논문 20-45-08-01 The Journal of Korean Institute of Communications and Information Sciences '20-08 Vol.45 No.08
https://doi.org/10.7840/kics.2020.45.8.1323

Sidelnikov 수열로부터 생성된 좋은 상관 관계를 갖는 유사-다상 수열

이 민 형◆, 김 강 산*, 송 홍 엽°

Almost-Polyphase Sequences with Good Correlation Property from Sidelnikov Sequences

Min Hyung Lee◆, Gangsan Kim*, Hong-Yeop Song°

요 약

본 논문은 q를 소수의 거듭제곱, k를 $q-1$의 약수라 할 때, 주기가 $q-1$인 k진 Sidelnikov 수열 하나를 이용하여 주기가 $q-1$이고 크기가 $k-1$인 유사-다상 수열 집합의 생성법을 제안한다. 또한, 이 집단의 모든 수열의 비동기 자기 상관의 절댓값의 최댓값이 2이며, 상호 상관의 절댓값의 최댓값이 $\sqrt{q}+1$임을 증명했다.

Key Words : Polyphase sequences, Almost-polyphase sequences, Sidelnikov sequences, Correlation of sequences

ABSTRACT

Let q be a power of a prime and let k be a divisor of $q-1$. We propose a construction of an almost-polyphase sequence set of size $k-1$ and of period $q-1$ using a k-ary Sidelnikov sequence of period $q-1$. we prove that the out-of-phase autocorrelation magnitude of the sequences in the set is upper-bounded by 2 and the crosscorrelation magnitude is upper bounded by $\sqrt{q}+1$.

Ⅰ. 서 론

CDMA에서 서명수열은 좋은 자기 상관 특성과 상호 상관 특성을 가져야한다[1]. 대부분의 수열 연구는 작은 비동기 자기 상관 특성과 상호 상관 특성에 중점을 두었다.

$m-$수열은 이상적인 자기 상관을 갖는 잘 알려진 이진 수열이다[2]. 비이진 Power Residue 수열(PRS)와 Sidelnikov 수열은 처음에는 좋은 자기 상관 특성을 가졌다고 제안 되었으며[3], 이후에 좋은 상호 상관 특성을 갖는 수열군임이 밝혀졌다[4-11].

유사-다상 수열이란 0인 일부 포함된 다상 수열로[12] 1의 중근인 복소수들과 0으로 이루어진 비이진 수열이며 wateramarked DS-CDMA에 성공적으로 활용되었다[13-17]. 2019년, Shi와 그의 연구원들은 주기가 p인 PRS에 해당하는 복소 다상 수열에서 하나의 1을 0으로 교체함으로써 좋은 자기 상관을 갖는 유사-다상 수열 생성법을 제안했다[18].

본 논문에서는 비슷한 방법을 주기가 $q-1$인 k진 Sidelnikov 수열에 적용하였으며 그 결과 기존의

※ 이 논문은 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.2020R1A2C201196911).
◆ First Author : Yonsei University School of Electrical and Electronic Engineering, mhlee95@yonsei.ac.kr, 학생(석사과정), 학생회원
° Corresponding Author : Yonsei University School of Electrical and Electronic Engineering, hysong@yonsei.ac.kr, 정교수, 종신회원
* Yonsei University School of Electrical and Electronic Engineering, gs.kim@yonsei.ac.kr,학생(석박사과정), 학생회원
논문번호 : 202002-033-A-RN, Received February 24, 2020; Revised March 26, 2020; Accepted March 26, 2020

Sidelnikov 수열보다 상관 특성이 더 좋은 수열의 집합을 생성할 수 있었다. 본 논문은 q를 홀수인 소수의 거듭제곱, k를 $q-1$의 약수라 할 때, 주기가 $q-1$인 k진 Sidelnikov 수열 하나를 이용하여 주기가 $q-1$이고 크기가 $k-1$인 유사-다상 수열 집합의 생성법을 제안하며, 이 집단의 수열의 비동기 자기 상관의 절댓값이 2로, 상호 상관의 절댓값이 $\sqrt{q}+1$으로 제한됨을 증명했다.

