講 座

符號理論의 槪念

巡回符號篇

李 晩 榮
漢陽大學校 敎授

本 誌 2月號에서 講述한 線形符號에 이어 이번號에서는 巡回符號에 對해 記述하고자 한다.

線形블럭符號中 重要한 部類에 屬하는 巡回符號(cyclic code)는 그 內容이 代數的 構造를 갖고 있어 符號化 回路는 勿論 復號에 必要한 誤症(syndrome)計算回路 等 歸還連結이 있는 置換레지스터(shift register)를 使用한 裝置化(implementation)가 매우 容易하다는 利點이 있다. 이런 巡回符號는 散發誤謬(random error)뿐 아니라 連集誤謬(burst error)도 訂正할 수 있는 매우 效果的인 符號로서 多重誤謬訂正能力(multiple error correcting capability)을 갖는 BCH符號도 巡回符號의 一種이다.

Ⅰ. 巡回符號의 定義

(n, k)線形블럭符號 C에서 任意의 符號語를

$\bar{c}^{(0)}=(c_0, c_1, \cdots, c_{n-2}, c_{n-1})$

라 할 때 이것을 順次的으로 한 디지트씩 오른쪽으로 巡回置換(cyclic shift)하면 다음과 같이 된다.

$\bar{c}^{(1)}=(c_{n-1}, c_0, c_1, \cdots, c_{n-3}, c_{n-2})$

그리고 $\bar{c}^{(0)}$를 두 디지트 巡回置換시킨 것은

$\bar{c}^{(2)}=(c_{n-2}, c_{n-1}, c_0, \cdots, c_{n-4}, c_{n-3})$

로 되므로, 一般的으로 $\bar{c}^{(0)}$를 오른쪽으로 i 디지트 順次的으로 巡回置換시킨 $\bar{c}^{(i)}$는 아래와 같이 나타낼 수 있다.

$\bar{c}^{(i)}=(c_{n-i}, c_{n-i+1}, \cdots, c_{n-1}, c_0, c_1, \cdots, c_{n-i-2}, c_{n-i-1})$

이와 같이 符號 C 內의 任意의 符號語 $\bar{c}^{(0)}$를 i番 巡回置換한 $\bar{c}^{(i)}$ 亦是 C 內의 한 符號語가 될 때 이런 符號 C를 巡回符號라 定義한다.

Ⅱ. 巡回符號의 多項式 表現

巡回符號는 그 特性에 依해 多項式으로 表現할 수 있으며, 이 多項式表現(polynomial representation)은 巡回符號의 基礎가 된다.

情報長 k에 檢査長 n−k를 附加한 符號長 n의 符號語를 傳送하는 境遇에 n次元 符號벡터 $\bar{c}=(c_0, c_1, \cdots, c_{n-1})$는 一般的으로 GF(2) 上에서 n−1次 以下의 多項式

$$c(x)=c_0+c_1x+c_2x^2+\cdots+c_{n-1}x^{n-1} \qquad (1)$$

로 나타낼 수 있고, 이 多項式을 符號多項式(code polynomial)이라 부른다. 即, 符號長 n의 2元系列은 n−1次 以下인 符號多項式의 係數로 이루어지며, 1對1 對應關係를 이루는 것이다. 巡回符號 C 內의 모든 符號多項式 中 零을 除外한 最小次數의 多項式을 골라 g(x)라 할 때 모든 符號多項式 c(x)가 g(x)로 나누어 떨어지면 이 多項式 g(x)를 巡回符號 C의 生成多項式(generator polynomial)이라 한다. 따라서 n−1次 以下의 多項式 c(x)가 符號多項式이 되기 爲한 必要 充分條件은 $c(x)=d(x)g(x)$를 滿足하는 多項式 d(x)가 存在하는 것이다.

g(x)를 n−k次의 모닉多項式(monic polynomial)이라 하면 k個의 多項式 g(x), xg(x), $x^2g(x)$, …, $x^{k-1}g(x)$는 各各의 次數가 n−1 以下인 多項式이며, 이들을 線形結合하면

$$\begin{aligned} c(x) &= d_0g(x)+d_1xg(x)+\cdots+d_{k-1}x^{k-1}g(x) \\ &= (d_0+d_1x+\cdots+d_{k-1}x^{k-1})g(x) \\ &= d(x)g(x) \end{aligned} \qquad (2)$$

가 되므로 c(x)는 次數가 n−1 以下이고 g(x)를 因數로 갖는 多項式임을 알 수 있다. 여기서 모닉多項式이란 最高次項의 係數가 "1"인 多項式을 뜻한다.

한편 d(x)의 係數로 이루어진 벡터를 $\bar{d}=(d_0, d_1, \cdots, d_{k-1})$ (여기서 d_i는 "0" 또는 "1"인 2元記號이다.) 라 하면 이것이 符號化하려는 k個의 情報비트가 되므로 c(x)는 符號多項式이 될 것이다. 따라서 情報多項式 d(x)를 符號化한다는 것은 d(x)에 g(x)를 곱하는 것에 不過하며, 2^k個의 情報多項式에 對應되는 2^k個의 符號多項式이 (n, k)線形巡回符號를 形成하게 된다. 이

렇게 生成되는 符號多項式 $c(x)$로부터 모두 2^k個의符號語 $\bar{c}$를 얻을 수 있고, 이 巡回符號는 非組織構造(non-systematic form)를 갖는다.

여기서 生成多項式 $g(x)$의 性質을 다음 네 가지 定理를 通해 알아보자.

定理 1. $g(x)=g_0+g_1x+\cdots+g_{n-k-1}x^{n-k-1}+x^{n-k}$를 符號 C 內에서 零이 아닌 最小次數의 符號多項式이라 하면 이 모닉多項式 $g(x)$는 n−k次 生成多項式이 되며 常數項 g_0는 "1"의 값을 갖는다.

定理 2. (n, k)巡回符號의 生成多項式 $g(x)$는 x^n+1의 因數이다. 即,

$$x^n+1=h(x)g(x) \qquad (3)$$

이 된다.

(3)式에 나타낸 k次 多項式 $h(x)=h_0+h_1x+\cdots+h_kx^k$를 $g(x)$에 依해 生成된 符號 C의 패리티檢査多項式(parity-check polynomial)이라 부르는데 $h(x)$ 亦是 x^n+1의 因數이므로 巡回符號의 生成多項式으로 使用할 수 있다. $h(x)$에 依해 生成되는 $(n, n-k)$巡回符號를 $g(x)$에 依해 生成된 (n, k)巡回符號의 雙對符號(dual code)라 부른다.

定理 3. $x^n+1=g(x)h(x)$에서 $h(x)$는 x^n+1의 因數이므로 $h^*(x)=x^kh(x^{-1})$ 亦是 x^n+1의 因數가 된다. 또한 $h^*(x)$는 (n, k)巡回符號의 雙對符號인 $(n, n-k)$巡回符號를 生成하는 唯一한 生成多項式이 된다.

여기서 $h^*(x)$는 $h(x)$의 相反多項式(reciprocal polynomial)이다.

定理 4. 生成多項式 $g(x)$가 x^n+1의 因數이면 n−1次 以下의 符號多項式 $c(x)$를 한 번 巡回置換한 $c^{(1)}(x)$도 $g(x)$를 因數로 갖는다.

定理 4 로부터 符號多項式 $c(x)$에 x를 곱하고 x^n+1로 나누었을 때 얻는 나머지는 符號語를 한번 巡回置換한 것의 多項式表現이 됨을 알 수 있다. 또 이 나머지 即, 剩餘多項式(remainder polynomial)은 符號多項式 $c(x)$의 係數들을 한번 巡回置換한 것과 同一하다. 이런 事實은 一般的으로 i番의 巡回置換한 境遇에도 適用된다.

