

## 연 습 문 제 (5.5)

1. 체  $\mathbb{F}_2$  위의 4 차의 원시다항식  $f(x) = 1 + x + x^4$  에 대하여 동차 선형 점화수열  $\{a_t\} \in \mathcal{Q}(f(x))$  의 초기 상태벡터가  $(1, 1, 1, 1)$  일 때,  $\{a_t\}$  가 주기 15 인 최대주기수열임을 밝히고 그 생성순환마디를 구하여라.

[풀이] (1)  $a_{t+4} = a_t + a_{t+1} \quad (t = 0, 1, 2, \dots)$

$$a_0 = 1, a_1 = 1, a_2 = 1, a_3 = 1,$$

$$a_4 = a_0 + a_1 = 1 + 1 = 0, \quad a_5 = a_1 + a_2 = 1 + 1 = 0,$$

$$a_6 = a_2 + a_3 = 1 + 1 = 0, \quad a_7 = a_3 + a_4 = 1 + 0 = 1,$$

$$a_8 = a_4 + a_5 = 0 + 0 = 0, \quad a_9 = a_5 + a_6 = 0 + 0 = 0,$$

$$a_{10} = a_6 + a_7 = 0 + 1 = 1, \quad a_{11} = a_7 + a_8 = 1 + 0 = 1,$$

$$a_{12} = a_8 + a_9 = 0 + 0 = 0, \quad a_{13} = a_9 + a_{10} = 0 + 1 = 1,$$

$$a_{14} = a_{10} + a_{11} = 1 + 1 = 0,$$

$$a_{15} = a_{11} + a_{12} = 1 + 0 = 1 = a_0,$$

$$a_{16} = a_{12} + a_{13} = 0 + 1 = 1 = a_1,$$

$$a_{17} = a_{13} + a_{14} = 1 + 0 = 1 = a_2,$$

$$a_{18} = a_{14} + a_{15} = 0 + 1 = 1 = a_3$$

따라서  $\{a_t\}$  는 주기 15 인 최대주기수열이고 그 생성순환마디는 다음과 같다.

$$1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0$$

2. 체  $\mathbb{F}_2$  위의 4 차의 원시다항식  $g(x) = 1 + x^3 + x^4$  에 대하여 동차 선형 점화수열  $\{a_t\} \in \mathcal{Q}(g(x))$  의 초기 상태벡터가  $(0, 0, 0, 1)$  일 때,  $\{a_t\}$  는 주기 15 인 최대주기수열임을 밝히고 그 생성순환마디를 구하여라.

[답]

$$0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1$$

3. 체  $\mathbb{F}_2$  위의 다항식  $f(x) = 1 + x + x^5$ 에 대하여 다음 물음에 답하여라.

- (1) 체  $\mathbb{F}_2$  위의 무한수열  $\{a_t\}$ 가  $f(x)$ 를 고유다항식으로 가지는 동차선형 점화수열일 때, 그 초기 상태벡터가  $(0, 0, 0, 0, 1)$ 인 경우에  $\{a_t\}$ 의 주기와 생성순환마디를 구하여라.
- (2)  $f(x)$ 가 체  $\mathbb{F}_2$  위의 원시다항식인지를 판정하여라.

[풀이] (1) 무한수열  $\{a_t\}$ 는 동차선형점화식

$$a_{t+5} = a_t + a_{t+1} \quad (t = 0, 1, 2, \dots)$$

을 만족시키는 동차 선형점화수열이고 다음이 성립한다.

$$\begin{aligned} a_0 &= 0, a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 1 \\ a_5 &= a_0 + a_1 = 0 + 0 = 0, & a_6 &= a_1 + a_2 = 0 + 0 = 0, \\ a_7 &= a_2 + a_3 = 0 + 0 = 0, & a_8 &= a_3 + a_4 = 0 + 1 = 1, \\ a_9 &= a_4 + a_5 = 1 + 0 = 1, & a_{10} &= a_5 + a_6 = 0 + 0 = 0, \\ a_{11} &= a_6 + a_7 = 0 + 0 = 0, & a_{12} &= a_7 + a_8 = 0 + 1 = 1, \\ a_{13} &= a_8 + a_9 = 1 + 1 = 0, & a_{14} &= a_9 + a_{10} = 1 + 0 = 1, \\ a_{15} &= a_{10} + a_{11} = 0 + 0 = 0, & a_{16} &= a_{11} + a_{12} = 0 + 1 = 1, \\ a_{17} &= a_{12} + a_{13} = 1 + 0 = 1, & a_{18} &= a_{13} + a_{14} = 0 + 1 = 1, \\ a_{19} &= a_{14} + a_{15} = 1 + 0 = 1, & a_{20} &= a_{15} + a_{16} = 0 + 1 = 1, \\ a_{21} &= a_{16} + a_{17} = 1 + 1 = 0 = a_0, \\ a_{22} &= a_{17} + a_{18} = 1 + 1 = 0 = a_1, \\ a_{23} &= a_{18} + a_{19} = 1 + 1 = 0 = a_2, \\ a_{24} &= a_{19} + a_{20} = 1 + 1 = 0 = a_3, \\ a_{25} &= a_{20} + a_{21} = 1 + 0 = 1 = a_4 \end{aligned}$$

