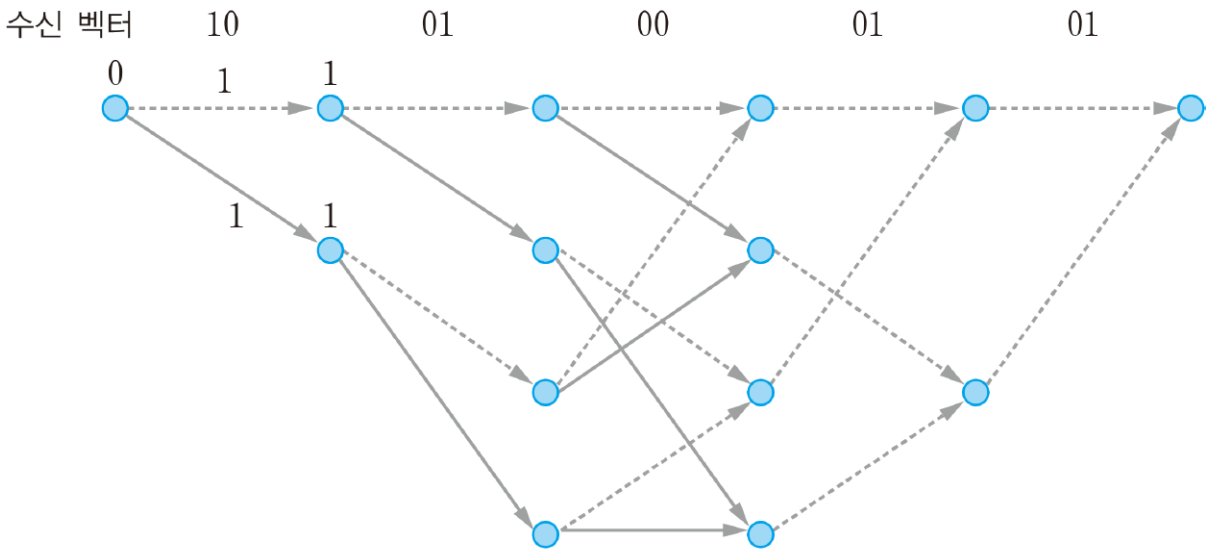


[그림 11-16] [그림 11-15]의 컨볼루션 부호의 상태 변화 다이어그램



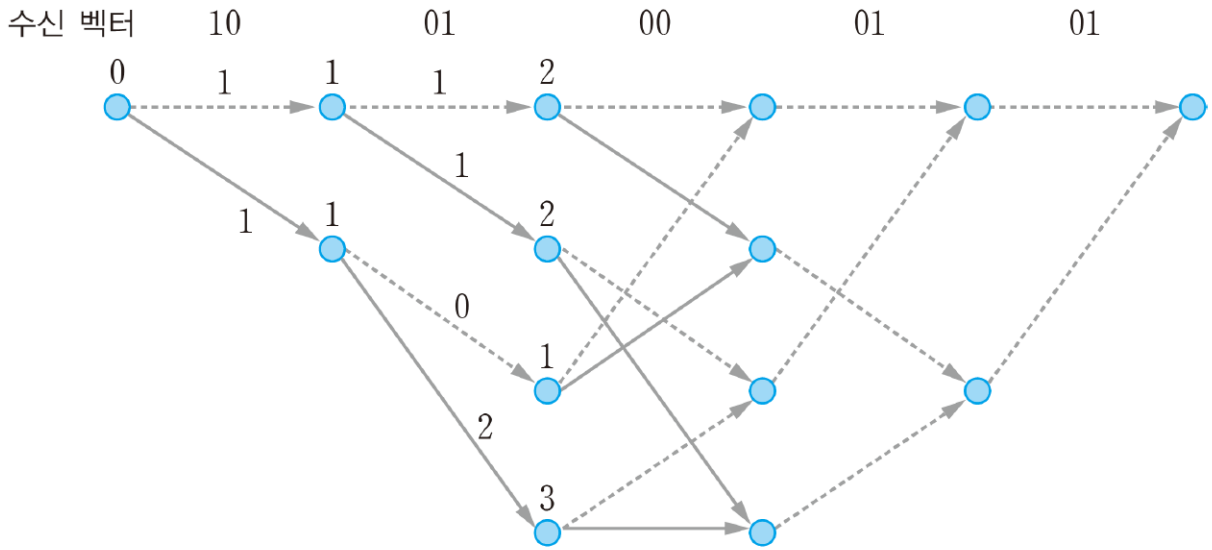
[그림 11-17] [그림 11-15]의 컨볼루션 부호의 트렐리스

11.8 컨볼루션 부호



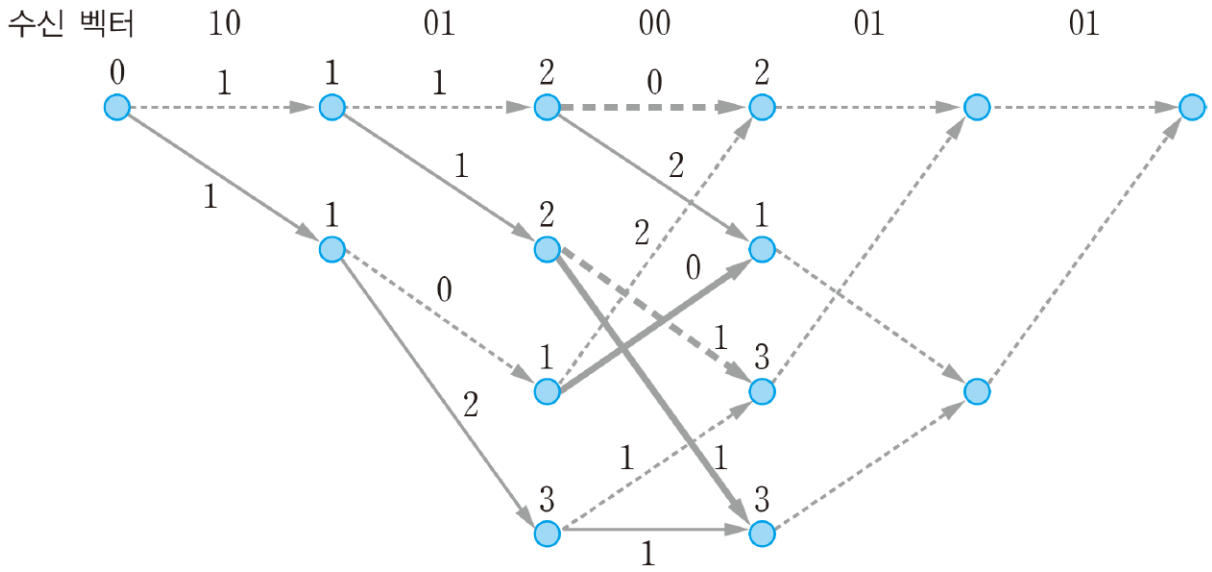
[그림 11-19] 다섯 개의 비트를 복호화하는 비터비 알고리즘 첫 단계(꼬리 비트 : 00)