例題 1. $(7, 3)$巡回符號의 符號語를 求해보자. 生成多項式 $g(x)$는 x^n+1의 因數이고 次數는 $n-k=4$ 이어야 하므로

$$x^7+1=(1+x)(1+x+x^3)(1+x^2+x^3)$$

에서 $g(x)$는 $1+x+x^2+x^4$ 或은 $1+x^2+x^3+x^4$이 된다. 여기서 $g(x)$의 次數 4는 이 符號의 檢査비트數와 같다. 이제 情報 $\bar{d}=(011)$에 對應되는 符號語를 求해 보자. $\bar{d}=(011)$의 多項式表現 $d(x)=x+x^2$과 $g(x)=1+x+x^2+x^4$을 (2)式에 代入하여

$$c(x)=(x+x^2)(1+x+x^2+x^4)$$
$$=x+x^4+x^5+x^6$$

를 얻을 수 있으며, 이 符號多項式에 該當하는 符號語 $\bar{c}=(0100111)$를 求할 수 있다. 이 符號의 符號語數는 모두 $2^3=8$個인데 이것을 求해 보면 표 1과 같다.

표 1. $g(x)=1+x+x^2+x^4$에 依해 生成되는 $(7, 3)$巡回符號

情報, $\bar{d}$	$d(x)$	$c(x)$
0 0 0	0	0
0 0 1	x^2	$x^2+x^3+x^4+x^6$
0 1 0	x	$x+x^2+x^3+x^5$
0 1 1	$x+x^2$	$x+x^4+x^5+x^6$
1 0 0	1	$1+x+x^2+x^4$
1 0 1	$1+x^2$	$1+x+x^3+x^6$
1 1 0	$1+x$	$1+x^3+x^4+x^5$
1 1 1	$1+x+x^2$	$1+x^2+x^5+x^6$

표 1에서 보는 바와 같이 이 符號는 非組織構造를 가지며 最小距離가 $d_{min}=4$이므로 誤謬訂正能力은 $t=[(d_{min}-1)/2]=1$이다. 여기서 [A]는 A 以下의 最大整數를 表示한다. 따라서 이 符號는 單一誤謬를 訂正할 수 있다.

Ⅲ. 巡回符號의 組織構造

(n, k)巡回符號의 生成多項式 $g(x)$가 주어질 때 符號語의 k個 情報비트와 n−k個 檢査비트를 다음과 같이 組織的으로 配列할 수 있다.

$$\bar{c}=(\gamma_0, \gamma_1, \cdots, \gamma_{n-k-1}, d_0, d_1, \cdots, d_{k-1}) \qquad (4)$$

(4)式으로부터 情報多項式 $d(x)$와 檢査多項式 $\gamma(x)$를 各各 아래와 같이 表現할 수 있으며

$$d(x)=d_0+d_1x+\cdots+d_{k-1}x^{k-1} \qquad (5)$$

$$\gamma(x)=\gamma_0+\gamma_1x+\cdots+\gamma_{n-k-1}x^{n-k-1} \qquad (6)$$

(6)式의 n−k−1次 檢査多項式 $\gamma(x)$는 $x^{n-k}d(x)$를 $g(x)$로 나눈 剩餘多項式이다. 即,

$$x^{n-k}d(x)=q(x)g(x)+\gamma(x) \qquad (7)$$

여기서 $q(x)$를 몫多項式(quotient polynomial)이라 부르며, $g(x)$에 依해 生成되는 巡回符號의 符號多項式은 (7)式을 아래와 같이 再配列함으로써 얻어진다.

$$c(x)=\gamma(x)+x^{n-k}d(x)=q(x)g(x)$$
$$=(\gamma_0+\gamma_1x+\cdots+\gamma_{n-k-1}x^{n-k-1})$$
$$+(d_0x^{n-k}+d_1x^{n-k+1}+\cdots+d_{k-1}x^{n-1}) \qquad (8)$$

이 符號多項式에 對應되는 符號語는

$\bar{c}=(\gamma_0, \gamma_1, \cdots, \gamma_{n-k-1}, d_0, d_1, \cdots, d_{k-1})$

이며 k個 情報비트와 n−k個 檢査비트로 完全히 分離되었으므로 組織構造(systematic form)를 가진 巡回符號임을 알 수 있다.

例題 2. (7, 4)巡回符號의 生成多項式이 $g(x)=1+x+x^3$일 때 16個의 모든 符號語를 組織構造와 非組織構造로 各各 求해 보자. 符號化하려는 情報를 $\bar{d}=(1100)$라 하면, 이의 多項式表現은 $d(x)=1+x$이다.

1. 非組織符號語

(2)式으로부터 符號多項式은

$$\begin{aligned} c(x) &= d(x)g(x) \\ &= (1+x)(1+x+x^3) \\ &= 1+x^2+x^3+x^4 \end{aligned}$$

로 求해지며 이에 對應되는 符號語는 $\bar{c}=(1011100)$이다.

2. 組織符號語

剩餘多項式을 求하기 爲해 $x^3d(x)=x^3(1+x)$를 $g(x)$로 나누면 $\gamma(x)=1+x^2$를 얻는다. 따라서 符號多項式은 (8)式에 依해

$$\begin{aligned} c(x) &= \gamma(x)+x^3d(x) \\ &= 1+x^2+x^3+x^4 \end{aligned}$$

가 되며, 이에 對應되는 符號語는 $\bar{c}=(1011100)$이다.

표 2에는 위의 方法으로 求한 (7, 4)巡回符號의 非組織符號語와 組織符號語를 모두 나타냈다.

표 2. $g(x)=1+x+x^3$에 依해 生成된 (7, 4)巡回符號

情報語	非組織符號語	組織符號語
0 0 0 0	0 0 0 0 0 0 0	0 0 0 0 0 0 0
0 0 0 1	0 0 0 1 1 0 1	1 0 1 0 0 0 1
0 0 1 0	0 0 1 1 0 1 0	1 1 1 0 0 1 0
0 0 1 1	0 0 1 0 1 1 1	0 1 0 0 0 1 1
0 1 0 0	0 1 1 0 1 0 0	0 1 1 0 1 0 0
0 1 0 1	0 1 1 1 0 0 1	1 1 0 0 1 0 1
0 1 1 0	0 1 0 1 1 1 0	1 0 0 0 1 1 0
0 1 1 1	0 1 0 0 0 1 1	0 0 1 0 1 1 1
1 0 0 0	1 1 0 1 0 0 0	1 1 0 1 0 0 0
1 0 0 1	1 1 0 0 1 0 1	0 1 1 1 0 0 1
1 0 1 0	1 1 1 0 0 1 0	0 0 1 1 0 1 0
1 0 1 1	1 1 1 1 1 1 1	1 0 0 1 0 1 1
1 1 0 0	1 0 1 1 1 0 0	1 0 1 1 1 0 0
1 1 0 1	1 0 1 0 0 0 1	0 0 0 1 1 0 1
1 1 1 0	1 0 0 0 1 1 0	0 1 0 1 1 1 0
1 1 1 1	1 0 0 1 0 1 1	1 1 1 1 1 1 1

Ⅳ. 巡回符號의 生成行列과 檢査行列

이제 組織巡回符號에서 生成行列과 檢査行列의 一般的인 表現에 對해 알아 보자.

x^{n-k+1}를 生成多項式 $g(x)$로 나눈 나머지를

$$\gamma_i(x)=\gamma_{i,0}+\gamma_{i,1}x+\gamma_{i,2}x^2+\cdots+\gamma_{i,n-k-1}x^{n-k-1} \tag{9}$$

라 하면 다음 式이 成立된다.

$$x^{n-k+1}=q_i(x)g(x)+\gamma_i(x),\ i=0, 1, \cdots, k-1 \tag{10}$$

여기서 $\gamma_i(x)$는 剩餘多項式이며 n−k−1次의 檢査多項式과 같다. (10)式을 다음과 같이 表現하면 이 式은 符號多項式임이 分明하다.

$$c_i(x)=q_i(x)g(x)=\gamma_i(x)+x^{n-k+1},\quad i=0, 1, \cdots, k-1 \tag{11}$$

各 符號多項式은 그에 該當하는 符號語와 1對1 對應되므로 다음과 같은 結果를 얻을 수 있다.