따라서  $\{a_t\}$ 는 주기 21인 순환수열이고 그 생성순환마디는 다음과 같다.

$$0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1$$

- (2)  $f(x)$ 는 체  $\mathbb{F}_2$  위의 원시다항식이 아니다(정리 5.5.2 참조).

5. 체  $\mathbb{F}_2$  위에서 주기가  $2^6 - 1$  인 최대주기수열을 구하려면, 어떤 조건을 만족시키는 동차 선형점화수열을 구하여야 하는지 말하여라.

[풀이] 체  $\mathbb{F}_2$  위의 6 차의 다항식  $f(x) = 1 + x + x^6$  는 원시다항식이다.

따라서 예를 들어 다음 두 조건을 만족시키는 무한수열  $\{a_t\}$  는 주기  $2^6 - 1$  인 최대주기수열이다.

$$(i) (a_0, a_1, a_2, a_3, a_4, a_5) = (0, 0, 0, 0, 0, 1)$$

$$(ii) a_{t+6} = a_t + a_{t+1} \quad (t = 0, 1, 2, \dots)$$

6. 체  $\mathbb{F}_2$  위의 원시다항식  $f(x) = x^3 + x + 1$  에 정리 5.5.4 를 적용하여 주기  $2^3 - 1$  인 최대주기수열을 구하여라.

[풀이] Galois 체  $\mathbb{F}_{2^3}$  에서  $\alpha$  를  $f(\alpha) = 0$  인 원시원소라고 하면 다음이 성립한다(보기 4.2.4).

$$\mathbb{F}_{2^3} = \{a_0 + a_1 \alpha + a_2 \alpha^2 \mid a_0, a_1, a_2 \in \mathbb{F}_2\}$$

$$f(\alpha) = \alpha^3 + \alpha + 1 = 0 \quad \text{즉} \quad \alpha^3 = 1 + \alpha$$

	$a_0$	$a_1$	$a_2$
$\alpha^0 = 1 + 0\alpha + 0\alpha^2$	1	0	0
$\alpha^1 = 0 + 1\alpha + 0\alpha^2$	0	1	0
$\alpha^2 = 0 + 0\alpha + 1\alpha^2$	0	0	1
$\alpha^3 = 1 + 1\alpha$	1	1	0
$\alpha^4 = 0 + 1\alpha + 1\alpha^2$	0	1	1
$\alpha^5 = 1 + 1\alpha + 1\alpha^2$	1	1	1
$\alpha^6 = 1 + 0\alpha + 1\alpha^2$	1	0	1
$\alpha^7 = 1 = \alpha^0$			

이로부터 다음과 같은 주기  $2^3 - 1$  인 최대주기수열을 얻는다.

$$1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, \dots$$

$$0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, \dots$$

$$0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, \dots$$

## 연 습 문 제 (5.6)

1. 체  $\mathbb{F}_2 = \{0, 1\}$  에서의 무한수열  $\{a_t\}$  가 다항식

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

를 고유다항식으로 가지는 동차 선형점화수열일 때,  $\{a_t\}$  의 초기 상태벡터가  $(a_0, a_1, a_2) = (0, 0, 1)$  인 경우에  $\{a_t\}$  의 최소다항식은  $f(x)$  임을 밝혀라.

[풀이] 정리 5.6.2를 이용하여 증명한다.

체  $\mathbb{F}_2$  위의 다항식

$$f_0(x) = 1 + x + x^2 + x^3$$

이라고 하면,  $f_0(x)$  는  $\{a_t\}$  의 한 고유다항식이고 그 상반다항식은 다음과 같다.

$$f_0^*(x) = 1 + x + x^2 + x^3 = f_0(x)$$

또,  $\{a_t\}$  의 생성함수를  $G(x) = \sum_{t=0}^{\infty} a_t x^t$  이라고 하면 다음이 성립한다.

