르장드로 심볼과 트레이스 함수를 이용한 이진 수열의 3-레벨 자기상관 특성

이민형, 김강산, 송민규, 송홍엽
연세대학교
2018년도 한국통신학회 동계종합학술발표회

1. 표기법과 사전 지식

- α : 유한체 $GF(p^n)$의 임의의 원시원소
- $Tr_{p^n/p^m}(x)=\sum_{i=0}^{\frac{n}{m}-1} x^{p^{mi}}$: $GF(p^n)$에서 $GF(p^m)$로의 대각합 함수
- $\left(\frac{y}{GF(p^m)}\right)=\begin{cases} 0, & \text{if } y=0 \\ 1, & \text{if y is a quadratic element} \\ -1, & \text{otherwise} \end{cases}$
  : $GF(p^m)$에서 {-1, 0, 1}으로의 르장드로 함수
- 자기 상관: 주기 L인 2진 수열 a_t의 임의의 순환지연 τ에서의 자기상관 $C_{a_t}(\tau)$는

$$C_{a_t}(\tau)=\sum_{t=0}^{L-1}(-1)^{a_t-a_{t+\tau}}$$

와 같이 정의함.

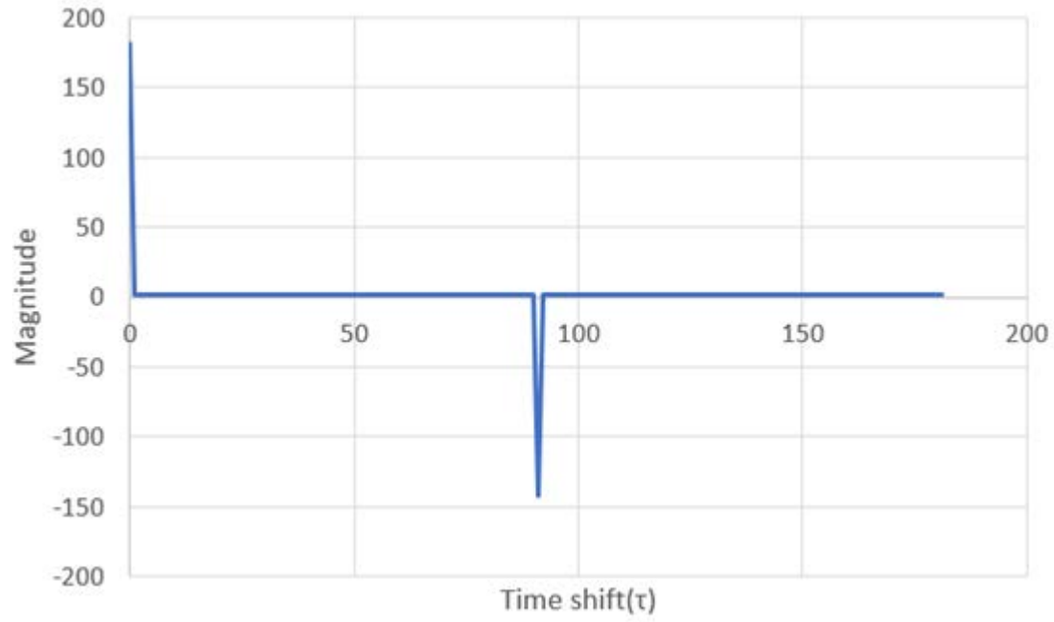
2. 수열 s_t 생성

- 임의의 홀수인 소수p, 임의의 자연수 n, n의 임의의 양의약수 m에 대해, 2진 수열 s_t를 다음과 같이 정의함[2].

$$s_t = f_2\left(\frac{Tr_{p^n/p^m}(\alpha^t)}{GF(p^m)}\right)$$

여기서 $f_2(x)$는 $x=-1,0,1$에 대해 아래와 같이 정의됨.

$$f_2(x)=\begin{cases} 0, & if\ x=0,1 \\ 1, & if\ x=-1 \end{cases}$$



$(p,n,m)=(3,6,2)$일 때, 지연시간 τ에 따른 수열 s_t의 자기상관 특성

4. 결과 분석

- 실험한 모든 (p,n,m)에 대해 자기상관 레벨이 항상 3이 나오는 것을 확인할 수 있음.
- 한 주기 내에서 2개만 제외하고 0에 가까운 자기상관 값을 갖음.

3. 수열 s_t의 자기상관 실험

- 수열 s_t의 Linear complexity는 매우 크고, 주기는 $2\frac{p^n-1}{p^m-1}$임이 알려져있음[2].
- 본 논문에서는 수열 s_t의 자기상관 특성에 관해 실험을 수행함.

▪ 실험 결과

p	n	m	주기	자기상관 프로파일	레벨
3	4	2	20	20:1, -16:1, 0:18	3
	6	2	182	182:1 –142:1 2:180	3
		3	56	56:1, -52:1, 0:54	3
	8	2	1640	1640:1,-1276:1,20:1638	3
		4	164	164:1,-160:1,0:162	3
5	4	2	52	152:1,-48:1,0:50	3
	6	2	1302	1302:1,-1198:1,2:1300	3
		3	252	252:1,-248:1,0:250	3
7	4	2	100	100:1,-96:1,0:98	3
	6	2	4902	4900:1,-4702:1,2:4900	3
		3	688	688:1,-684:1,0:686	3

P, n, m 에 따른 자기 상관 특성 표

5. 결론

- 수열 s_t는 2. 에 제시된 조건을 만족하는 (p, n, m)에 대해 명확한 자기상관 특성을 갖을 것이라 추정됨.
- 이 특성을 정확히 파악하고 검증하는 것이 추후 연구 주제임.

▪ 참고문헌

[1] A. Canteaut and M. Videau, “Degree of Composition of Highly Nonlinear Functions and Applications to Higher Order Differential Cryptanalysis”, *Advances in Crytology Eurocrypt*, INCS 2332, pp 513-533, 2002

[2] A. M. ARSHAD, “Linear Complexity of Pseudo Random Binary Sequence Generated by Trace Function and Legendre Symbol Over 4. Proper Sub Extension Field”, *Proc. of IWSDA’17*, 2017

[3]. L. Guerra and E. Ughi, “On the distribution of Legendre symbols in Galois Fields”, North-Holland Publishing Company, *Discrete Mathematics* 42, pp 197-208, 1982