符號多項式

$$\begin{aligned} c_0(x) &= \gamma_0(x) + x^{n-k} \\ c_1(x) &= \gamma_1(x) + x^{n-k+1} \\ &\vdots \\ c_{k-1}(x) &= \gamma_{k-1}(x)+x^{n-1} \end{aligned}$$

符 號 語

$$\begin{aligned} \bar{c}_0 &= (\gamma_{00}, \gamma_{01}, \cdots, \gamma_{0,n-k-1}, 1\ 0\ 0 \cdots 0) \\ \bar{c}_1 &= (\gamma_{10}, \gamma_{11}, \cdots, \gamma_{1,n-k-1}, 0\ 1\ 0 \cdots 0) \\ &\vdots \\ \bar{c}_{k-1} &= (\gamma_{k-1,0}, \gamma_{k-1,1}, \cdots, \gamma_{k-1,n-k-1}, 0\ 0\ 0 \cdots 1) \end{aligned}$$

그리고 k個의 符號多項式에 對應되는 k個의 n 次元벡터를 k×n行列의 行으로 使用하면 符號 C의 一般的인 組織形 生成行列(generator matrix)表現이 얻어진다.

$$\bar{G}=\begin{bmatrix}\bar{c}_0\\ \bar{c}_1\\ \vdots\\ \bar{c}_{k-1}\end{bmatrix}=\begin{bmatrix}\gamma_{00} & \gamma_{01} & \cdots & \gamma_{0,n-k-1} & 1\ 0\ 0 \cdots 0\\ \gamma_{10} & \gamma_{11} & \cdots & \gamma_{1,n-k-1} & 0\ 1\ 0 \cdots 0\\ & & \vdots & & \\ \gamma_{k-1,0} & \gamma_{k-1,1} & \cdots & \gamma_{k-1,n-k-1} & 0\ 0\ 0 \cdots 1\end{bmatrix}=[\bar{\Gamma}_{k\times(n-k)} \vdots \bar{I}_k] \tag{12}$$

또 (12)式으로부터 組織巡回符號의 檢査行列(parity-check matrix)은 다음과 같이 求해 진다.

$$\bar{H}=[\bar{I}_{n-k} \vdots \bar{\Gamma}^T_{k\times(n-k)}]=\begin{bmatrix}1\ 0\ 0 \cdots 0\ \gamma_{00} & \gamma_{10} & \cdots \gamma_{k-1,0}\\ 0\ 1\ 0 \cdots 0\ \gamma_{01} & \gamma_{11} & \cdots \gamma_{k-1,1}\\ 0\ 0\ 1 \cdots 0\ \gamma_{02} & \gamma_{12} & \cdots \gamma_{k-1,2}\\ & \vdots & \\ 0\ 0\ 0 \cdots 1\ \gamma_{0,n-k-1} & \gamma_{1,n-k-1} & \cdots \gamma_{k-1,n-k-1}\end{bmatrix} \tag{13}$$

例題 3. 生成多項式이 $g(x)=1+x^2+x^3$인 (7, 4) 巡回符號의 生成行列과 檢査行列을 求해 보자. 이

符號는 n=7, k=4이므로 (11)式은

$$c_i(x)=\gamma_i(x)+x^3\cdot x^i=q_i(x)g(x),\ i=0,1,2,3$$

로 되며, 이 式에 i값을 各各 代入함으로써 아래와 같은 結果를 얻는다.

i	x^{3+i}	$\gamma_i(x)$	$c_i(x)=\gamma_i(x)+x^{3+i}$	$\bar{c}_i$
0	x^3	$1+x^2$	$1+x^2+x^3$	1011000
1	x^4	$1+x+x^2$	$1+x+x^2+x^4$	1110100
2	x^5	$1+x$	$1+x+x^5$	1100010
3	x^6	$x+x^2$	$x+x^2+x^6$	0110001

여기서 $\bar{c}_i$를 行列의 各 行으로 羅列하면 生成行列 $\bar{G}$를 求할 수 있고,

$$\bar{G}=\begin{bmatrix}1&0&1&1&0&0&0\\1&1&1&0&1&0&0\\1&1&0&0&0&1&0\\0&1&1&0&0&0&1\end{bmatrix}$$

이로부터 檢査行列 $\bar{H}$는 다음과 같이 求해 진다.

$$\bar{H}=\begin{bmatrix}1&0&0&1&1&1&0\\0&1&0&0&1&1&1\\0&0&1&1&1&0&1\end{bmatrix}$$

巡回符號에서 生成行列과 檢査行列 사이에는 重要한 關係가 있다. 그것은 符號 C가 非組織形 生成行列에 依해 生成되었건, 組織形 生成行列에 依해 生成되었건間에 符號 C의 모든 符號語는 檢査行列 $\bar{H}$의 各 行과 直交(orthogonal)關係에 있다는 것이다. 이런 事實로부터 檢査行列과 生成行列 間에는 다음과 같은 式이 成立되는데

$$\bar{G}\cdot\bar{H}^T=\bar{O} \qquad (14)$$

(12)式과 (13)式을 (14)式에 代入함으로써 이 直交關係를 쉽게 알 수 있을 것이다.

例題 4. 앞의 例題 3에서 求한 (7, 4)巡回符號의 生成行列과 檢査行列을 (14)式에 代入하면

$$\bar{G}\cdot\bar{H}^T=\begin{bmatrix}1&0&1&1&0&0&0\\1&1&1&0&1&0&0\\1&1&0&0&0&1&0\\0&1&1&0&0&0&1\end{bmatrix}\cdot\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\\1&0&1\\1&1&1\\1&1&0\\0&1&1\end{bmatrix}$$

$$=\begin{bmatrix}0&0&0\\0&0&0\\0&0&0\\0&0&0\end{bmatrix}=\bar{O}$$

가 되어 앞에서 說明한 直交關係를 確認할 수 있다.

V. 線形論理回路

주어진 情報를 符號化하는 符號器와 受信벡터를 復號하는 復號器를 裝置化하는 데에는 多項式 演算을 遂行하는 論理回路가 必要하다. 이런 必要性에 비추어, 다음節에서 說明할 符號化過程을 理解하는데 도움이 되는 몇가지 論理回路에 對한 豫備知識을 記述하기로 한다.

[乘算論理回路]

入力으로 들어오는 任意의 多項式 $a(x)=a_0+a_1x+\cdots+a_{k-1}x^{k-1}+a_kx^k$와 特定多項式 $b(x)=b_0+b_1x+\cdots+b_{r-1}x^{r-1}+b_rx^r$을 곱하는 多項式 乘算 論理回路에對해 알아보자.

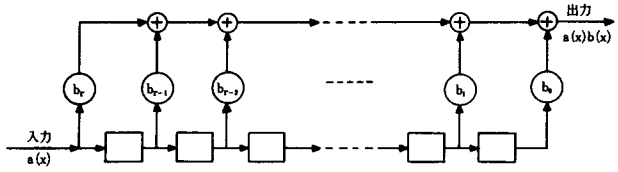

그림 1. 多項式 乘算論理回路(Ⅰ)

이 回路에서 →□→는 置換레지스터(shift register)의 各 段(stage)에 使用되는 플립플롭(filp-flop)을, →⊕→는 2元 加算器(modulo-2 adder)를, →(b_r)→은 b_r의 2元價(binary value) {0, 1}에 따라 回路의 開閉狀態(open or close)를 나타내는 係數器를 各各 意味한다.