$$\begin{aligned} f_0^*(x) G(x) &= (1 + x + x^2 + x^3)(0 + 0x + x^2 + a_3x^3 + \cdots) \\ &= x^2 = g_0(x) \end{aligned}$$

$$G(x) = \frac{g_0(x)}{f_0^*(x)} = \frac{x^2}{f_0^*(x)}$$

따라서

$$g_0^*(x) = x^2 g_0\left(\frac{1}{x}\right) = 1$$

이라고 하면,

$$d(x) = \gcd \{f_0(x), g_0^*(x)\} = 1$$

이고 따라서  $\{a_t\}$  의 최소다항식은 다음과 같다.

$$m(x) = \frac{f_0(x)}{d(x)} = f_0(x) = f(x)$$

3. 체  $\mathbb{F}_2$  에서의 무한수열  $\{a_t\}$  가 다항식

$$f(x) = x^4 + x^2 + x$$

를 고유다항식으로 가지는 동차 섬형점화수열일 때,  $\{a_t\}$  의 초기 상태벡터가  $(a_0, a_1, a_2, a_3) = (1, 0, 1, 0)$  인 경우에  $\{a_t\}$  의 최소다항식은  $f(x)$  임을 밝혀라.

[풀이] 체  $\mathbb{F}_2$  위에서 다항식  $f(x)$  는 다음과 같이 기약다항식의 곱으로 인수분해된다.

$$f(x) = x^4 + x^2 + x = x(x^3 + x + 1)$$

그런데,  $\{a_t\}$  는 영수열이 아니므로  $\{a_t\}$  의 최소다항식은 다음 세 다항식 중의 어느 하나와 같다(정리 5.6.1).

$$m_1(x) = x, \quad m_2(x) = x^3 + x + 1, \quad f(x) = x^4 + x^2 + x$$

그리고, 가정에 의하여  $(a_0, a_1, a_2, a_3) = (1, 0, 1, 0)$  이고 또 최소다항식은 고유다항식이기도 하다(정리 5.6.1).

그런데, 최소다항식이  $m_1(x) = x$  이면,

$$a_{t+1} = 0 \cdot a_t \quad (t = 0, 1, 2, \dots)$$

이므로  $a_0 = a_1 = a_2 = a_3 = 0$  으로 되어  $(a_0, a_1, a_2, a_3) = (1, 0, 1, 0)$  이라는 사실에 모순된다.

한편, 최소다항식이  $m_2(x) = x^3 + x + 1$  이면,

$$a_{t+3} = a_t + a_{t+1} \quad (t = 0, 1, 2, \dots)$$

이고  $a_0 = 1, a_1 = 0, a_2 = 1$  이므로

$$a_3 = a_0 + a_1 = 1 + 0 = 1$$

로 되어  $(a_0, a_1, a_2, a_3) = (1, 0, 1, 0)$  에 모순이 생긴다.

따라서  $\{a_t\}$  의 최소다항식은  $f(x) = x^4 + x^2 + x$  이다.

4. 다음과 같은 체  $\mathbb{F}_2$ 에서의 무한수열은 주기 3인 순환수열이다.

$$\{a_t\} : 1, 1, 0, 1, 1, 0, 1, 1, 0, \dots$$

이 순환수열의 최소다항식은  $m(x) = x^2 + x + 1$ 임을 밝혀라.

[풀이] 보기 5.6.3의 기호를 그대로 사영하기로 한다.

이 순환수열의 생성순환마디는  $1, 1, 0$ 이므로, 체  $\mathbb{F}_2$  위에서

$$f_0(x) = x^3 - 1 = x^3 + 1,$$

$$g^*(x) = a_0x^2 + a_1x + a_2 = x^2 + x$$

이고  $f_0(x)$ 와  $g^*(x)$ 의 최대공약수는  $d(x) = x + 1$ 이다.

따라서  $\{a_t\}$ 의 최소다항식  $m(x)$ 는 다음과 같다.

$$m(x) = \frac{x^3 + 1}{d(x)} = x^2 + x + 1$$

$x$	$x^3 \quad +1$	$x^2 + x$	$x$
$+1$	$x^3 + x^2$	$x^2 + x$	
	$x^2 + 1$	$0$	
	$x^2 + x$		
	$x + 1$		

$$\begin{array}{r}
 \phantom{x+1} \overline{x^2 + x + 1} \\
 x+1 \ ) \ x^3 + 1 \\
 \phantom{x+1} \underline{x^3 + x^2} \phantom{+1} \\
 \phantom{x+1} \phantom{x+1} x^2 + 1 \\
 \phantom{x+1} \phantom{x+1} \underline{x^2 + x} \phantom{+1} \\
 \phantom{x+1} \phantom{x+1} \phantom{x+1} x + 1 \\
 \phantom{x+1} \phantom{x+1} \phantom{x+1} \underline{x + 1} \\
 \phantom{x+1} \phantom{x+1} \phantom{x+1} \phantom{x+1} 0
 \end{array}$$

6. 체  $\mathbb{F}_2$  에서 다음 무한수열은 주기 21 인 순환수열이다.

$$0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, \dots$$

이 순환수열의 최소다항식은  $m(x) = x^5 + x + 1$  임을 밝혀라.

