$GF(p)$ 위의 특성 다항식을 가진 $GF(p^k)$ 위의 수열의 생성

홍윤표, 송홍엽

yp.hong@coding.yonsei.ac.kr, hy.song@coding.yonsei.ac.kr

2002. 4. 26

연세대학교 전기전자공학과

부호 및 정보이론 연구실

1. 서 론

■큰 심볼 집합을 갖는 수열의 요구 (ex. 주파수 도약 패턴)

⇨ 기존 수열로부터 k-tuple 수열을 생성

■$GF(p)$ 위의 수열로부터 p^k-ary 수열을 생성

⇨ $GF(p)$ 위의 k-tuple을 $GF(p^k)$로 올릴 때 기저의 선택 문제

⇨ 기저의 선택은 심볼 간의 치환과 동일

⇨ 기저의 변화에 따라 $GF(p^k)$ 위의 수열의 특성다항식과 선형복잡도 변화

2. $GF(p)$ 위의 특성 다항식을 가진 $GF(p^k)$ 위의 수열의 생성

■$S=\{s_n\}$, $n=1,2,\ldots,$: $GF(p)$ 위의 수열

⇨ $T(k,S)=\{t_n\}$, $n=1,2,\ldots,$를 생성

$$t_n = (s_n, s_{n+1}, \cdots, s_{n+k-1}) \quad (1)$$

⇨ p-ary k-tuple인 t_n을 임의의 고정된 기저를 사용하여 $GF(p^k)$로 올림

명제 1: *$GF(p)$ 위의 수열 $S=\{s_n\}$를 생성하는 선형 궤환 쉬프트 레지스터 (LFSR)는 기저의 선택에 관계없이 식 (1)로 정의된 $GF(p^k)$ 위의 수열 $T(k,S)$도 생성한다. 반대의 경우는 $GF(p^k)$ 위의 T를 생성하는 연결 다항식이 $GF(p)$ 위에 있을 경우에 성립한다.*

2. $GF(p)$ 위의 특성 다항식을 가진 $GF(p^k)$ 위의 수열의 생성

예제 2: *주기가 26인 3진 수열 S={00111021121010022201221202 00 …}*

⇨ *T(3,S) = {001 011 111 110 102 021 211 112 121 210 …}*

⇨ *T(4,S) = {0011 0111 1110 1102 1021 0211 2112 1121 1210 2101 …}*

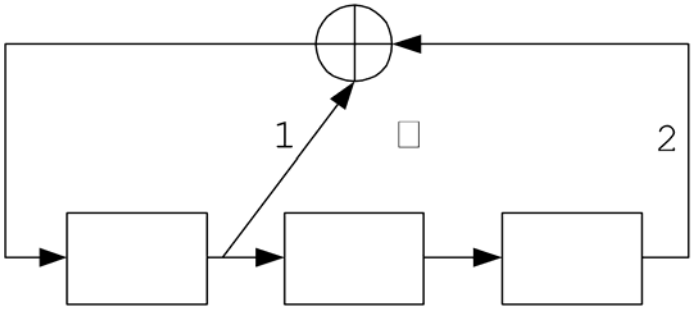

그림 1. 예제 2의 S와 T를 생성하는 LFSR

2. $GF(p)$ 위의 특성 다항식을 가진 $GF(p^k)$ 위의 수열의 생성

■문제 제기

(1) 명제 1은 $GF(p)$ 위의 S를 생성하는 최소 단수 LFSR이 $GF(p^k)$ 위의 $T(k,S)$, $k \geq 2$,를 생성하는 최소 단수 LFSR이라는 것을 보장하지 못함

(2) $GF(p^k)$ 위의 $T(k,S)$, $k \geq 2$,를 생성하는 최소 단수 LFSR은 $GF(p^k)$의 기저가 고정되지 않으면 유일하게 결정할 수 없음

2. $GF(p)$ 위의 특성 다항식을 가진 $GF(p^k)$ 위의 수열의 생성

예제 3: (a) 주기가 63인 이진 수열 S_1 ={1100100000111111010100100100110101011101101101110100111111010 …}

⇨ S_1의 선형 복잡도 = 62

⇨ 모든 다항식 기저에 대한 $T(3,S_1)$의 선형 복잡도 = 60

(b) 주기가 63인 이진 수열 S_2={0101111111001100000110111110101001111110001100111010010100101011 …}

⇨ $T(3,S_2)$의 선형 복잡도는 x^3+x+1과 x^3+x^2+1중 어떠한 원시 다항식의 근을 원시 원소로 하는 다항식 기저를 사용하느냐에 따라 각각 55와 53이 된다.