$[7, k]$ RS 부호와 $[21, 3k]$ 이진 순회 부호의 대응 관계

*최 기 훈, **염 창 열, *김 정 헌, *송 홍 엽

*연세대학교 전기전자공학과, **한국전산원

발표자 : 최 기 훈 (khchoi@eve.yonsei.ac.kr)

▶발표 순서

1. 서론
2. 대응시키는 방법
3. $[7, k]$ RS 부호의 $[21, 3k]$ 이진순회 부호로의 대응
4. 결론

1. 서론

▶ Multilevel 전송, 연집 오류 정정이 필요한 경우

⇒ $GF(2^m)$ 위에서의 비이진 심볼로 구성된 부호를 사용

(ex. $GF(2^m)$에서의 $[n, k]$ RS 부호)

▶ 대부분의 부호기와 복호기

⇒ 이진 심볼에서 작동

(ex. $[mn, mk]$ 이진 부호)

☞ 따라서 이러한 비이진 부호를 이진 부호로 대응시키는 방법을 생각

($GF(2^m)$ 위에서의 한 심볼 → $GF(2)$에서 m bit로 표현)

▶ 이진 부호가 만약 순회 부호라면 부호화와 복호화 하는데 shift register 관점에서 매우 효율적

☞ $GF(2^3)$위에서의 $[7, k]$ RS 부호 $\Rightarrow$ $[21, 3k]$ 이진 순회 부호

① $k = 1, 3, 5, 6$: 알려진 경우

② $k = 2, 4$: 알려지지 않은 경우

2. 대응시키는 방법

▶ $GF(2^3)$ 위에서의 한 심볼 → $GF(2)$에서 3 bit로 표현

· 유한체 $GF(2^3)$의 원소를 $GF(2)$ 위의 벡터 형태로 표현

⇒ 원시 다항식 $x^3 + x + 1$을 사용

· 이 유한체 $GF(2^3)$를 $GF(2)$ 위에서의 벡터 공간으로 생각

⇒ 기저 $(\alpha_2, \alpha_1, \alpha_0)$ 존재

· 유한체 $GF(2^3)$의 모든 원소 b

⇒ $b = b_2\alpha_2 + b_1\alpha_1 + b_0\alpha_0$ (단 $b_i \in GF(2)$, $b \in GF(2^3)$)

▶ $[7, k]$ RS 부호 → $[21, 3k]$ 이진 순회 부호

1) $[21, 3k]$ RS 이진 부호

· 길이 7, 정보의 길이 k인 $[7, k]$ RS 부호

· RS 부호의 비이진 심볼을 어떤 기저를 정하여 그 기저에 따라 이진수로 표현

⇒ $[21, 3k]$ RS 이진 부호

2) 새로운 $[21, 3k]$ 이진 부호

· $[7, k]$ RS 부호 : $g(x) = x^d + g_{d-1} x^{d-1} + \cdots + g_1 x + g_0$

· 새로운 $[21, 3k]$ 이진 부호 : $g_i = g'_{2,i}\,\alpha_2 + g'_{1,i}\,\alpha_1 + g'_{0,i}$ 를 사용

$$\Rightarrow \quad g'(y) = y^{3d} + g'_{2,d-1} y^{3d-1} + g'_{1,d-1} y^{3d-2} + g'_{0,d-1} y^{3d-3}$$

$$+ g'_{2,d-2} y^{3d-4} + g'_{1,d-2} y^{3d-5} + g'_{0,d-2} y^{3d-6} + \cdots + g'_{2,0} y^2 + g'_{1,0} y + g'_{0,0}$$

☞ 1)과 2)의 각 이진 부호의 부호어가 서로 일치하고, $g'(y)$가 순회부호의 생성다항식이 되도록 하는 기저를 찾는 문제

(예) [7, 3] RS 부호

· $g(x) = (x+\alpha)(x+\alpha^2)(x+\alpha^3)(x+\alpha^4)$

$= x^4 + \alpha^3 x^3 + x^2 + \alpha x + \alpha^3$

0	000
1	001
α	010
α^3	011

· 기저 (α^2, α, 1)을 이용

⇒ $g'(y) = y^{12} + y^{10} + y^9 + y^6 + y^4 + y + 1$

$= (y+\beta^9)(y+\beta^{18})(y+\beta^{36})$

· $(y+\beta^{15})(y+\beta^{30})(y+\beta^{60})(y+\beta^{57})(y+\beta^{51})(y+\beta^{39})$

· $(y+\beta^{27})(y+\beta^{54})(y+\beta^{45})$

(단 β는 $GF(64)$의 원소로 y^6+y+1의 근)

