Run, Span, Multiplier, Ideal autoccorealtion 특성 분석

김강산, 이민형, 변성철, 조현우, 김원준, 송홍엽

연세대학교

2019년도한국통신학회하계종합학술발표회

본 논문은 대표적인 난수 특성인 Run, Span, Multiplier, Ideal autocorrelation 특성에 개수에 대한 분석을 하고, 몇가지 특성에서 흥미로운 실험 결과를 제시하고 분석한다.

1. 이진수열의 4가지 Randomness 특성

- **정의 1(Run 특성).** 길이가 2^n-1인 이진 수열은 다음과 같은 Run 분포를 가지면 Run 특성을 갖는다.

길이	1의 run	0의 run
n	1	0
$n-1$	0	1
$n-2$	2^0	2^0
$n-3$	2^1	2^1
…	…	…
2	2^{n-4}	2^{n-4}
1	2^{n-3}	2^{n-3}
합계	2^{n-2}	2^{n-2}
총합계	2^{n-1}	

표1. Run 특성을 갖는 수열의 Run 분포

- **정의 2(Span 특성).** 길이가 2^n-1인 이진 수열은 길이 n인 벡터 중 모두가 0은 아닌 벡터들이 한 주기 안에 꼭 한번씩 등장 할 때 Span 특성을 갖는다.
- **정의 3(Ideal autocorrelation 특성).** 길이가 2^n-1인 이진 수열 $\boldsymbol{s}=\{s_t\}$는 2^n-1로 나눈 나머지가 0이 아닌 정수 τ에 대해

$$\sum_{t=0}^{2^n-2}(-1)^{s_t+s_{t+\tau}}=-1$$

을 만족하면 Ideal autocorrelation 특성을 갖는다.

- **정의 4(Multiplier 특성).** 길이가 2^n-1인 이진 수열 $\boldsymbol{s}=\{s_t\}$는 어떤 정수 τ와 모든 가능한 t에 대해 $s_t=s_{2t+\tau}$를 만족하면 Multiplier 특성을 갖는다.
- 길이가 2^n-1인 이진 수열은 span특성을 갖으면 run 특성을 갖고, Ideal autocorrelation 특성을 갖으면 Multiplier 특성을 갖음.

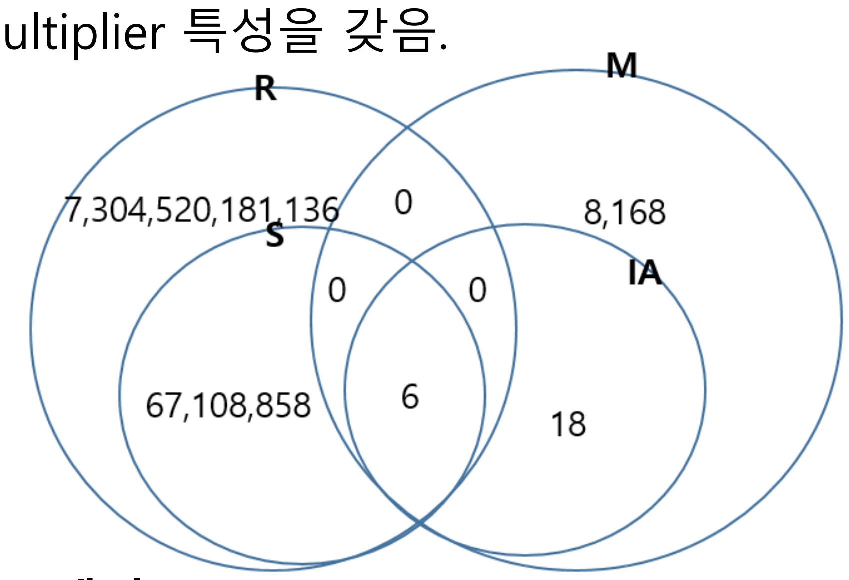

그림1. n=6에서 Run(R), Span(S), Multiplier(M), Ideal autocorrelation(IA) 특성을 갖는 수열 개수의 벤 다이어그램

2. Run 특성을 갖는 이진수열의 특징 분석

- Run 특성을 갖는 길이가 2^n-1인 모든 이진 수열에서 길이가 n인 각각의 이진 벡터들의 발생 평균이 모두 1이 되지는 않음.