본 논문의 구조는 다음과 같다. Ⅱ장에서 유사-다상 수열과 기본적인 개념들을 간단히 소개한 후, Ⅲ장에서 주요 결과를 제시하며, Ⅳ장에서 몇 가지 흥미로운 논의들과 추측들로 논문을 마친다.

Ⅱ. Sidelnikov 수열

본 논문에서 다음과 같은 표기들을 사용한다.

- p 는 홀수인 소수이다.
- 양의 정수 m에 대해 $q=p^m$는 홀수인 소수의 거듭 제곱이다.
- $\mathbb{F}_q$는 크기가 q인 유한체이다.
- μ는 $\mathbb{F}_q$의 원시근이다.
- k는 $q-1$의 약수이다.
- $\mathbb{Z}_k$는 mod k의 정수들의 집합이다.

정의 1[3] 양의 정수 k, f에 대해 $q=kf+1$이라 하고, μ를 $\mathbb{F}_q$의 원시근이라 할 때, 집합 D_0는 다음과 같다.

$$D_0=\{\mu^{kl} | l=0,1,\ldots,f-1\}$$

$i=0,1,\ldots,k-1$에 대해 $D_i=\mu^i D_0$이라 하면, 주기가 $q-1$인 k진 Sidelnikov 수열 $\mathbf{s}$는 다음과 정의한다.

$$s(n)=\begin{cases}0 & if \quad \mu^n+1=0,\\ i & if \quad \mu^n+1\in D_i.\end{cases}$$

정의 1에서 정의된 k진 Sidelnikov 수열 $\mathbf{s}$는 다상 수열이고 $\omega=e^{j\frac{2\pi}{k}}$를 1의 복소 원시 k제곱근이라 할 때, $\mathbf{s}$를 복소 다상 수열 $\mathbf{t}$로 변환할 수 있으며, n번째 위치는 다음과 같다.

$$t(n)=\omega^{s(n)}, \quad n=0,1,2,\ldots \tag{1}$$

$1\le c\le k-1$인 양의 정수 c를 k진 Sidelnikov 수열 $\mathbf{s}$에 곱할 수 있으며 이때 n번째 위치는 $c\cdot s(n)$이다. 이러한 복소 다상 수열은 $\mathbf{t}_c$라고 표기하며, n번째 위치는 다음과 같다.

$$t_c(n)=\omega^{c\cdot s(n)}, \quad n=0,1,2,\ldots \tag{2}$$

정의 1에서 정의된 주기가 $q-1$인 k진 Sidelnikov 수열 $\mathbf{s}$는 아래에서 정의된 Power Residue 함수 $g:\mathbb{F}_q\mapsto\mathbb{Z}_k$ 를 이용해 나타낼 수 있다.

정의 2 q, k, μ, D_i가 **정의 1**과 같이 주어졌을 때, Power Residue 함수 $g:\mathbb{F}_q\mapsto\mathbb{Z}_k$는 다음과 같이 정의된다.

$$g(x)=\begin{cases}0 & if \quad x=0,\\ i & if \quad x\in D_i.\end{cases}$$

이제 주기가 $q-1$인 k진 Sidelnikov 수열 $\mathbf{s}$는 다음과 같이 나타낼 수 있다.

$$s(n)=g(\mu^n+1), \quad n=0,1,2,\ldots$$

μ의 위수가 $q-1$이므로, $\mu^{\frac{q-1}{2}}=-1$이다. 그러므로,

$$s\left(\frac{q-1}{2}\right)=g(0)=0$$

이고 따라서,

$$t\left(\frac{q-1}{2}\right)=\omega^0=1 \tag{3}$$

다음은 Sidelnikov 수열 $\mathbf{s}$의 잘 알려진 성질들이다.

따름정리 1(Sidelnikov 수열들의 상관[4]) 정의 1에서 정의된 주기가 $q-1$인 k진 Sidelnikov 수열을

$\mathbf{s}$, (2)에서 주어진 복수 다상 수열 $\mathbf{t}_c$라 할 때, 다음과 같은 성질들을 갖는다.

