Hall's Sextic Residue 수열의 선형 복잡도에 관하여

최기훈°, 김정헌, 송홍엽

연세대학교 전기전자공학과

발표자 : 최 기 훈 (khchoi@eve.yonsei.ac.kr)

▶발표 순서

1. 서론
2. 선형 복잡도
3. Hall's Sextic Residue 수열의 선형 복잡도
4. 결론

1. 서론

▶ 최적 자기상관특성과 밸런스특성을 갖는 주기적 이진 수열

1. 무작위 특성과 생성의 용이성
   ⇒ 대역 확산 통신을 포함한 많은 응용에서 중요한 역할
2. 순환 하다마드 차집합 (cyclic Hadamard difference sets)과 동치

▶ 이러한 수열들의 주기

(i) mod 4로 3과 congruent한 소수⇒ 르장드르 수열, Hall's sextic residue 수열

(ii) twin 소수들의 곱의 형태

(iii) 어떤 정수 n에 대해서 $2^n - 1$ 형태

▶ 주기 p인 Hall's sextic residue 수열

$p = 4u^2 + 27 = 6f + 1$를 소수, g를 modulo p에 대한 원시근이라 하자. 그러면, mod p에 대한 정수들의 모든 0이 아닌 원소들은 6개의 cyclotomic class C_l, $l = 0, 1, 2, \cdots, 5$,로 다음과 같이

$$C_l = \{ g^{6i+l} \mid i = 0, 1, \cdots, f-1 \} \quad (1)$$

분할될 수 있다.

주기 p인 Hall's sextic residue 수열은 다음과 같이 정의된다.

$$s(t) = \begin{cases} 1 & \text{if } t \in C_0 \cup C_1 \cup C_3 \\ 0 & otherwise \end{cases}$$

여기서 $t = 0, 1, \cdots, p-1$이고, g는 $3 \in C_1$가 되도록 선택된다.

(예) $p = 4(1)^2 + 27 = 6(5) + 1 = 31 \Rightarrow u = 1, f = 5$ 일 때, $(g = 3)$

$$C_0 = \{3^0, 3^6, 3^{12}, 3^{18}, 3^{24}\} = \{1, 16, 8, 4, 2\} \vee$$

$$C_1 = \{3^1, 3^7, 3^{13}, 3^{19}, 3^{25}\} = \{3, 17, 24, 12, 6\} \vee$$

$$C_2 = \{3^2, 3^8, 3^{14}, 3^{20}, 3^{26}\} = \{9, 20, 10, 5, 18\}$$

$$C_3 = \{3^3, 3^9, 3^{15}, 3^{21}, 3^{27}\} = \{27, 29, 30, 15, 23\} \vee$$

$$C_4 = \{3^4, 3^{10}, 3^{16}, 3^{22}, 3^{28}\} = \{19, 25, 28, 14, 7\}$$

$$C_5 = \{3^5, 3^{11}, 3^{17}, 3^{23}, 3^{29}\} = \{26, 13, 22, 11, 21\}$$

· 주기 31인 Hall's sextic residue 수열

t:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
$\Rightarrow$	0	1	1	1	1	0	1	0	1	0	0	0	1	0	0	1	1	1	0	0	0	0	0	1	1	0	0	1	0	1	1

⇒ (32×32) **Hadamard Matrix**

2. 선형 복잡도

· 주기적 이진 수열의 선형 복잡도 L
⇒적절한 연결과 초기 조건으로 만들어지는 가장 짧은 LFSR의 단의 수

▶ 주기 p인 이진 수열 $\{s(t)\}$, 선형 복잡도 L

다음을 만족하는 상수들 $c_0 = 1, c_1, c_2, \cdots, c_{L-1}, c_L = 1 \in GF(2)$이 존재

$$s_i = c_{L-1}s_{i-1} + c_{L-2}s_{i-2} + \cdots + c_0 s_{i-L},$$

for all $L \leq i < p$

다항식 $c(X) = X^L + c_{L-1}X^{L-1} + \cdots + c_0$: 이 수열의 특성 다항식

· 수열 $\{ s(t) \}$의 reciprocal 특성 다항식:

$$c^*(x) = c_0 x^L + c_1 x^{L-1} + \cdots + c_{L-1} x + 1$$

$$= (x^p - 1) / \gcd(x^p - 1, S(x))$$

where $S(x) = s_0 + s_1 x + \cdots + s_{p-1} x^{p-1}$

· 수열 $\{ s(t) \}$의 선형 복잡도

$$L = p - \deg[\gcd(x^p - 1, S(x))]$$

▶ 주기 p인 Hall's sextic residue 수열

· 대응되는 $S(x)$: $S(x) = C_0(x) + C_1(x) + C_3(x)$

여기서 $3 \in C_1$이기 때문에, $C_l(x)$는 다음과 같이 표현될 수 있다.