[풀이] 보기 5.6.3 의 기호를 그대로 사용하기로 한다.

$$f_0(x) = x^r - 1 = x^{21} - 1 = x^{21} + 1$$

$$\begin{aligned} g^*(x) &= a_0 x^{r-1} + a_1 x^{r-2} + \dots + a_{r-2} x + a_{r-1} \\ &= x^{16} + x^{12} + x^{11} + x^8 + x^6 + x^4 + x^3 + x^2 + x + 1 \end{aligned}$$

$$\begin{aligned} f_0(x) &= x^{21} + 1 \\ &= (x^{16} + x^{12} + x^{11} + x^8 + x^6 + x^4 + x^3 + x^2 + x + 1)(x^5 + x + 1) \\ &= g^*(x)(x^5 + x + 1) \end{aligned}$$

따라서

$$d(x) = \gcd\{f_0(x), g^*(x)\} = g^*(x)$$

이므로, 이 순환수열의 최소다항식은 다음과 같다.

$$m(x) = \frac{x^r - 1}{d(x)} = x^5 + x + 1$$

$$\begin{array}{r} \frac{x^5 + x + 1}{g^*(x) \mid x^{21} + 1} \\ \begin{array}{r} x^{21} + x^{17} + x^{16} + x^{13} + x^{11} + x^9 + x^8 + x^7 + x^6 + x^5 \\ \underline{x^{17} + x^{16} + x^{13} + x^{11} + x^9 + x^8 + x^7 + x^6 + x^5 + 1} \\ x^{17} + x^{13} + x^{12} + x^9 + x^7 + x^5 + x^4 + x^3 + x^2 + x \\ \underline{x^{16} + x^{12} + x^{11} + x^8 + x^6 + x^4 + x^3 + x^2 + x + 1} \\ x^{16} + x^{12} + x^{11} + x^8 + x^6 + x^4 + x^3 + x^2 + x + 1 \\ \underline{\phantom{x^{16} + x^{12} + x^{11} + x^8 + x^6 + x^4 + x^3 + x^2 + x + 1}} \\ 0 \end{array} \end{array}$$







## 연 습 문 제 (5.7)

1. Galois 체  $\mathbb{F}_q$  에서의 동차 선형점화수열  $\{a_t\}$  의 최소다항식이

$$m(x) = b_0 + b_1x + \cdots + b_{k-1}x^{k-1} + x^k, \quad k \geq 1$$

일 때,  $m(0) = b_0 \neq 0$  이면  $\{a_t\}$  는 순환수열임을 증명하여라.

[풀이] 최소다항식  $m(x)$  는  $\{a_t\}$  의 고유다항식이기도 하다(정리 5.6.1).

따라서  $m(0) \neq 0$  일 때, 정리 5.4.8 에 의하여  $\{a_t\}$  는 순환수열이다.

2. Galois 체  $\mathbb{F}_q$  에서의 영수열이 아닌 동차 선형점화수열  $\{a_t\}$  의 최소다항식

이  $m(x)$  일 때 다음이 성립한다.

- (1) 각 정수  $d (\geq 0)$  에 대하여  ${}_d\{a_t\}$  의 최소다항식을  $m_d(x)$  이라고 하면  $m_d(x) \mid m(x)$  이다.  
 (2)  $\{a_t\}$  가 순환수열이면, 각 정수  $d (\geq 0)$  에 대하여  ${}_d\{a_t\}$  의 최소다항식은  $m(x)$  이다.

[풀이] (1) 다항식  $m(x)$  는  $\{a_t\}$  의 고유다항식이기도 하다(정리 5.7.1).

따라서  $\{a_t\} \in \Omega(m(x))$  이므로, 정리 5.3.5 에 의하여 각 정수  $d (\geq 0)$  에 대하여  ${}_d\{a_t\} \in \Omega(m(x))$  이고  ${}_d\{a_t\}$  는 영수열이 아니다.

그러므로  $m(x)$  는  ${}_d\{a_t\}$  의 고유다항식이고 따라서 정리 5.6.1 에 의하여  $m_d(x) \mid m(x)$  이다.

(2) 무한수열  $\{a_t\}$  가 주기  $r$  인 순환수열일 때, 정수  $d (\geq 0)$  에 대하여  $\{b_t\} = {}_d\{a_t\}$  이라 하고  $m_d(x)$  를  $\{b_t\}$  의 최소다항식이라고 하자.