임의의 $\tau \neq 0$과 $1 \leq c \leq k-1$인 양의 정수 c에 대해 $\mathbf{t}_c$의 비동기 자기 상관은 다음과 같다.

$$\begin{aligned} R_{\mathbf{t}_c}(\tau) &= \sum_{x=0}^{q-2} t_c(x+\tau) t_c(x)^* \\ &= -\omega^{c \cdot g(\mu^\tau)} - 1 + \omega^{c \cdot g(-\mu^\tau+1)} \\ &\quad + \omega^{-c \cdot g(-\mu^{-\tau}+1)} \end{aligned}$$

따라서,

$$\left| R_{\mathbf{t}_c}(\tau) \right| \leq 4.$$

정수 a, b가 $1 \leq a \neq b \leq k-1$일 때, $\mathbf{t}_a$와 $\mathbf{t}_b$의 상호 상관은 다음과 같다.

$\tau = 0$일 때,

$$C_{\mathbf{t}_a, \mathbf{t}_b}(0) = 0$$

$\tau \neq 0$일 때,

$$\begin{aligned} C_{\mathbf{t}_a, \mathbf{t}_b}(\tau) &= \omega^{a \cdot g(-\mu^\tau+1)} + \omega^{b \cdot g(-\mu^{-\tau}+1)} \\ &+ \sum_{x \in \mathbb{F}_q \setminus \{0, -1, -\mu^{-\tau}\}} \omega^{a \cdot g(\mu^\tau x+1) - b \cdot g(x+1)} \end{aligned}$$

따라서,

$$\left| C_{\mathbf{t}_a, \mathbf{t}_b}(\tau) \right| \leq \sqrt{q} + 3.$$

Ⅲ. 주요 결과

본 논문이 제안하는 하나의 주기 $q-1$인 k진 Sidelnikov 수열을 이용해 생성한 유사-다상 수열은 다음과 같다.

정의 3 정의 1에서 정의된 주기가 $q-1$인 k진 Sidelnikov 수열을 $\mathbf{s}$, $\omega = e^{j\frac{2\pi}{k}}$라 하자.

유사-다상 수열 $\mathbf{t}^+$는 다음과 같이 정의된다.

$$t^+(n) = \begin{cases} 0 & if \quad n = \dfrac{q-1}{2}, \\ \omega^{s(n)} & otherwise. \end{cases}$$

양의 정수 c가 $1 \leq c \leq k-1$일 때, 유사-다상 수열 $\mathbf{t}_c^+$는 다음과 같이 정의된다.

$$t_c^+(n) = \begin{cases} 0 & if \quad n = \dfrac{q-1}{2}, \\ \omega^{c \cdot s(n)} & otherwise. \end{cases}$$

크기가 $k-1$인 유사-다상 수열 집단 T는 다음과 같이 정의된다.

$$T = \left\{ \mathbf{t}_c^+ \mid c = 1, 2, \ldots, k-1 \right\}.$$

정리 1 $\mathbf{t}_c^+$를 정의 3에서 정의된 유사-다상 수열이라고 할 때, $\mathbf{t}_c^+$의 비동기 자기 상관의 절댓값의 최댓값은 2이다.

$$\left| R_{\mathbf{t}_c^+}(\tau) \right| \leq 2.$$

증명) $\tau \neq 0$이라 가정하면

$$\begin{aligned} R_{\mathbf{t}_c^+}(\tau) &= \sum_{x=0}^{q-2} t_c^+(x+\tau) t_c^+(x)^* \\ &= R_{\mathbf{t}_c}(\tau) - t_c\left(\frac{q-1}{2} + \tau\right) t_c\left(\frac{q-1}{2}\right)^* \\ &\quad - t_c\left(\frac{q-1}{2}\right) t_c\left(\frac{q-1}{2} - \tau\right)^*. \end{aligned}$$

(3)에 의해서 $\mu^{\frac{q-1}{2}} = -1$이고 모든 c에 대해 $t_c\left(\dfrac{q-1}{2}\right) = 1$이다. 따름정리 1-(i)를 사용하면

$$\begin{aligned} R_{\mathbf{t}_c^+}(\tau) &= R_{\mathbf{t}_c}(\tau) - \omega^{c \cdot g(-\mu^\tau+1)} - \omega^{-c \cdot g(-\mu^{-\tau}+1)} \\ &= -\omega^{c \cdot g(\mu^\tau)} - 1. \end{aligned}$$