$$C_l(x) = \sum_{i \in C_l} x^i = \sum_{i=0}^{f-1} x^{3^l g^{6i}} \tag{2}$$

· 주기 p인 Hall's sextic residue 수열의 선형 복잡도

$$\begin{aligned} L &= p - \deg[\gcd(x^p - 1, S(x))] \\ &= p - |\{ j : S(\beta^j) = 0, \quad 0 \le j \le p-1 \}| \end{aligned} \tag{3}$$

여기서 β는 $x^p - 1$의 splitting field인 $GF(2^n)$상의 p차 원시근

3. Hall's sextic residue 수열의 선형 복잡도

정리. 주기 $p = 4u^2 + 27$인 Hall's sextic residue 수열은 다음과 같은 reciprocal 특성 다항식 $c^*(x)$을 갖는다:

$$c^*(x) = \begin{cases} (x-1) \prod_{i \in C_0} (x-\beta^i) & \text{if } p \equiv 7 \pmod 8 \\ x^p - 1 & \text{if } p \equiv 3 \pmod 8 \end{cases}$$

여기서 β는 $S(\beta) = 1$을 만족하는 p차 원시근이다. 선형 복잡도 L은 다음과 같이 주어진다.

$$L = \begin{cases} 1 + \dfrac{p-1}{6} & \text{if } p \equiv 7 \pmod 8 \\ p & \text{if } p \equiv 3 \pmod 8 \end{cases}$$

(증명)

1) $p \equiv 7 \pmod 8$

$L = p - |\{ j : S(\beta^j) = 0, \quad 0 \le j \le p-1 \}| \Rightarrow S(\beta^j) \neq 0$이 되는 j의 수를 고려

$p \equiv 7 \pmod 8$인 경우에 $S(\beta) = 1$이 되는 p차 원시근 β가 존재하고, $a \in C_0$인 어떤 a에 대하여 $C_I(\beta^a) = C_I(\beta)$이기 때문에,

$$S(\beta^a) = 1 \quad \text{for} \quad a \in C_0$$

$i = 1, \cdots, 5$에 대하여 $S(\beta^{3^i}) = 0$이고, 같은 cyclotomic class에 있는 i와 j에 대하여 $C_I(\beta^i) = C_I(\beta^j)$이므로,

$$S(\beta^b) = 0 \quad \text{for} \quad b \in C_1 \cup C_2 \cup C_3 \cup C_4 \cup C_5$$

$$\text{and} \quad S(1) = [\,(p-1)/2 \pmod 2\,] = 1$$

$$c^*(x) = \frac{(x^p - 1)}{\gcd(x^p - 1, S(x))}$$

$$= (x-1) \prod_{i \in C_0} (x - \beta^i)$$

여기서 $c^*(x)$는 $GF(2)$상의 다항식 ($\because 2C_0 = C_0$)

$\therefore$ 선형 복잡도 $L = 1 + (p-1)/6$

2) $p \equiv 3 \pmod 8$

$S(\beta^j) \neq 0$ for $j = 1, \cdots, p-1$

and $S(1) = [(p-1)/2 \pmod 2] = 1$

$\Rightarrow \gcd(x^p - 1, S(x)) = 1$

$\therefore c^*(x) = x^p - 1 \Rightarrow$ 선형 복잡도 $L = p$

4. 결론

▶ Hall's sextic residue 수열의 선형 복잡도 결정

· 주기 $p = 4u^2 + 27$인 Hall's sextic residue 수열의 선형 복잡도 L

$$L = \begin{cases} 1 + \dfrac{p-1}{6} & \text{if } p \equiv 7 \pmod 8 \\ p & \text{if } p \equiv 3 \pmod 8 \end{cases}$$