이 때, (1) 에 의하여  $\{b_r\} \in \Omega(m(x))$  이고  $\{b_r\}$  는 영수열이 아니며  $m_d(x) \mid m(x)$  이다

한편,  $d+e$ 가  $r$ 의 배수가 되도록 양의 정수  $e$ 를 택하면, 정리 5.2.4에 의하여

$${}_e\{b_t\} = {}_{d+e}\{a_t\} = {}_0\{a_t\} = \{a_t\}$$

이고 또  $\{b_t\} \in \Omega(m(x))$  이고  $\{b_t\} \neq \{0\}$  이다.

그러므로 (1)에 의하여  $m(x) \mid m_d(x)$  이고, 따라서  $m_d(x) = m(x)$  이다.

3. 체  $\mathbb{F}_2$ 에서의 무한수열  $\{a_t\}$ 가 다항식

$$f(x) = x^4 + x^2 + x$$

를 고유다항식으로 가지는 동차 선형점화수열일 때,  $\{a_t\}$ 의 초기 상태벡터가  $(a_0, a_1, a_2, a_3) = (1, 0, 1, 0)$ 인 경우에 수열  $\{a_t\}$ 의 최소다항식은  $f(x) = x^4 + x^2 + x$ 이다(문제 5.6.3 참조).

이 때, 무한수열  ${}_1\{a_t\}$ 의 최소다항식은

$$m_1(x) = x^3 + x + 1$$

임을 밝혀라.

[풀이] 체  $\mathbb{F}_2$  위에서 다항식  $f(x)$ 는 다음과 같이 기약다항식의 곱으로 인수분해된다.

$$f(x) = x^4 + x^2 + x = x(x^3 + x + 1)$$

이제  $\{b_t\} = {}_1\{a_t\}$ 이라 하고  $m(x)$ 를  $\{b_t\}$ 의 최소다항식이라고 하자.

이 때, 문제 2에 의하여  $m(x) \mid f(x)$ 이므로  $m(x)$ 는 다음 세 다항식 중의 하나가 성립한다.

$$f_1(x) = x,$$

$$f_2(x) = x^3 + x + 1,$$

$$f(x) = x^4 + x^2 + x$$

그런데,  $(b_0, b_1, b_2) = (a_1, a_2, a_3) = (0, 1, 0)$ 이므로  $\{b_t\}$ 는 영수열이 아니다.

한편,  $m(x) = f_1(x) = x$  이라고 가정하면,

$$a_{t+1} = 0 a_t \quad (t = 0, 1, 2, \dots)$$

이므로  $a_0 = a_1 = a_2 = a_3 = 0$  으로 되어 가정에 모순된다.

그런데, 가정에 의하여  $\{a_t\}$  는 동차 선형점화식

$$a_{t+4} = a_{t+1} + a_{t+2} \quad (t = 0, 1, 2, \dots)$$

를 만족시키는 동차 선형점화수열이다. 그리고,

$$b_t = a_{t+1} \quad (t = 0, 1, 2, \dots)$$

이므로  $\{b_t\}$  는 동차 선형점화식

$$b_{t+3} = b_t + b_{t+1} \quad (t = 0, 1, 2, \dots)$$

를 만족시키는 동차 선형점화수열이고 따라서 다항식

$$f_2(x) = x^3 + x + 1$$

는  $\{b_t\}$  의 고유다항식이고 또 체  $\mathbb{F}_2$  위에서  $f_2(x)$  는 기약이다.

따라서  $\{a_t\} = \{b_t\}$  의 최소다항식은 다음과 같다.

$$m_1(x) = f_2(x) = x^3 + x + 1$$

## 연 습 문 제 (5.8)

1. 이진수열  $\{s_t\}$  가 함수

$$f : \mathbb{F}_2^3 \rightarrow \mathbb{F}_2, f(x_0, x_1, x_2) = x_0 + x_1(1 + x_2)$$

를 feedback 함수로 가지는 선형 Shift Register 에 의하여 생성될 때,  $\{s_t\}$  가 만족시키는 선형점화식을 구하여라.

그리고,  $(s_0, s_1, s_2) = (0, 0, 1)$  일 때의  $\{s_t\}$  를 구하여라.

