르장드로 심볼과 트레이스 함수를 이용한 이진 수열의 5-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

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

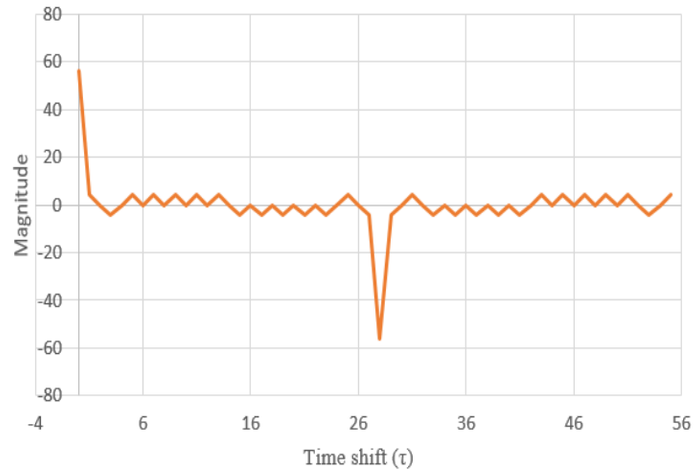
와 같이 정의함.

2. 수열 s_t^* 생성

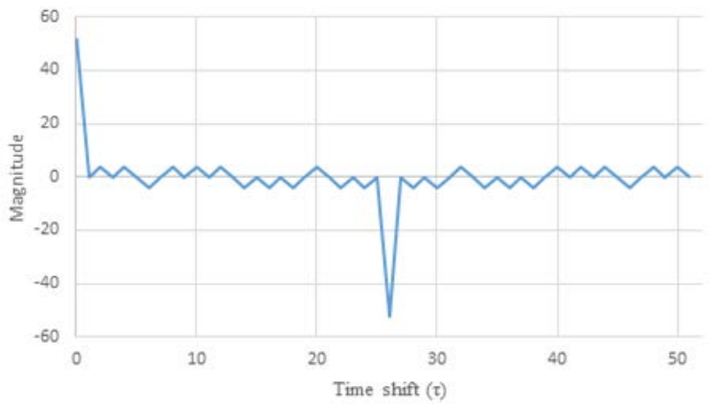
- 임의의 홀수인 소수 p, 임의의 자연수 m에 대해, 2진 수열 s_t^*를 다음과 같이 정의함[2].

$$s_t^*=h_2\left(\frac{Tr_{p^{2m}/p^m}(\alpha^t)}{GF(p^m)},t\right)$$

여기서 $h_2(x,t)$는 $x=-1,0,1, t=0,1,2,\ldots$ 에 대해 아래와 같이 정의됨.



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



$(p,m)=(5,4)$일 때, 지연시간 τ에 따른 수열 s_t의 자기상관 특성

4. 결과 분석

- 실험한 모든 (p,m)에 대해 자기상관 레벨이 항상 5가 나오는 것을 확인할 수 있음.
- 한 주기 내에서 2개만 제외하고 0에 가까운 자기상관 값을 갖음.

$$h_2(x) = \begin{cases} 0, & if\ \ x = 1 \\ & or\ x = 0, t = 0, 1, 2, \dots, p^m (mod\ 2(p^m + 1) \\ 1, & otherwise \end{cases}$$

3. 수열 s_t^*의 자기상관 실험

- s_t^* 주기는 $2(p^m + 1)$임이 알려져있음[2].
- 본 논문에서는 수열 s_t^*의 자기상관 특성에 관해 실험을 수행함.

▪ 실험 결과

p	m	주기	자기상관 프로파일	레벨
3	2	20	-20:1,-4:4,0:10.4:4,20:1	5
	3	56	-56:1,-4:14,0:26,4:14,56:1	5
	4	164	-164:1,-4:40,0:82,4:40,164:1	5
	5	488	-488:1,-4:122,0:242,4:122,488:1	5
5	2	52	-52:1,-4:12,0:26,4:12,52:1	5
	3	252	-252:1,-4:62,0:136,4:62,252:1	5
7	2	100	-100:1,-4:24,0:50,4:24,100:1	5
	3	688	-688:1,-4:172,0:342,4:172,688:1	5
11	2	244	-244:1,-4:60,0:122,4:60,244:1	5

P, m 에 따른 s_t^*자기 상관 특성 표

5. 결론

- 수열 s_t^*는 2. 에 제시된 조건을 만족하는 (p, 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