11.8 컨볼루션 부호



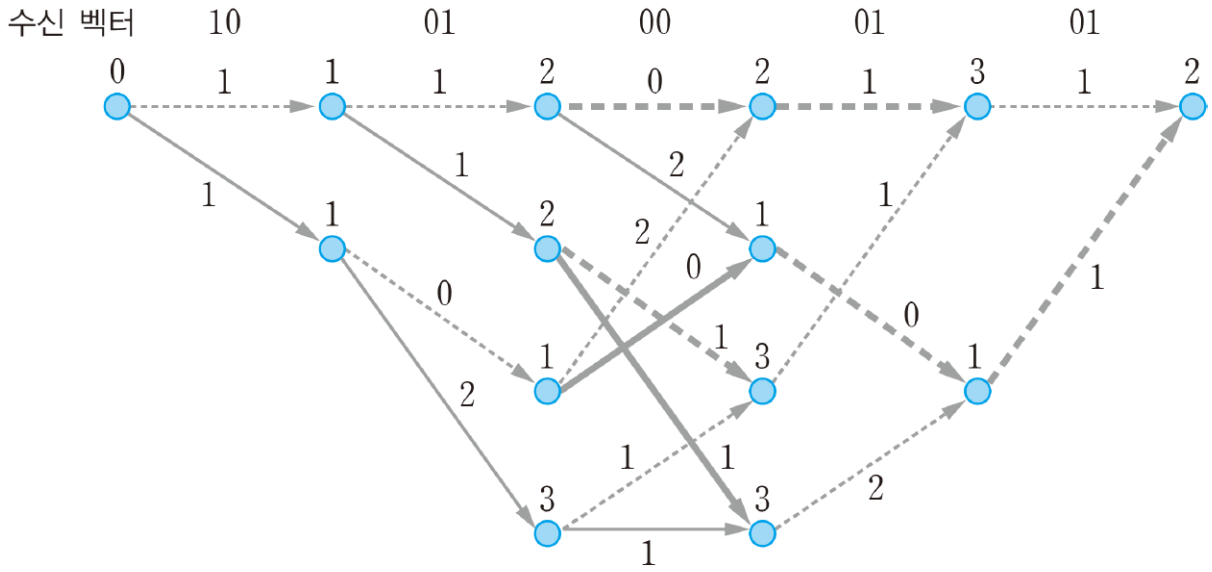
[그림 11-20] 다섯 개의 비트를 복호화하는 비터비 알고리즘 두 번째 단계(꼬리 비트 : 00)

11.8 컨볼루션 부호



[그림 11-21] 다섯 개의 비트를 복호화하는 비터비 알고리즘 세 번째 단계(꼬리 비트 : 00)

11.8 컨볼루션 부호



[그림 11-22] 다섯 개의 비트를 복호화하는 비터비 알고리즘 마지막 단계(꼬리 비트 : 00)

Q & A

수고하셨습니다.