外部回路에서 發生되는 클럭펄스(clock pulse)에 依해 乘算論理回路의 入力은 펄스의 發生 瞬間마다 한 비트씩 乘算論理回路 內로 轉移되어, 펄스의 終了瞬間에 各 段의 出力으로 나타난다. 그리고 置換레지스터의 各 段의 初期値는 零이며 入力端에는 a(x)의 最高次項부터 들어간다. a(x)의 最高次項係數 a_k가 置換레지스터로 들어가면 a(x)b(x)의 最高次項係數인 a_kb_r이 出力에 나타나는데 그 瞬間에 置換레지스터 各 段의 出力은 모두 零이다. 置換이 한번 이루어지면 a_{k-1}이 置換레지스터의 入力이 되고, a_k는 첫 段의 出力이 된다. 이 첫 段의 出力을 除外한 모든 段의 出力은 "0"狀態를 維持하며 置換레지스터의 出力은 $a_{k-1}b_r+a_kb_{r-1}$로 되어 a(x)b(x)의 k+r−1 次項 係數가 된다. 이어서 置換이 다시 한번 이루어지면, a_{k-2}가 置換레지스터의 入力이 되고 各 段의 出力은 a_{k-1}, a_k, 0, 0, …, 0가 된다. 이 때 置換레지스터의 出力은

$a_{k-2}b_r+a_{k-1}b_{r-1}+a_kb_{r-2}$이며 이것은 $a(x)b(x)$의 k+r−2 次項 係數가 된다. 이와 같은 方法으로 置換이 r번 이루어지면 a_k가 置換레지스터의 마지막 段 出力으로 나타나며, r+k−1番 置換이 이루어지면 a_1이 마지막 段의 出力으로 나타나 置換레지스터의 內容은 $0, 0, \cdots, a_0, a_1$이 된다. 이 때 置換레지스터의 出力은 $a_0b_1+a_1b_0$로 $a(x)b(x)$의 1次項 係數가 된다. r+k番의 置換이 이루어진 後, 마지막 段의 出力은 a_0이고 置換레지스터의 內容은 $0, 0, 0, \cdots, a_0$가 된다. 그러므로 置換레지스터의 出力은 a_0b_0이며 이것은 $a(x)b(x)$의 常數項이 된다. 이로써 多項式 乘算이 完結되며 그 結果는 $a(x)$와 $b(x)$를 곱한 多項式으로 다음과 같다.

$$a(x)b(x)=a_0b_0+(a_0b_1+a_1b_0)x+(a_0b_2+a_1b_1+a_2b_0)x^2+\cdots+(a_{k-2}b_r+a_{k-1}b_{r-1}+a_kb_{r-2})x^{k+r-2}+(a_{k-1}b_r+a_kb_{r-1})x^{k+r-1}+a_kb_rx^{k+r}$$

即, 入力系列$(a_0, a_1, \cdots, a_{k-1}, a_k)$에 對해 出力系列로서$(a_0b_0, a_0b_1+a_1b_0, \cdots, a_{k-1}b_r+a_kb_{r-1}, a_kb_r)$이 나타나게 되는 것이다.

至今까지 說明한, 乘算을 遂行하는 乘算論理回路 의 一例로서 入力多項式 $a(x)=a_0+a_1x+a_2x^2+a_3x^3+a_4x^4$를 特定多項式 $b(x)=b_0+b_1x+b_2x^2+b_3x^3$에 곱하는 回路를 그림 2에 圖示하였으며 置換에 따른 이 乘算論理回路의 作動을 順次的으로 표 3에 나타냈다.

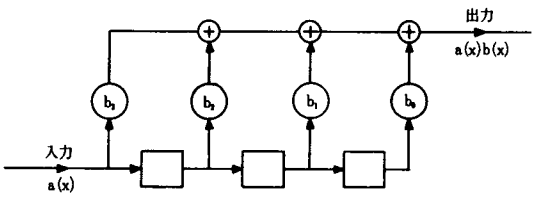

그림 2. 特定 多項式 $b(x)=b_0+b_1x+b_2x^2+b_3x^3$에 依한 乘算論理回路

표 3. 그림 2에 나타낸 乘算論理回路의 段階的 作動

置換回數	i回 置換 後의		
i	入力	置換레지스터內容	出力
0	a_4	0 0 0	a_4b_3
1	a_3	a_4 0 0	$a_3b_3+a_4b_2$
2	a_2	a_3 a_4 0	$a_2b_3+a_3b_2+a_4b_1$
3	a_1	a_2 a_3 a_4	$a_1b_3+a_2b_2+a_3b_1+a_4b_0$
4	a_0	a_1 a_2 a_3	$a_0b_3+a_1b_2+a_2b_1+a_3b_0$
5	0	a_0 a_1 a_2	$a_0b_2+a_1b_1+a_2b_0$
6	0	0 a_0 a_1	$a_0b_1+a_1b_0$
7	0	0 0 a_0	a_0b_0

例題 5. GF(2) 上에서 入力多項式 $a(x)=1+x^2+x^4$를 特定多項式 $b(x)=1+x+x^3$에 곱하는 乘算論理回路와 이 回路의 作動을 생각해 보자.

먼저 두 多項式을 곱하면

$$a(x)b(x)=(1+x^2+x^4)(1+x+x^3)=1+x+x^2+x^4+x^7$$

로 되며, 이 式으로부터 入力系列이 (10101)일 때 乘算論理回路를 거친 出力系列은 (11101001)이 되어야 함을 알 수 있다.

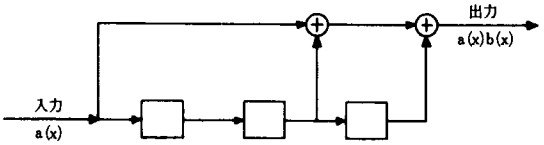

그림 3. 特定 多項式 $b(x)=1+x+x^3$에 依한 乘算論理回路

그리고 乘算論理回路는 그림 3과 같으며 이 乘算論理回路의 作動은 표 4와 같이 이루어 진다.

표 4. 그림 3에 나타낸 乘算論理回路의 段階的 作動

置換回數	i回 置換後의		
i	入力	置換레지스터內容	出力
0	1	0 0 0	1
1	0	1 0 0	0
2	1	0 1 0	0
3	0	1 0 1	1
4	1	0 1 0	0
5	0	1 0 1	1
6	0	0 1 0	1
7	0	0 0 1	1

그림 4는 또다른 方法에 依한 乘算論理回路를 나타낸 것이다. 이 乘算論理回路에서는 乘算에 따른 係數들이 그림 1의 回路와는 달리 置換레지스터 內에서 形成된다.

入力벡터가 $\bar{a}=(a_0, a_1, \cdots, a_{k-1}, a_k)$이므로 $a(x)$ 의 最高次項 係數 a_k가 入力端을 通해 들어가는 瞬間, 出力端에는 a_kb_r이 即時 나타난다. 이때 置換레지스터 各 段의 出力은 모두 "0"이다. 置換이 한번 일어나면 入力에 a_{k-1}이 들어감과 同時에 出力端에는 $a(x)b(x)$의 k+r−1次項 係數인 $a_kb_{r-1}+a_{k-1}b_r$이 나타나며, 이

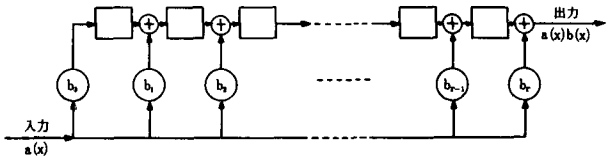

그림 4. 多項式 乘算論理回路(Ⅱ)

때 各 段의 出力은 $a_kb_0, a_kb_1, a_kb_2, \cdots, a_kb_{r-2}, a_kb_{r-1}$ 이 된다. 置換이 두번 이루어졌을 때 入力端에는 a_{k-2} 가 들어가며 各 段의 出力은 $a_{k-1}b_0, a_kb_0+a_{k-1}b_1, a_kb_1+a_{k-1}b_2, \cdots, a_kb_{r-2}+a_{k-1}b_{r-1}$ 이 된다. 따라서 出力端에는 a(x)b(x)의 k+r−2次項 係數인 $a_kb_{r-2}+a_{k-1}b_{r-1}+a_{k-2}b_r$ 이 나타난다. 이와 같은 作動은 a(x)b(x) 의 常數인 a_0b_0 가 出力端에 나타날 때까지 繼續되며, 乘算의 結果로서 a(x)b(x)에 對한 모든 項의 係數들을 求할 수 있다.

例題 6. GF(2) 上에서 入力多項式 $a(x)=1+x^2+x^4$ 를 $b(x)=1+x+x^2$에 곱하는 乘算論理回路를 위에서 說明한 方式으로 構成하면 그림 5 와 같이 되며 이 回路의 作動을 표 5 에 順次的으로 나타냈다.