☞ $g'(y) \mid (y^{21}+1)$ ⇒ 순회 부호

3. $[7, k]$ RS 부호의 $[21, 3k]$ 이진순회 부호로의 대응

① 알려진 경우 ($k = 1, 3, 5, 6$)

k	$g(x)$	기저	$g'(y)$
1	$x^6 + \alpha^4 x^5 + \alpha x^4 + \alpha^5 x^3 + \alpha^2 x^2 + \alpha^6 x +$	$(\alpha^5, \alpha^6, 1)$	$y^{18} + y^{17} + y^{16} + y^{14} + y^{11} + y^{10} + y^9 + y^7 + y^4 + y^3 +$
3	$x^4 + \alpha^3 x^3 + x^2 + \alpha x + \alpha^3$	$(\alpha^2, \alpha, 1)$	$y^{12} + y^{10} + y^9 + y^6 + y^4 + y + 1$
5	$x^2 + \alpha x + \alpha^4$	$(\alpha^6, \alpha, 1)$	$y^6 + y^4 + y^2 + y + 1$
6	$x + \alpha^3$	$(\alpha^2, \alpha, 1)$	$y^3 + y + 1$

② 알려지지 않은 경우 ($k = 2, 4$)

Lemma

mapping ψ :

$[7, I]$ RS 부호 → $[21, 3I]$ 이진 순회 부호

가 존재할 때, 다음과 같은 새로운 mapping Ψ가 존재한다.

mapping Ψ :

$[7, I]$ RS 부호의 dual 부호 → $[21, 3I]$ 이진 순회 부호의 dual 부호

(여기서 새로운 mapping Ψ는 기존의 mapping ψ의 multipliers를 기저로 갖는다.)

i) $k = 2$ ($[7,2]$ RS 부호)

· $[7,2]$ RS 부호와 dual 관계에 있는 $[7,5]$ RS 부호의 대응관계를 이용

☞ mapping ($[7,5] \rightarrow [21,15]$)의 multipliers $(\alpha^2, \alpha, 1)$

$g'(y)$의 차수									대응되는 $g(x)$	multipliers
8	7	6	5	4	3	2	1	0		
		1	0	1	0	1	1	1	$x^2 + \alpha x + \alpha^4$	1
	1	0	1	0	1	1	1	0	$\alpha x^2 + \alpha^2 x + \alpha^5$	α
1	0	1	0	1	1	1	0	0	$\alpha^2 x^2 + \alpha^3 x + \alpha^6$	α^2

⇒ $(\alpha^2, \alpha, 1)$가 $[7,2]$ RS 부호의 $[21,6]$ 이진 순회부호로의 mapping 에서

기저로 사용

ii) $k = 4$ ($[7,4]$ RS 부호)

· $[7,4]$ RS 부호와 dual 관계에 있는 $[7,3]$ RS 부호의 대응관계를 이용

☞ mapping ($[7,3] \rightarrow [21,9]$)의 multipliers ($\alpha^6, \alpha, 1$)

$g'(y)$의 차수															대응되는 $g(x)$	multipliers
14	13	12	11	10	9	8	7	6	5	4	3	2	1	0		
		1	0	1	1	0	0	1	0	1	0	0	1	1	$x^4 + \alpha^3 x^3 + x^2 + \alpha x + \alpha^3$	1
	1	0	1	1	0	0	1	0	1	0	0	1	1	0	$\alpha x^4 + \alpha^4 x^3 + \alpha x^2 + \alpha^2 x +$	α
1	0	1	1	0	0	1	0	1	0	0	1	1	0	0	$\alpha^6 x^4 + \alpha^2 x^3 + \alpha^6 x^2 + x +$	α^6

⇒ $(\alpha^6, \alpha, 1)$가 $[7,4]$ RS 부호의 $[21,12]$ 이진 순회부호로의 mapping 에서

기저로 사용

4. 결론

☞ 모든 정보길이 $k(=1,2,3,4,5,6)$에 대해서 $[7,k]$ RS 부호는 $[21,3k]$ 이진순회 부호로 대응된다.

k	$g(x)$	기저	$g'(y)$
1	$x^6+\alpha^4x^5+\alpha x^4+\alpha^5x^3+\alpha^2x^2+\alpha^6x+$	$(\alpha^5,\alpha^6,1)$	$y^{18}+y^{17}+y^{16}+y^{14}+y^{11}+y^{10}+y^9+y^7+y^4+y^3+$
2	$x^5+\alpha x^4+\alpha x^3+\alpha^3x^2+x+\alpha$	$(\alpha^2,\alpha,1)$	$y^{15}+y^{13}+y^{10}+y^7+y^6+y^3+y+1$
3	$x^4+\alpha^3x^3+x^2+\alpha x+\alpha^3$	$(\alpha^2,\alpha,1)$	$y^{12}+y^{10}+y^9+y^6+y^4+y+1$
4	$x^3+\alpha^3x^2+\alpha^2x+\alpha^4$	$(\alpha^6,\alpha,1)$	$y^9+y^7+y^6+y^5+y^3+y^2+y+1$
5	$x^2+\alpha x+\alpha^4$	$(\alpha^6,\alpha,1)$	$y^6+y^4+y^2+y+1$
6	$x+\alpha^3$	$(\alpha^2,\alpha,1)$	y^3+y+1