[풀이] (1) 정의에 따라  $s_{t+3} = f(s_t, s_{t+1}, s_{t+2})$  이므로,  $\{s_t\}$  가 만족시키는 선형점화식은 다음과 같다.

$$s_{t+3} = s_t + s_{t+1}(1 + s_{t+2}) \quad (t = 0, 1, 2, \dots)$$

(2) 초기 상태벡터가  $(s_0, s_1, s_2) = (0, 0, 1)$  일 때,

$$s_0 = 0,$$

$$s_1 = 0,$$

$$s_2 = 1,$$

$$s_3 = s_0 + s_1(1 + s_2) = 0 + 0 = 0 = s_0,$$

$$s_4 = s_1 + s_2(1 + s_3) = 1 + (1 + 0) = 0 = s_1,$$

$$s_5 = s_2 + s_3(1 + s_4) = 1 + 0 = 1 = s_2,$$

따라서  $\{s_t\}$  는 다음과 같이 주기가 3 고 생성순환마디가 0, 0, 1 인 순환수열이다.

$$\{s_t\} : 0, 0, 1, 0, 0, 1, 0, 0, 1, \dots$$

2. 체  $\mathbb{F}_3 = \{0, 1, 2\}$  에서의 무한수열  $\{s_t\}$  가 선형함수

$$f : \mathbb{F}_3^3 \rightarrow \mathbb{F}_3, f(x_0, x_1, x_2) = x_0 + x_1 + 2x_2$$

를 feedback 함수로 가지는 선형 Shift Register 에 의하여 생성될 때,  $\{s_t\}$  가 만족시키는 선형점화식과  $(s_0, s_1, s_2) = (0, 0, 1)$  일 때의  $\{s_t\}$  를 구하여라.

$$[\text{풀이}] (1) \quad s_{t+2} = s_t + s_{t+1} + 2s_{t+2} \quad (t = 0, 1, 2, \dots)$$

$$s_0 = 0,$$

$$s_1 = 0,$$

$$s_2 = 1,$$

$$s_3 = s_0 + s_1 + 2s_2 = 0 + 0 + 2 = 2,$$

$$s_4 = s_1 + s_2 + 2s_3 = 0 + 1 + 2 \cdot 2 = 2,$$

$$s_5 = s_2 + s_3 + 2s_4 = 1 + 2 + 2 \cdot 2 = 1,$$

$$s_6 = s_3 + s_4 + 2s_5 = 2 + 2 + 2 \cdot 1 = 0 = s_0,$$

$$s_7 = s_4 + s_5 + 2s_6 = 2 + 1 + 2 \cdot 0 = 0 = s_1,$$

$$s_8 = s_5 + s_6 + 2s_7 = 1 + 0 + 2 \cdot 0 = 1 = s_2$$

따라서  $\{s_t\}$  는 다음과 같이 주기가 6 고 생성순환마디가  $0, 0, 1, 2, 2, 1$  인 순환수열이다.

$$\{s_t\} : 0, 0, 1, 2, 2, 1, 0, 0, 1, 2, 2, 1, \dots$$

## 3. 두 함수

$$f : \mathbb{F}_2^2 \rightarrow \mathbb{F}_2, \quad g : \mathbb{F}_2^2 \rightarrow \mathbb{F}_2$$

의 함수값이 오른쪽 표와 같을 때, 임의의  $(x_0, x_1) \in \mathbb{F}_2^2$ 에 대하여  $f(x_0, x_1)$ 와  $g(x_0, x_1)$ 를  $x_0, x_1$ 에 관한 식으로 나타내어라.

$x_0$	$x_1$	$f(x_0, x_1)$	$g(x_0, x_1)$
0	0	0	1
0	1	1	1
1	0	0	0
1	1	1	1

$$\begin{aligned}
 [\text{풀이}] \quad f(x_0, x_1) &= (x_0 + 1)x_1 + x_0x_1 = x_0x_1 + x_1 + x_0x_1 = x_1 \\
 g(x_0, x_1) &= (x_0 + 1)(x_1 + 1) + (x_0 + 1)x_1 + x_0x_1 \\
 &= x_0x_1 + x_0 + x_1 + 1 + x_0x_1 + x_1 + x_0x_1 \\
 &= x_0x_1 + x_0 + 1
 \end{aligned}$$

## 4. 함수

$$f : \mathbb{F}_2^3 \rightarrow \mathbb{F}_2$$

의 함수값이 오른쪽 표와 같을 때, 임의의  $(x_0, x_1, x_2) \in \mathbb{F}_2^3$ 에 대하여  $f(x_0, x_1, x_2)$ 를  $x_0, x_1, x_2$ 에 관한 식으로 나타내어라.