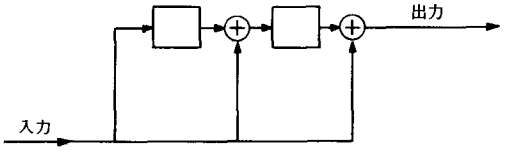

그림 5. 特定多項式 $b(x)=1+x+x^2$ 에 依한 乘算論理回路

표 5. 乘算論理回路의 順次的 作動

置換回數	i回 置換後의		
i	入力	置換레지스터內容	出力
0	1	0 0	1
1	0	1 1	1
2	1	0 1	0
3	0	1 1	1
4	1	0 1	0
5	0	1 1	1
6	0	0 0	1

[除算論理回路]

그림 6 은 GF(q) 上에서 任意의 多項式 $a(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n$ 를 特定多項式 $b(x)=b_0+b_1x+b_2x^2+\cdots+b_rx^r$ 로 나누는 除算論理回路이다.

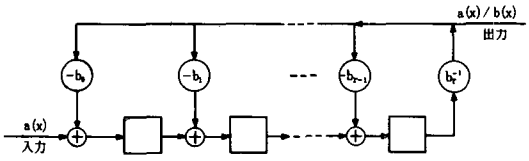

그림 6. 多項式 除算論理回路

置換레지스터 各 段의 初期內容은 모두 "0"이며, 이 回路의 出力은 r回의 置換이 일어날 때까지, 即 入力의 첫번 記號가 置換레지스터의 마지막 段에 이를 때까지는 "0"이다. 이렇게 r番의 置換이 일어난 後, 最初의 "0"이 아닌 出力은 $a_nb_r^{-1}$ 이며 이것이 除算에 依한 몫(quotient)의 첫번 係數가 된다. 몫의 各 係數 q_i 에 對한 多項式 $q_ib(x)$는 被除多項式(dividend polynomial)으로부터 減算되어야 하며, 이와 같은 減算은 除算論理回路의 歸還(feedback)에 依해 이루어진다. n+1番의 置換이 이루어지면 出力端에는 完全한 몫이 나타나게 되며, 나머지(remainder)는 置換레지스터 各 段의 內容으로서 形成된다. 除算論理回路의 作動過程을 다음 例題를 通해 살펴보자.

例題 7. GF(2) 上에서 入力多項式 $a(x)=1+x^2+x^4$ 를 $b(x)=1+x+x^2$로 나누는 除算論理回路는 그림 7 과 같으며 이 回路의 作動을 표 6에서 順次的으로 說明하였다.

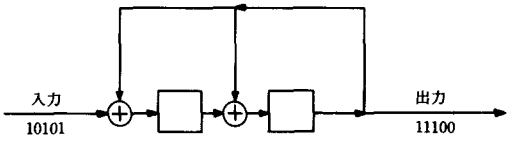

그림 7. $b(x)=1+x+x^2$ 에 依한 除算論理回路

표 6. 그림 7 에 나타낸 除算論理回路의 順次的 作動

置換回數	i回 置換後의		歸還	
i	入力	레지스터內容	歸還	出力
0	1	0 0	0 0	0
1	0	1 0	0 0	0
2	1	0 1	1 1	1
3	0	0 1	1 1	1
4	1	1 1	1 1	1
5	0	0 0	0 0	0

몫의 係數는 最高次의 係數부터 나타나며, 이 例題의 境遇에는 몫의 最高次項인 x^2의 係數 "1"이 두번 置換이 일어난 後 出力端에 나타난다. 完全한 몫은 4番의 置換이 일어나는 동안 出力端에 나타나며 除算의 結果로 생긴 나머지는 置換레지스터의 內容으로 形成된다.

[乘除算論理回路]

그림 8은 入力多項式 $a(x)=a_0+a_1x+\cdots+a_{k-1}x^{k-1}+a_kx^k$에 乘多項式 $b(x)=b_0+b_1x+\cdots+b_rx^r$을 곱하고 그와 同時에 除多項式 $c(x)=c_0+c_1x+\cdots+c_rx^r$로 나누는 乘除算論理回路이다.

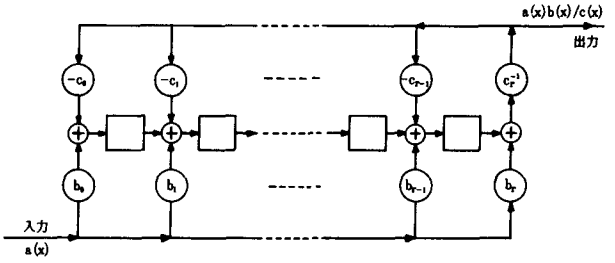

그림 8. 乘多項式 b(x)와 除多項式 c(x)에 依한 乘除算論理回路

이 乘除算論理回路는 그림 4의 乘算論理回路와 그림 6의 除算論理回路를 結合시킨 것이며, 注意해야 할 點은 乘除算論理回路에서 乘多項式 b(x)의 次數가 除多項式 c(x)의 次數보다 크지 않아야한다는 것이다.

例題 8. 入力多項式이 $a(x)=1+x^2+x^4$이고, 乘多項式이 $b(x)=1+x^2$이며, 除多項式이 $c(x)=1+x+x^2$ 인 乘除算論理回路에 對해 알아보자.

먼저, 入力多項式 a(x)에 乘多項式 b(x)를 곱하면

$$a(x)b(x)=(1+x^2+x^4)(1+x^2)$$
$$=1+x^6$$

가 되고, 이것을 다시 除多項式 c(x)로 나누면

$$a(x)b(x)/c(x)=(1+x^6)/(1+x+x^2)$$

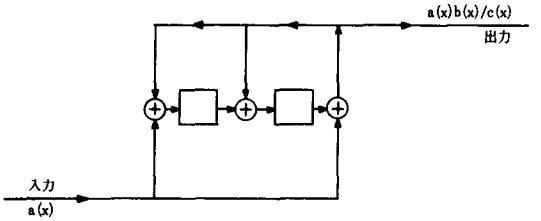

그림 9. 乘多項式 $b(x)=1+x^2$와 除多項式 $c(x)=1+x+x^2$에 依한 乘除算論理回路

$$=1+x+x^3+x^4$$

이 된다. 即, 이 除算의 結果 몫은 $1+x+x^3+x^4$ 이며 剩餘는 없다. 그림 9는 위의 多項式들에 基礎를 둔 乘除算論理回路이며 이 回路의 順次的 作動은 표 7과 같다.

표 7. 그림 9에 나타낸 乘除算論理回路의 順次的 作動

置換回數	i回 置換後의			
i	入力	置換레지스터內容	歸還	出力
0	1	0 0	1 1	1
1	0	0 1	1 1	1
2	1	1 1	0 0	0
3	0	1 1	1 1	1
4	1	1 0	1 1	1
5	0	0 0	0 0	0

Ⅵ. 符 號 化

이제 k個 디지트의 情報를 n個 디지트의 符號語로 만드는 符號化에 對해 알아보자. 주어진 情報를 符號化하는 方法에는 두가지 方式이 있는데 하나는 k段의 置換레지스터를 利用하는 方法이며, 다른 하나는 n−k段의 置換레지스터를 利用하는 方法이다. 一般的으로 檢査비트數가 情報비트數보다 많은 符號에서는 앞의 符號化 方法이 效率的이고 $k/n>1/2$인 境遇, 即, 情報비트數가 檢査비트數보다 많은 境遇에는 뒤의 方法이 經濟的이다. 그러나 어느 方法을 使用하더라도 하나의 情報에 對해서는 同一한 符號語가 만들어진다.

