Sidelnikov 수열의 배열 구조로부터 얻어진 열 수열들의 상관 특성에 대한 연구

김지현, 김수연, 송민규, 송홍엽, 이장용

연세대학교

2016년도 한국통신학회 추계종합학술발표회

▪ Notation

- q : 소수 또는 소수의 제곱수
- $GF(q^d)$: q^d 개의 원소로 이루어진 유한체

$$(2 \le d < \frac{1}{2}(\sqrt{q} - \frac{2}{\sqrt{q}} + 1))$$

- M : $q-1$의 2이상의 제수
- α : $GF(q^d)$의 원시근

▪ Sidelnikov 수열의 정의

$$s(t) \equiv \log_{\alpha}(\alpha^t + 1) \bmod M$$

▪ 복소/해밍 상관관계 정의

- 복소 상관관계

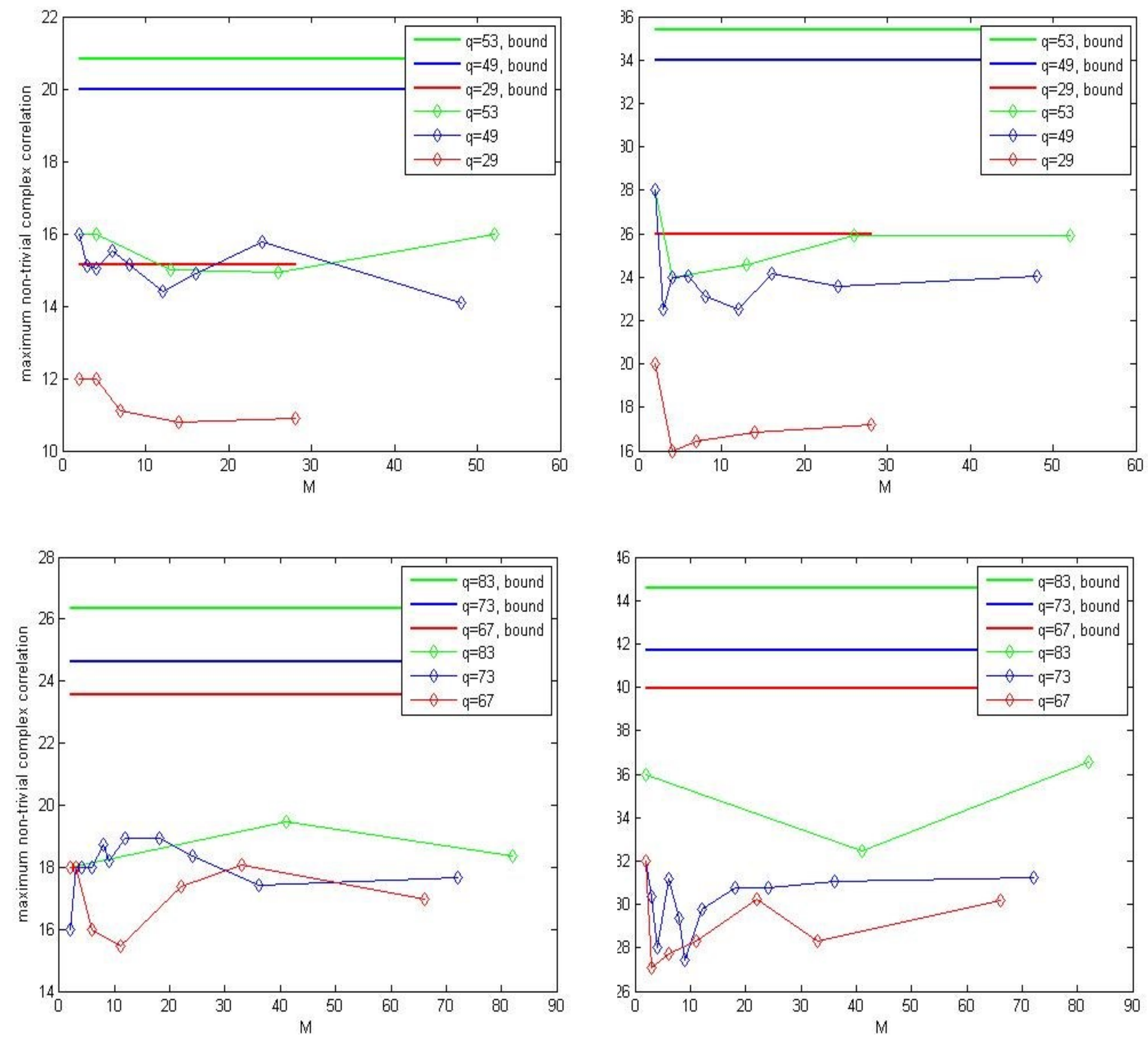
$$C_{a,b}(\tau) = \sum_{t=0}^{L-1} \exp(j\frac{2\pi}{M})^{a(t)-b(t+\tau)}$$

