Branchless state diagram을 이용해 생성한 주기 2^4-1 Binary sequences와 그 특성에 대한 조사

이민형, 김강산, 변성철, 조현우, 김원준, 송홍엽
연세대학교
2019년도 한국통신학회 동계종합학술발표회

본 논문은 최대 주기가 2^4-1 인 Branchless state diagram으로부터 생성된 Branchless sequence 중 주기가 2^4-1인 sequences를 모두 찾은 후 이들의 Pseudo random 특성들을 조사하였다.

1. Branchless state diagram

x_0	x_1	x_2	…	x_{L-2}	x_{L-1}	f
	0	0	…	0	0	
	0	0	…	0	1	
	0	0	…	1	0	
			⋮			
	1	1	…	1	1	
	0	0	…	0	0	
	0	0	…	0	1	
	0	0	…	1	0	
			⋮			
	1	1	…	1	1	

Complement

$$f(x_0, x_1, x_2, \dots, x_{L-1}) = x_0 \oplus g(x_1, x_2, \dots, x_{L-1})$$

- 위의 그림과 식과 같이 $f(1, x_1, x_2, \dots, x_{L-1})$ 와 $f(0, x_1, x_2, \dots, x_{L-1})$ 이 Complement 관계에 있는 State diagram을 Branchless state diagram이라 하고, 이를 이용해 생성한 Binary Sequence를 Branchless Sequence라 함
- 최대 주기가 2^4-1인 state diagram으로부터 생성된 Branchless sequence는 모두 2^8개가 있으며, 이 중 주기가 2^4-1 인 sequences는 모두 24개가 있음
- 생성된 주기가 2^4-1인 Branchless sequences의 다음의 특성들을 조사함 [1]
  - ✓ Multiplier : sequence $s(t)$에 대해 $s(dt) = s(t)$이면 multiplier를 만족한다.
  - ✓ Ideal Autocorrelation : 주기가 L인 Binary sequence $s(t)$에 대해

$$A(\tau) = \sum_{t=0}^{L-1} (-1)^{s(t+\tau)+s(t)} \begin{cases} L, & \text{if } \tau = 0 \\ -1, & \text{otherwise} \end{cases}$$

    이면 Ideal Autocorrelation을 만족한다.
  - ✓ Autocorrelation Level : 주기가 L인 Binary sequence $s(t)$에 대해 τ에 따른 가능한

$$A(\tau) = \sum_{t=0}^{L-1} (-1)^{s(t+\tau)+s(t)}$$ 의

    개수를 Autocorrelation Level 이라 한다.
  - ✓ Linear complexity : Binary sequence $s(t)$에 대해 $s(t)$를 생성하는 L-stage linear feedback shift register들 중 필요로 하는 stage가 최소일 때의 L을 Linear complexity 라 하며, Berlekamp – Massey 알고리즘을 이용해 구할 수 있다.

2. 주기가 2^4-1인 Branchless sequences와 특성

Index	Output sequence	Multiplier	Ideal Autocorr.	Autocorr. Level	Linear complexity	Complement with
1	000111011001010	O	O	2	5	13
2	000101001110110	X	X	4	8	14
3	000110010111010	X	X	4	8	15
4	000111010110010	X	X	4	7	16
5	000101100111010	X	X	4	7	17
6	000101110100110	X	X	4	8	18
7	000100111010110	X	X	4	8	19
8	000110111001010	X	X	4	8	20
9	000101001101110	O	O	2	5	21
10	000110101110010	X	X	4	8	22
11	000101110011010	X	X	4	8	23
12	000100110101110	X	X	4	11	24
13	000100110101111	O	O	2	4	1
14	000100111101011	X	X	4	8	2
15	000101111001101	X	X	4	7	3
16	000101001101111	X	X	4	10	4
17	000101111010011	X	X	4	9	5
18	000101100111101	X	X	4	8	6
19	000101001111011	X	X	4	9	7
20	000110101111001	X	X	4	10	8
21	000111101011001	O	O	2	4	9
22	000110111100101	X	X	4	10	10
23	000110010111101	X	X	4	8	11
24	000111101100101	X	X	4	7	12

- 1 - 12번 sequences는 13- 24번 까지의 sequences들의 complement로 나타낼 수 있음
- 1, 9 번 sequence는 m-sequence임
- 주기가 2^4-1이고 Ideal Autocorrelation을 만족하는 sequences는 1, 9, 13, 21번 수열로 모두 4개이며, 2개의 m-sequences와 이들에 대한 complement임
- $p_i(x)$: i 번째 sequence의 minimal polynomial이라 할 때
  $p_1(x) = (x+1)p_{13}(x),\ \ p_9(x) = (x+1)p_{21}(x)$
  로 나타낼 수 있음

REFERENCES

[1] S. W. Golomb, Shift Register Sequences, Holden-Day, San Francisco, CA, 1967; Revised Edition, Aegean Park Press, Laguna Hills, CA, 1982; 3rd Revised Edition, World Scientific Publishing Co. Pte. Ltd, 2017.