[方法 I]

n−k次 生成多項式 g(x)에 依해 生成되는 (n, k) 巡回符號의 符號化는 $h(x)=(x^n+1)/g(x)$의 關係式에 基礎를 두고 構成되는 k段 置換레지스터를 使用함으로써 이루어질 수 있다. k段 置換레지스터에 k비트의 情報를 入力시키면 直接 傳送路로 빠져나감과 同時에 置換레지스터의 各 段에 順次的으로 蓄積된다. 蓄積이 完了되고나면 乘算論理에 依해 檢査비트가 生成되어 傳送路로 送出됨으로써 組織構造를 갖는 하나의 完全한 n次元 符號語가 만들어진다.

定理 5. $h(x)=\sum_{i=0}^{k}h_ix^i$, $h_0=h_k=1$, 가 x^n+1의 因數이므로 h(x)와 符號多項式 $c(x)=\sum_{i=0}^{n-1}c_ix^i$의 곱은 $c(x)h(x)=q(x)(x^n+1)$이 된다. 여기서 左邊의 c(x)h(x)를 展開하면 다음과 같은 差分方程式(difference equation)을 얻는다.

$$c_{n-k-j}=\sum_{i=0}^{k-1}h_ic_{n-i-j},\quad 1\leqq j\leqq n-k \qquad (15)$$

多項式 h(x)는 生成多項式 g(x)에 依해 만들어지는 巡回符號의 패리티 檢査多項式이며 (15)式을 基礎로 한 符號器는 그림10과 같다.

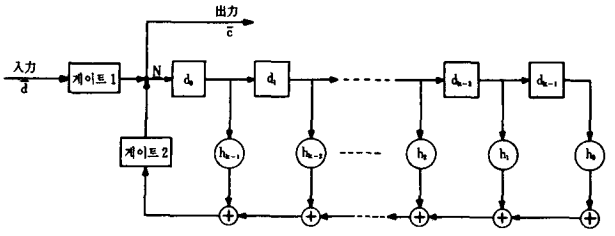

그림10. k段 置換레지스터를 使用한 符號器

符號벡터 $\bar{c}$의 組織形態는

$$\bar{c}=(c_0, c_1, c_2, \cdots, c_{n-k-1}, c_{n-k}, c_{n-k+1}, \cdots, c_{n-1})$$
$$=(\gamma_0, \gamma_1, \gamma_2, \cdots, \gamma_{n-k-1}, d_0, d_1, \cdots, d_{k-1})$$

(n−k個 檢査비트 — k個 情報비트)

이며 k個의 情報비트가 符號器의 入力이 된다. 그림 10의 符號器가 符號化하는 過程을 살펴보면 다음과 같다.

게이트 1이 "ON"狀態, 게이트 2는 "OFF"狀態일 때 情報 $\bar{d}=(d_0, d_1, \cdots, d_{k-1})$가 한 비트씩 k段 置換레지스터에 入力됨과 동시에 傳送路(channel)로 送出된다. k個의 情報비트가 置換레지스터의 各 段에 모두 入力되면 게이트 1은 "OFF"狀態, 게이트 2는 "ON"狀態로 轉換되며 이와 同時에 첫번째 檢査비트

$$c_{n-k-1}=h_0d_{k-1}+h_1d_{k-2}+\cdots+h_{k-2}d_1+h_{k-1}d_0$$
$$=h_0c_{n-1}+h_1c_{n-2}+\cdots+h_{k-2}c_{n-k+1}+h_{k-1}c_{n-k}$$

가 節點(node) N에 나타난다.

다시 한번 置換이 일어나면 첫번째 檢査비트 c_{n-k-1}이 置換레지스터의 첫 段으로 入力됨과 同時에 傳送路로 옮겨진다. 이 瞬間 두 번째 檢査비트

$$c_{n-k-2}=h_0d_{k-2}+h_1d_{k-3}+\cdots+h_{k-2}d_0+h_{k-1}c_{n-k-1}$$
$$=h_0c_{n-2}+h_1c_{n-3}+\cdots+h_{k-1}c_{n-k-1}$$

가 節點N에 나타나게 된다. 이와 같은 作動이 繼續되어 n−k個의 檢査비트가 모두 傳送路로 빠져 나가고 나면 自動的으로 게이트 1은 "ON"狀態, 게이트 2는 "OFF"狀態로 轉換되어 다음 情報블럭이 置換레지스터에 入力된다.

例題 9. 生成多項式이 $g(x)=1+x^2+x^3$ 이고 패리티 檢査多項式이 $h(x)=(x^7+1)/(1+x^2+x^3)=1+x^2+x^3+x^4$인 (7, 4)巡回符號의 符號器는 h(x)의 係數 $h_0=1$, $h_1=0$, $h_2=h_3=h_4=1$에 따라 그림11과 같이 된다.

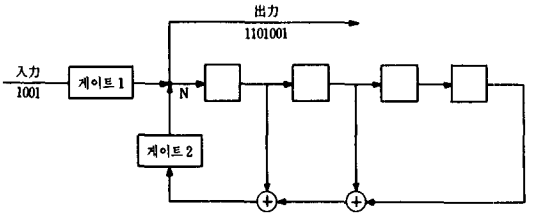

그림11. $h(x)=1+x^2+x^3+x^4$인 (7, 4)巡回符號의 符號器

符號長이 7인 符號벡터의 一般的 表現은

$$\bar{c}=(c_0, c_1, c_2, c_3, c_4, c_5, c_6)$$

로서 右側 4個 디지트는 情報비트이고, 左側 3個 디지트는 檢査비트이다. 이 符號의 檢査비트를 求하는 差分方程式은 (15)式에 依해

$$c_{3-j}=\sum_{i=0}^{3}h_ic_{7-i-j},\ 1\leq j\leq 3$$
$$=h_0c_{7-j}+h_1c_{6-j}+h_2c_{5-j}+h_3c_{4-j}$$
$$=c_{7-j}+c_{5-j}+c_{4-j}$$

가 되며 符號化할 情報를 $\bar{d}=(1001)$이라 하면 $c_3=1$, $c_4=c_5=0$, $c_6=1$이 된다. 따라서 첫 번째 檢査비트는

$$c_2=c_6+c_4+c_3,\ j=1$$
$$=1+0+1$$
$$=0$$

이고, 두 번째 檢査비트는

$$c_1=c_5+c_3+c_2,\ j=2$$
$$=0+1+0$$
$$=1$$

이며, 끝으로 세 번째 檢査비트는 다음과 같이 된다.

$$c_0=c_4+c_2+c_1,\ j=3$$
$$=0+0+1$$
$$=1$$

그러므로 情報 $\bar{d}=(1001)$에 對應되는 符號語는 $\bar{c}=(1101001)$이 되는데, 이 結果를 例題 2에서 說明한 方法을 使用하여 檢討해 보자.

(7)式과 (8)式으로부터 符號多項式은 $c(x)=\gamma(x)+x^{n-k}d(x)$로 나타내어지며, 情報벡터 $\bar{d}=(1001)$을 多項式으로 表現하면 $d(x)=1+x^3$이므로 $x^3d(x)=x^3+x^6$이 된다. 檢査多項式 $\gamma(x)$를 求하기 爲해 $x^3d(x)$를 生成多項式 g(x)로 나누면 $\gamma(x)=1+x$로 되므로 符號多項式은 $c(x)=1+x+x^3+x^6$로 求해지며, 이에 對應되는 符號語는 $\bar{c}=(11011001)$이 된다. 이 符號語는 符號器를 使用하여 求한 符號語와 正確히 一致됨을 알 수 있다.

표8에는 讀者들의 보다 빠른 理解를 돕기 爲하여 그림11에 圖示한 符號器를 使用한 符號化過程을 順次的으로 나타냈는데 置換레지스터 各 段의 初期狀態는 모두 零에서 始作하였다.