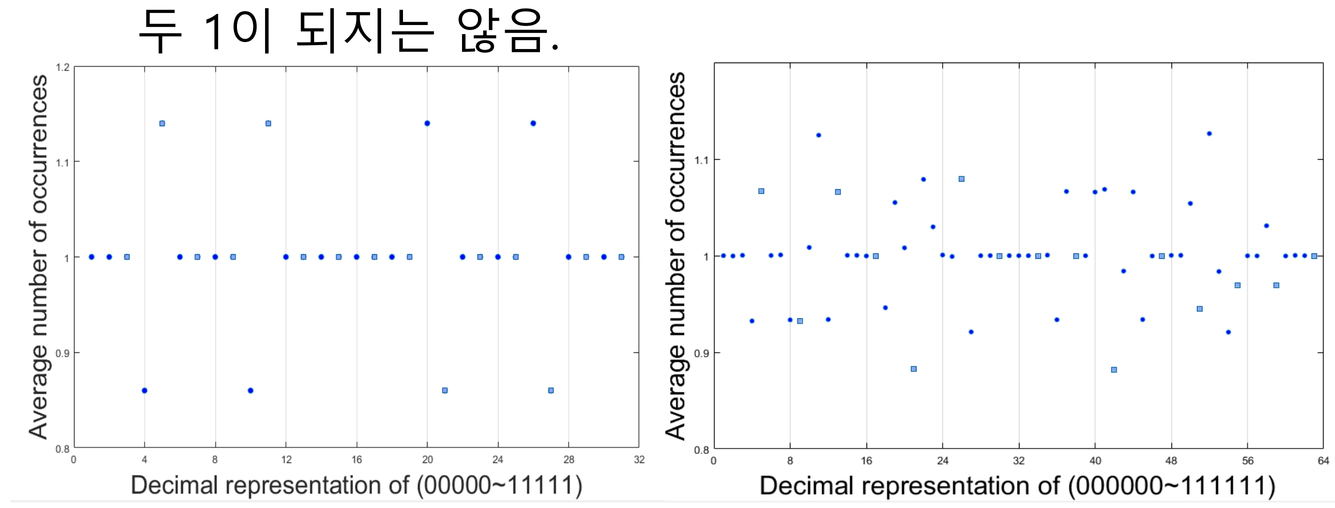

그림2. 길이 2^n-1인 모든 run 수열에서 n-tuple vector 분포의 평균값(n=5에서 전수조사(좌), n=6에서 통계적 조사(우))

- **정리 1.** Run특성을 갖는 길이가 2^n-1인 이진 수열의 개수는 다음과 같다.

$$\frac{1}{2^{n-2}}\binom{2^{n-2}}{2^{n-3},\ 2^{n-4},\dots,2^1,2^0,1}$$

3. Ideal autocorrelation 특성을 갖는 이진 수열의 특징 분석

- Ideal autocorrelation 특성을 갖는 이진 수열은 그 수열의 complement도 Ideal autocorrelation 특성을 갖음.
- 인접한 선형 복잡도를 가지는 Ideal autocorrelation 특성을 갖는 수열 쌍이 존재함.
  - ✓ 어떤 수열이 그 수열을 생성하는 LFSR이 $x+1$의 배수가 아닌 connection polynomial f(x)를 갖는다면 $(x+1)f(x)$을 connection polynomial로 하는 LFSR은 그 수열의 complement를 생성함.

선형 복잡도	n=5, IA 개수	선형 복잡도	n=6, IA 개수
5	6개	6	6개
6	6개	7	6개
15	2개	12	6개
16	2개	13	6개

표2. n=5, 6에서 선형복잡도에 따른 Ideal autocorrelation(IA) 수열의 개수

- **REFERENCES**

[1] Song, H-Y., "Feedback Shift register sequences," *Wiley Encyclopedia of Telecommunications*, 2003.

[2] Song, H-Y. and Golomb, S. W., "On the existence of cyclic Hadamard difference sets," IEEE transactions on Information Theory, vol.40(4), pp.1266-1268, 1994.

[3] Golomb, S. W. *Shift register sequences,* San Francisco, CA, Holden-Day, 1967; 2nd edition, Aegean Park Press, Laguana Hills, CA, 1982; 3rd edition, World Scientific, Hackensaek, NJ, 2017.

[4] Golomb, S. W., "On the classification of balanced binary sequences of period -1, " *IEEE Transactions on Information Theory*, vol. 26(6), pp. 730-732, 1980.