$x_0$	$x_1$	$x_2$	$f(x_0, x_1, x_2)$
0	0	0	1
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	0

$$\begin{aligned}
 [\text{풀이}] \quad f(x_0, x_1, x_2) &= (x_0 + 1)(x_1 + 1)(x_2 + 1) + (x_0 + 1)(x_1 + 1)x_2 \\
 &\quad + (x_0 + 1)x_1x_2 + x_0x_1(x_2 + 1) \\
 &= x_0x_1x_2 + x_0x_1 + x_0x_2 + x_1x_2 + x_0 + x_1 + x_2 + 1 \\
 &\quad + x_0x_1x_2 + x_0x_2 + x_1x_2 + x_2 \\
 &\quad + x_0x_1x_2 + x_1x_2 + x_0x_1x_2 + x_0x_1 \\
 &= 1 + x_0 + x_1 + x_1x_2
 \end{aligned}$$

## 연 습 문 제 (5.10)

1. 체  $\mathbb{F}_2$  위의 원시다항식

$$f(x) = x^{23} + x^5 + 1, \quad g(x) = x^{25} + x^3 + 1$$

에 대하여 두 수열  $\{a_t\}$ ,  $\{b_t\}$  가 각각  $f(x)$ ,  $g(x)$  를 고유다항식으로 가지는 최대주기수열일 때, 합  $\{a_t\} + \{b_t\}$  의 주기를 구하고 또 그 최소다항식과 선형복잡도를 구하여라.

[풀이] 수열  $\{a_t\}$  는 주기  $2^{23} - 1$  인 순환수열이고, 또 수열  $\{b_t\}$  는 주기  $2^{25} - 1$  인 순환수열이다.

한편,  $(23, 25) = 1$  이므로  $(2^{23} - 1, 2^{25} - 1) = 1$  이다(정리 1.2.16).

따라서  $\{a_t\} + \{b_t\}$  의 주기는  $(2^{23} - 1)(2^{25} - 1)$  이다.

그리고,  $f(x)$  와  $g(x)$  는 서로 소이므로  $\{a_t\} + \{b_t\}$  의 최소다항식은

$$f(x)g(x) = (x^{23} + x^5 + 1)(x^{25} + x^3 + 1)$$

이고 선형복잡도는  $23 + 25 = 48$  이다(정리 5.10.8).

3. 체  $\mathbb{F}_2$  에서의 두 순환수열

$$\{a_t\} : 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, \dots$$

$$\{b_t\} : 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, \dots$$

에 대하여 다음 물음에 답하여라(보기 5.6.3, 보기 5.6.1 참조).

(1)  $\{a_t\}$  의 최소다항식은 다음과 같음을 밝혀라.

$$m_1(x) = x^2 + 1 = (x+1)^2$$

(2)  $\{b_t\}$  의 최소다항식은 다음과 같음을 밝혀라.

$$m_2(x) = x^2 + x + 1$$

(3) 곱  $\{a_t\}\{b_t\}$  의 최소다항식은 다음과 같음을 밝혀라.

$$m(x) = x^4 + x^2 + 1 = (x^2 + x + 1)^2$$



[풀이] 보기 5.6.3 을 이용하여 최소다항식을 구한다.

(1) 무한수열  $\{a_t\}$  는 주기가 2 이고 생성순환마디가 0, 1 인 순환수열  
이므로, 체  $F_2$  위에서

$$f_0(x) = x^2 - 1 = x^2 + 1, \quad g^*(x) = 1$$

이고 또  $f_0(x)$  와  $g^*(x)$  의 최대공약수는  $d(x) = 1$  이다.

따라서  $\{a_t\}$  의 최소다항식  $m_1(x)$  는 다음과 같다.

$$m_1(x) = \frac{f_0(x)}{d(x)} = x^2 + 1 = (x+1)^2$$

(2) 무한수열  $\{b_t\}$  는 주기가 3 이고 생성순환마디가 1, 1, 0 인 순환수열  
이므로, 체  $F_2$  위에서

$$f_0(x) = x^3 - 1 = x^3 + 1 = (x+1)(x^2 + x + 1),$$

$$g^*(x) = x^2 + x = x(x+1)$$

이고  $f_0(x)$  와  $g^*(x)$  의 최대공약수는  $d(x) = x+1$  이다.

따라서  $\{b_t\}$  의 최소다항식  $m_2(x)$  는 다음과 같다.

$$m_2(x) = \frac{f_0(x)}{d(x)} = x^2 + x + 1$$

$x$	$x^3$	$+1$	$x^2+x$	$x$
	$x^3+x^2$		$x^2+x$	
$+1$	$x^2$	$+1$	$0$	
	$x^2+x$			
	$x+1$			

(3) 무한수열  $\{a_t\}\{b_t\}$  는 다음과 같다.

$$\{a_t\}\{b_t\} : 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, \dots$$