표 8. 그림11에 나타낸 符號器의 符號化過程

置換回數	게이트狀態		i回 置換後의		
i	게이트1	게이트2	置換레지스터內容	節點N	出力
0	ON	OFF	0 0 0 0	1	1
1	ON	OFF	1 0 0 0	0	01
2	ON	OFF	0 1 0 0	0	001
3	ON	OFF	0 0 1 0	1	1001
4	OFF	ON	1 0 0 1	0	01001
5	OFF	ON	0 1 0 0	1	101001
6	OFF	ON	1 0 1 0	1	1101001
7	ON	OFF	1 1 0 1	*	*1101001
8	ON	OFF	*1 1 0		

다음 情報블럭의 첫번째 비트

[方法Ⅱ]

k비트의 情報블럭을 n비트의 符號語로 符號化하는 두 번째 方法으로 n−k段 置換레지스터를 使用하는 方法이 있다. 이 方法은 檢査비트를 決定하기 爲해 $x^{n-k}d(x)$를 g(x)로 나눈 剩餘多項式 $\gamma(x)$를 求하는 것이며, 檢査비트數가 情報비트數보다 적은 符號에 對하여 裝置化에 드는 費用을 節約할 수 있는 利點이 있다. 그림12는 n−k段 置換레지스터를 使用한 (n, k)巡回符號의 符號器이다.

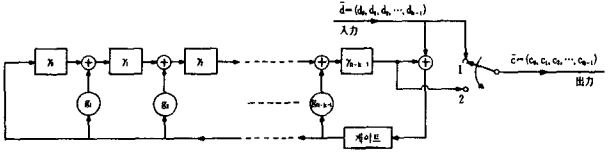

그림12. n−k段 置換레지스터를 使用한 (n, k) 巡回符號의 符號器

이 符號器의 作動은 다음의 過程으로 이루어진다. 게이트를 "ON"狀態로 하고 스위치를 端子 1에 놓으면 情報語 $\bar{d}=(d_0, d_1, \cdots, d_{k-1})$가 回路內로 入力됨과 同時에 傳送路로 送出된다. k個의 情報비트가 置換레지스터에 모두 入力되고 나면 置換레지스터 各 段의 狀態는 $\gamma(x)$의 係數 即, 檢査비트 $\bar{\gamma}=(\gamma_0, \gamma_1, \cdots, \gamma_{n-k-1})$를 나타나게 되며, 게이트를 "OFF"狀態로 하고 스위치를 端子 2로 傳換시키면 情報 $\bar{d}$에 이어서 檢査비트 $\bar{\gamma}$가 傳送路로 送出된다. 이렇게 함으로써 情報語 $\bar{d}$에 對한 符號語가 만들어진다. 이 符號化過程을 다음 例題를 通하여 仔細히 알아보기로 하자.

例題10. $g(x)=1+x^2+x^3$을 生成多項式으로 갖는 (7, 4)巡回符號의 符號器를 생각해보자. 生成多項式의 係數 $g_0=1, g_1=0, g_2=g_3=1$에 따른 係數器를 挿入한 符號器는 그림13과 같으며 符號化하려는 情報가 $\bar{d}=(1001)$일 때 이 符號器의 順次的 作動은 표9와 같다.

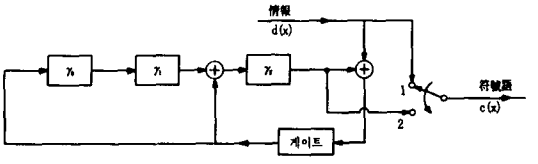

그림13. $g(x)=1+x^2+x^3$인 (7, 4)巡回符號의 符號器

표 9. 그림13에 나타낸 符號器의 符號化 過程

置換回數	게이트	i回 置換 後의	
i	狀態	置換레지스터內容	出力
0	ON	0 0 0	1
1	ON	1 0 1	0 1
2	ON	1 1 1	0 0 1
3	ON	1 1 0	1 0 0 1
4	OFF	1 1 0	0 1 0 0 1
5	OFF	0 1 1	1 0 1 0 0 1
6	OFF	0 0 1	1 1 0 1 0 0 1
7	ON	0 0 0	*1 1 0 1 0 0 1

다음 情報블럭의 첫번째 비트

Ⅶ. 巡回符號의 誤症

巡回符號는 誤謬를 檢出하는데 適切한 構造를 가지고 있어서, 誤謬가 어떤 形態(連集 또는 散發)이더라도 그 誤謬를 檢出및 訂正하는데 使用할 수 있도록 符號化回路및 誤症計算回路를 裝置化하는 것이 容易한 長點이 있다.

一般的으로, 受信벡터는 傳送路 上에서 雜音의 干涉如何에 따라 傳送된 符號벡터와 같을 수도 있고 다를 수도 있다. c(x)를 傳送된 符號多項式, r(x)를 受信된 符號多項式이라 할 때 r(x)를 生成多項式 g(x)로 나누면

$$r(x)=q(x)g(x)+s(x) \qquad (16)$$

로 表示된다. 여기서 q(x)는 몫이고 s(x)는 나머지이

며 s(x)의 次數는 g(x)의 次數보다 낮은 n−k−1 以下이다. 이 s(x)를 誤症(syndrome)이라 부른다. 誤症이 零일 때 即 s(x)=0일 때에는 r(x)가 g(x) 의 倍數가 되어 r(x)=c(x)로서 受信벡터는 誤謬가 存在하지 않은 傳送벡터와 一致한다. 그러나 s(x)≠0 일 때에는 傳送벡터에 誤謬가 發生한 境遇이며 r(x)≠c(x)가 되어 r(x)는 傳送된 符號多項式이 아니다.

誤症 s(x)의 一般的 表現은 다음 式과 같이 n−k−1 以下의 次數를 갖는 多項式이다.

$$s(x)=s_0+s_1x+\cdots+s_{n-k-1}x^{n-k-1} \qquad (17)$$

(17)式을 基礎로 除算論理回路를 使用하여 誤症計算回路를 構成하면 그림14와 같다.

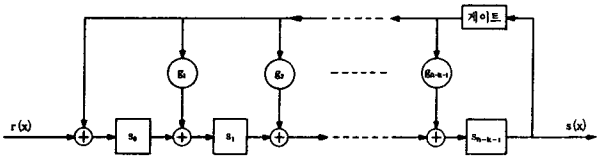

그림14. (n, k)巡回符號의 誤症計算回路

이 回路에서 受信벡터의 모든 디지트가 置換레지스터에 入力되고나면 레지스터의 內容은 誤症을 表示하게 된다. 誤謬多項式을 $e(x)=e_0+e_1x+e_2x^2+\cdots+e_{n-1}x^{n-1}$이라 할 때, 受信多項式은 r(x)=c(x)+e(x)이므로

$$\begin{aligned} e(x)&=c(x)+r(x)\\ &=[d(x)+q(x)]g(x)+s(x) \end{aligned} \qquad (18)$$

가 되어 誤症 s(x)는 誤謬多項式 e(x)를 生成多項式 g(x)로 나눈 나머지임을 알 수 있다. 이와같이 s(x)는 r(x)에 依해 얻어지므로 復號器의 役害은 但只, 誤症 s(x)로부터 誤謬多項式 e(x)를 誘導해 내는 것에 不過하다.

그림15에는 誤症을 計算하고 誤謬를 檢出하여 受信벡터를 訂正하는 一般的인 過程을 圖示하였다.

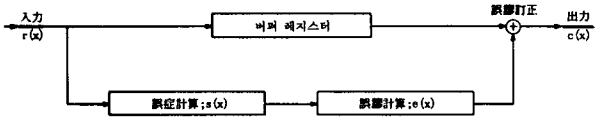

그림15. 誤謬訂正 復號器

例題11. 그림15에 圖示한 一般的인 復號器를 參照하여 生成多項式이 $g(x)=1+x+x^3$인 (7, 4)Hamming 巡回符號의 復號回路를 說計해 보자.

이 符號는 最小距離가 $d_{min}=3$이므로 單一誤謬訂正符號이다. 그리고 7個의 單一誤謬形態가 存在하는데 이것은 모두 線形符號篇에서 說明한 바 있는 標準配列의 剩餘類首로 使用되므로 訂正可能하다. 표10은 單一誤謬形態와 그에 對應되는 誤症을 나타낸 것이다.