- 해밍 상관관계

$$H_{a,b}(\tau) = \sum_{t=0}^{L-1} h(a(t), b(t+\tau)),$$

$$\text{where } h(x,y) = \begin{cases} 1 & \text{if x = y} \\ 0 & \text{otherwise} \end{cases}$$

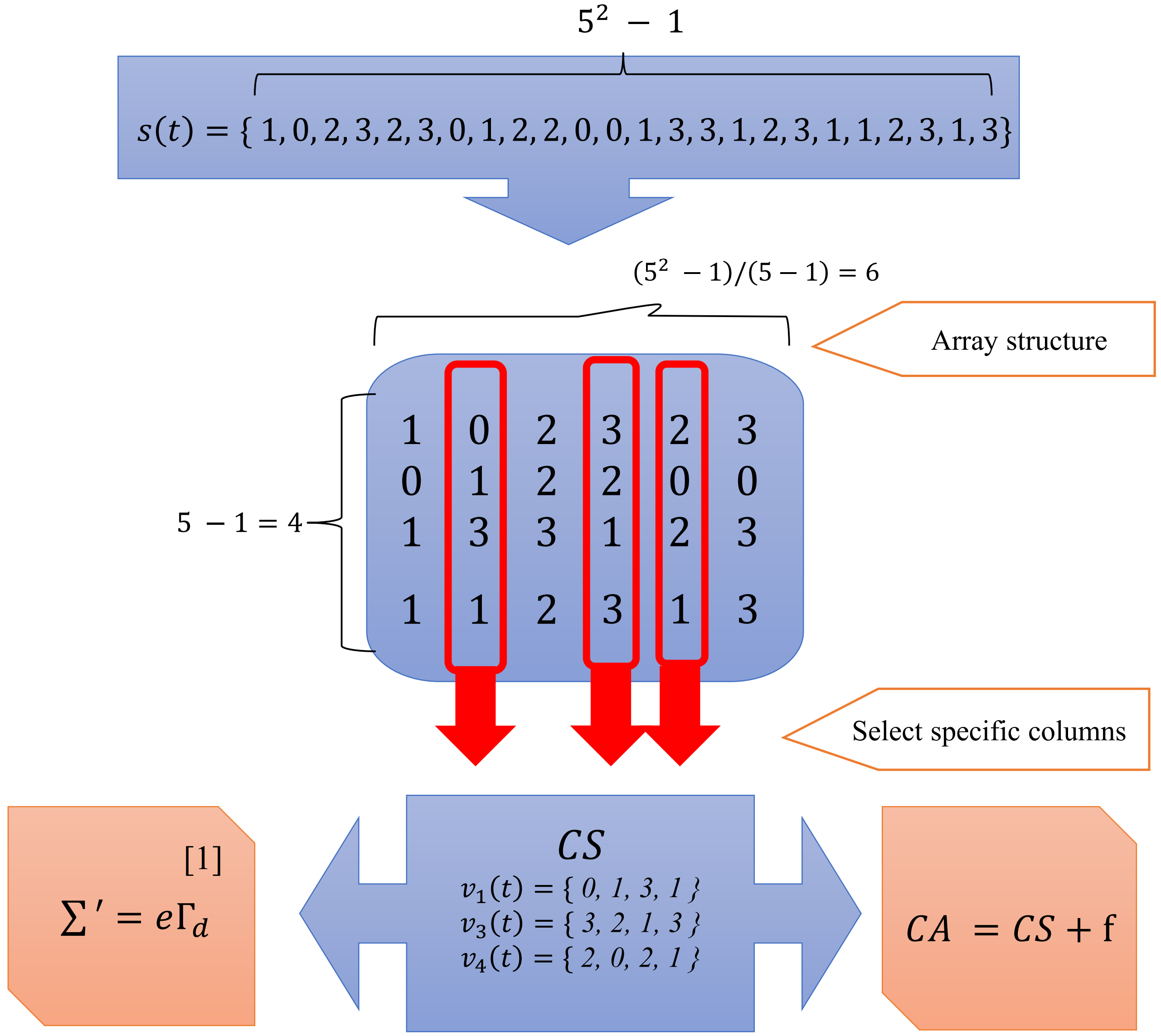
▪ Σ'의 비자명 최대 복소상관의 이론적 상계의 효용성 검증



▪ CS와 CA의 해밍 상관 특성

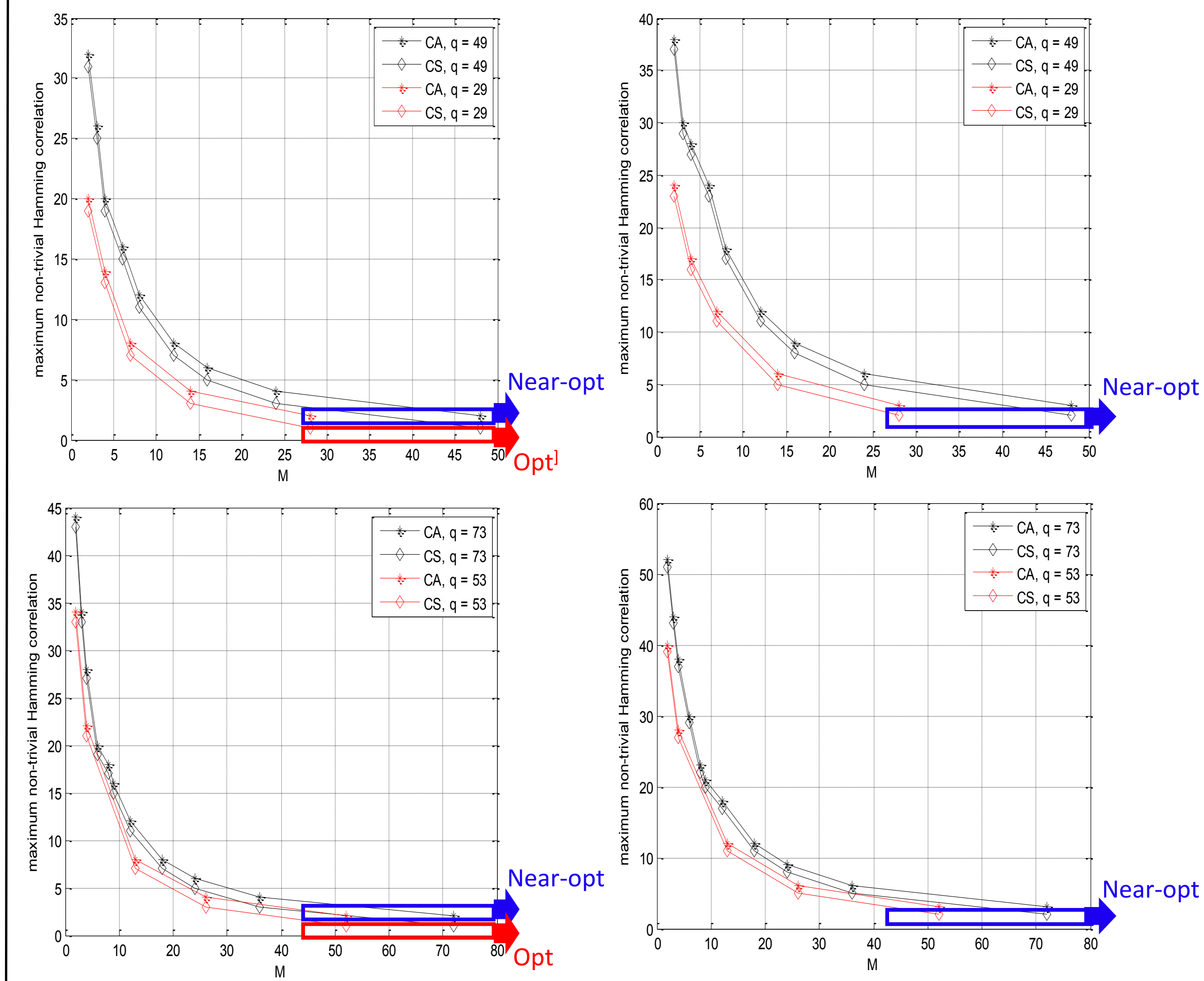
▪ Sidelnikov 수열의 2차원 배열로부터 얻어진 열 수열[1]

Example : $q = 5, d = 2, M = 4$



▪ Σ'의 비자명 최대 복소상관의 이론적 상계

$$C_{max}(\Sigma') \le (2d-1)\sqrt{q} + 1$$



▪ 실험결과

- q가 증가함에 따라 Σ'의 비자명 최대 복소 상관 값이 증가하며 이론적 상계와의 차이 역시 증가
- $M = q - 1$일 때 CS, CA의 비자명 최대 해밍 상관값은 M값과 관계없이 일정한 값을 나타냄 (optimal hopping sequence[2])

▪ 참고문헌

[1] Young-Tae Kim, Dae San Kim, and Hong-Yeop Song, "New M-ary sequence families with low correlation from the array structure of Sidelnikov sequences", *IEEE Transactions on Information Theory*, vol.61, no.1, pp.655-670, 2015.

[2] A. A. Shar and P. A. Davis, "A survey of one-coincidence sequences for frequency-hopped spread spectrum systems," *IEE Proceedings F*, vol. 131, no. 7, pp. 719-724, 1984.