따라서  $\{a_t\}\{b_t\}$  는 주기 6 이고 생성순환마디가  $0, 1, 0, 1, 0, 0$  인 순환 수열이므로, 따라서 체  $\mathbb{F}_2$  위에서

$$f_0(x) = x^6 - 1 = x^6 + 1, \quad g^*(x) = x^4 + x^2$$

이고  $f_0(x)$  와  $g^*(x)$  의 최대공약수는 다음과 같다.

$$d(x) = (x + 1)^2 = x^2 + 1$$

따라서  $\{a_t\}\{b_t\}$  의 최소다항식  $m(x)$  는 다음과 같다.

$$m(x) = \frac{f_0(x)}{d(x)} = x^4 + x^2 + 1 = (x^2 + x + 1)^2$$

$x^2$	$x^6$	$+ 1$	$x^4$	$+ x^2$	$1$
$+ 1$	$x^6$	$+ x^4$	$x^4$	$+ x^2$	
		$x^4$		$+ 1$	$0$
		$x^4$		$+ x^2$	
		$x^2$		$+ 1$	

## 연 습 문 제 (5.11)

1. 두 이진 선형 Shift Register LSR 1 과 LSR 2 가 각각 체  $\mathbb{F}_2$  위에서의 33 차의 원시다항식

$$f(x) = x^{33} + x^6 + x^4 + x + 1$$

과 35 차의 원시다항식

$$g(x) = x^{35} + x^2 + 1$$

를 고유다항식으로 가지는 선형 Shift Register 이라고 하자.

이 때,  $M = 2^{33} - 1$ ,  $L = 2^{35} - 1$  이라고 하면,  $2^3 - 1$  과  $2^{11} - 1$  은  $M$  의 약수이지만 이 경우에는 정리 5.11.2 를 적용할 수 없음을 밝혀라.

[풀이] (1) 분명히  $33 = 3 \cdot 11$  이므로

$$\begin{aligned} M &= 2^{33} - 1 = (2^3)^{11} - 1 \\ &= (2^3 - 1)(2^{30} + 2^{27} + \cdots + 2^3 + 1), \\ M &= 2^{33} - 1 = (2^{11})^3 - 1 \\ &= (2^{11} - 1)(2^{22} + 2^{11} + 1) \end{aligned}$$

이고, 따라서  $2^3 - 1$  과  $2^{11} - 1$  은  $M$  의 약수이다.

(2)  $2^3 - 1 = 7$  이고

$$2^{35} \equiv (2^3)^{11} \cdot 2^2 \equiv 1^{11} \cdot 4 \equiv 4 \not\equiv 1 \pmod{7}$$

이므로  $2^3 - 1$  은  $L = 2^{35} - 1$  의 약수가 아니다.

따라서  $2^3 - 1$  은  $M$  의 소인수이지만  $L$  의 약수가 아니다.

그러므로 이 경우에 정리 5.11.2 를 적용할 수 없다.

2. 다음이 성립함을 확인하여라.

$$\begin{aligned} \frac{1}{7} &= 0.\overline{001}_{(2)}, & \frac{2}{7} &= 0.\overline{010}_{(2)}, & \frac{4}{7} &= 0.\overline{100}_{(2)} \\ \frac{3}{7} &= 0.\overline{011}_{(2)}, & \frac{6}{7} &= 0.\overline{110}_{(2)}, & \frac{5}{7} &= 0.\overline{101}_{(2)} \end{aligned}$$

[풀이] 법 7에 관하여

$$2 \equiv 2 \pmod{7}, \quad 2^2 \equiv 4 \pmod{7}, \quad 2^3 \equiv 1 \pmod{7}$$

$$\frac{2^3-1}{7} = 1 = 1_{(2)}, \quad 2^2 < 7 < 2^3$$

이므로  $\text{ord}_7 2 = 3$  이고 또 다음 결과를 얻는다.

$$\frac{1}{7} = 0.\overline{001}_{(2)}, \quad \frac{2}{7} = 0.\overline{010}_{(2)}, \quad \frac{4}{7} = 0.\overline{100}_{(2)}$$

그리고,  $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$  의 원소 중에서 1, 2, 4 가 아닌 원소 3 을 택하면,

$$2^0 \cdot 3 \equiv 3 \pmod{7},$$

$$2 \cdot 3 \equiv 6 \pmod{7},$$

$$2^2 \cdot 3 \equiv 5 \pmod{7},$$

$i$	0	1	2
$2^i$	1	2	4
$2^i \cdot 3$	3	6	5

$$\frac{3(2^3-1)}{7} = 3 = 11_{(2)}$$

이므로 다음 결과를 얻는다.

$$\frac{3}{7} = 0.\overline{011}_{(2)}, \quad \frac{6}{7} = 0.\overline{110}_{(2)}, \quad \frac{5}{7} = 0.\overline{101}_{(2)}$$