표 10. 誤謬形態에 對應하는 誤症

誤謬形態 e(x)	誤 症 s(x)	誤症벡터 (s_0, s_1, s_2)
$e_0(x)=x^0$	$s(x)=1$	(1 0 0)
$e_1(x)=x^1$	$s(x)=x$	(0 1 0)
$e_2(x)=x^2$	$s(x)=x^2$	(0 0 1)
$e_3(x)=x^3$	$s(x)=1+x$	(1 1 0)
$e_4(x)=x^4$	$s(x)=x+x^2$	(0 1 1)
$e_5(x)=x^5$	$s(x)=1+x+x^2$	(1 1 1)
$e_6(x)=x^6$	$s(x)=1+x^2$	(1 0 1)

표10을 基礎로 이 符號의 復號器를 設計하면 그림16과 같다. 그러면 이 復號器의 復號過程을 살펴보기로 하자. 例를 들어 x^6位置에 誤謬가 發生하였다면 誤謬形態는 $e_6(x)=x^6$이 되고 受信係列 r(x)가 誤症生成器에 完全히 入力되는 瞬間 誤症은 (101)이 된다. 따라서 誤謬檢出器의 出力 "1"과 버퍼레지스터의 最右段디지트 r_6를 2元合(modulo-2 sum)하여 訂正이 이루어지는 것이다. 그러나 一般的으로 誤謬가 x^i, $0\le i\le 6$ 位置에 發生했을 때에는 버퍼레지스터와 誤症生成器를 同時에 6−i番 置換시킨 後 訂正한다.

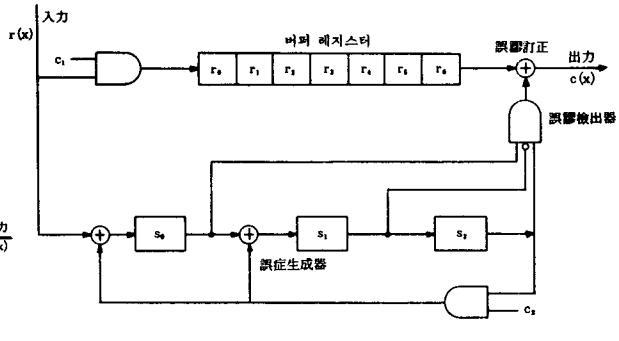

그림16. (7, 4)hamming 巡回符號의 復號回路

Ⅷ. 末 尾 言

本 號에서는 巡回符號와 그 特性, 特히 符號化에 對해서 알아보았다. 巡回符號에는 여러 種類가 있는데 이들은 서로 復號過程과 裝置化에 있어 큰 差異가 있다. 앞에서도 言及했듯이 BCH符號는 多重誤謬를 訂正하는 能力을 갖고 있는 巡回符號로서 符號의 裝置化가 複雜하고 價格이 비싼 것이 缺點이나, 多重散發誤謬를 訂正하는데 最善의 符號로 評價되고 있다. 그리고 非2元 BCH符號인 Reed-Solomon 符號는 鎖狀符號化(concatenated coding)하면 連集誤謬(burst error)를 訂正하는 데 매우 效果的이다.

한편 多數決素子를 使用한 多數決論理復號 符號는 BCH 符號에 比해 誤謬를 訂正하는 能力은 훨씬 떨어지나 復號器의 裝置化가 簡單하고 低廉하다는 利點이 있어서 BCH符號와 함께 宇宙通信 또는 衛星通信 分野를 包含한 通信系 및 電算機系에 널리 應用되고 있다. 多數決論理復號는 一段復號와 多段復號로 나눌 수 있는데 一段多數決論理復號로는 最大長符號와 差集合符號가 있고 多段多數決論理復號에는 Reed-Muller 符號와 有限幾何의 構造的 特性을 利用하여 復號하는 Euclid 幾何學符號, 射影幾何學符號가 있다.

그리고 이 外에 巡回符號의 復號에는 連集誤謬를 訂正하는 Fire符號를 利用한 高速復號器와 散發誤謬를 訂正하는 誤謬捕捉法(error-trapping)等이 있는데 그 內容과 量이 너무나 厖大하므로 本 講述에서는 取及이 不可能하다. 그러나 巡回符號의 復號問題에 關心이 많은 讀者는 電子工學會 1983年度 夏季(Vol. 6 No. 1, pp 3~19) 및 秋季(Vol. 6 No. 2, pp36~58) 綜合學術大會 論文集이나 本人의 著書 "符號理論"(8月 出版 豫定)을 參照하여 符號理論에 對한 一貫性있는 知識을 얻기 바라며 巡回符號에 對한 講述은 이것으로 끝마치고 다음 號에는 至今까지 講述해온 블럭符號(block codes)와는 그 構造 上, 符號化 및 復號에서 根本的으로 差異가 있는 길쌈符號(convolutional codes)에 關해서 講述하도록 하겠다. *

알아둡시다

측방관측 영상 레이다(SLAR)

레이다가 세상에 나타났을 때 애초의 목적은 물체를 검출하는데 있었다. 그러나 그후 기술의 진보는 단순히 검출에만 그치지 않고 그것의 영상화(映像化)에도 성공하였다.

제2차 대전중에 완성한 PPI(plane position indicator)화상이라 불러우는 레이다에서는 일단 해안선이나 산맥을 비쳐 낼 수 있었다. 우리가 지도를 볼 때와 같은 시각적인 파노라마식 화상이다. 그러나 세부까지 분명하게 보이는 것은 아니었다. 당시의 레이다의 분해능력이 그리 좋지 않았기 때문이다.

제2차 대전후 펄스 압축이라는 새로운 기술이 개발되었다. 이것을 사용하면 레이다 전파가 진행하는 방향에는 1m의 차이를 검출할 수 있을 만큼 고도의 거리분해 능력을 가진 화상이 얻어진다. 그래서 이번에는 레이다의 주사방향의 거리와 각도의 분해능력을 높여주자 레이다로써 지도를 그려낼 수 있게 된다. 이 주사방향의 분해능력은 레이다 전파의 주사방향의 비임폭과 관계되어 있기 때문에 안테나의 가로너비가 길수록 분해능력이 좋아진다.

안테나가 회전하는 방식의 레이다에서는 안테나의 크기에도 한도가 있다. 그래서 비행기의 측면을 이용하여 가로로 긴 안테나를 만들고 비행기를 비행시키면서 레이다의 전파비임을 주사하는 방법이라면 어떨까. 이것이라면 주사방향으로도 분해능력이 좋아진다.

이렇게 하여 고안된 기상(機上)용 레이다를 측방관측 영상 레이다 SLAR이라고 말한다. 또 비행기의 길다란 측면을 이용하여도 그래도 똑똑한 화상이 얻어지지 못할 때는 기상에서 얻은 레이다 반사전파를 계산기로 처리하여, 더 선명한 화상을 얻어내는 방법도 있다. 이 방법을 개구합성(開口合成) 레이다 SAR(synthetic aperture rader)라 한다.

높은 곳에 올라가면 전체를 파악할 수 있고 지상에 있을 때와는 색다른 정보를 얻을 수 있다. 비행기나 인공위성에 실려진 영상 레이다는 바다 위의 선박을 관제하는 데는 안성마춤이다. 태양광선과는 달리 레이다 전파는 말하자면 인공광선이다. 낮이건 밤이건, 비가 오건 구름이 있건 언제든지 지표를 관측할 수 있다. 이것이야말로 200해리 경제수역 시대의 슈퍼맨이라고 할 수 있지 않을까. 1978년 6월에 발사된 SEASAT-A 위성의 개구합성 레이다는 고도 800km인 곳으로부터 지상에 있는 25m 이상의 물체를 검출하는 능력을 가졌다.

영상 레이다의 본래의 목적은 전파 항공사진에 의한 지도의 작성이다. 늘 구름에 덮혀있는 적도지대의 정글이나 산악, 일조량이 적은 극지대 등의 지도는 이 전파기술의 덕분으로 말미암아 완성된 것이다. 그리고 현재는 지형, 지질 식생(植生), 수문(水文), 해양, 변난 것으로는 고고학의 연구에도 영상레이다가 적극적으로 이용되고 있다. 그리고 그 분해능력은 10m 이하라 한다.