그러므로,

$$\left| R_{\mathbf{t}_c^+}(\tau) \right| \le 2. \qquad \blacksquare$$

정리 2 T를 정의 3에서 정의된 크기가 $k-1$인 유사-다상 수열 집합이라고 하자. 양의 정수 a, b가 $1 \le a \ne b \le k-1$일 때, T 안에 있는 임의의 유사-다상 수열 $\mathbf{t}_a^+$, $\mathbf{t}_b^+$의 상호 상관의 절댓값의 최댓값은 $\sqrt{q}+1$이다.

$$\left| C_{\mathbf{t}_a^+, \mathbf{t}_b^+}(\tau) \right| \le \sqrt{q}+1.$$

증명) $\tau = 0$이라 가정하면

$$C_{\mathbf{t}_a^+, \mathbf{t}_b^+}(0) = C_{\mathbf{t}_a, \mathbf{t}_b}(0) - t_a\left(\frac{q-1}{2}\right) t_b\left(\frac{q-1}{2}\right)^* = -1.$$

$\tau \ne 0$이라 가정하면

$$C_{\mathbf{t}_a^+, \mathbf{t}_b^+}(\tau) = C_{\mathbf{t}_a, \mathbf{t}_b}(\tau) - t_a\left(\frac{q-1}{2}+\tau\right) t_b\left(\frac{q-1}{2}\right)^* - t_a\left(\frac{q-1}{2}\right) t_b\left(\frac{q-1}{2}-\tau\right)^*$$

(3)에 의해서 $\mu^{\frac{q-1}{2}} = -1$이고 모든 c에 대해 $t_c\left(\frac{q-1}{2}\right) = 1$이다. 따름정리 1-(ii)를 사용하면

$$\begin{aligned} C_{\mathbf{t}_a^+, \mathbf{t}_b^+}(\tau) &= C_{\mathbf{t}_a, \mathbf{t}_b}(\tau) - \omega^{a \cdot g(-\mu^{\tau}+1)} - \omega^{b \cdot g(-\mu^{-\tau}+1)} \\ &= \sum_{x \in \mathbf{F}_q \setminus \{0, -1, -\mu^{-\tau}\}} \omega^{a \cdot g(\mu^{\tau} x+1) - b \cdot g(x+1)} \end{aligned} \tag{4}$$

따름정리 1에 의해 (4)의 절댓값의 최댓값은 $\sqrt{q}+1$이므로,

$$\left| C_{\mathbf{t}_a^+, \mathbf{t}_b^+}(\tau) \right| \le \sqrt{q}+1. \qquad \blacksquare$$

Ⅳ. 결론과 논의

본 논문은 다상 수열인 k진 Sidelnikov 수열에 해당하는 복소 다상 수열 $\mathbf{t}_c$에서 한 개의 1을 0으로 대체함으로써 생성할 수 있는 크기가 $k-1$이고 주기가 $q-1$인 유사-다상 수열 집합의 생성법을 제안했다. T 안에 속한 수열들의 비동기 자기 상관의 절댓값의 최댓값은 2이고, 상호 상관의 절댓값의 최댓값은 $\sqrt{q}+1$로 기존의 상관 특성[4]보다 더 좋아짐을 확인하였으며, 정리1 과 정리2의 증명을 통해 이를 증명하였다.

저자는 길이가 $q-1$인 k진 Sidelnikov 수열에서 어떤 1의 위치를 n_1이라할 때, n_1 위치에 있는 한 개의 1을 0으로 교체함으로써 상관 특성을 좋게 하는 방법이 $\mathbf{t}_c$의 다른 1이 위치한 자리에서도 적용될 것이라고 추측했다. 그러나 이러한 현상은 일반적이지 않았으며, 몇몇 수열들의 경우 0으로 교체함으로써 상관 특성을 좋게 하는 특정 자리는 오직 하나만 존재했다.

예를 들어, $q-1 = 3^6 - 1 = 728 = 28 \times 26$이고 $k = 28$, ω를 1의 복소 28제곱근이라 하면, $\mathbf{s}$는 28진 Sidelnikov 수열이고 이에 해당하는 복소 다상 수열을 $\mathbf{t}$이라 하면, $t(n) = \omega^{s(n)}$이다. 이때 n_1에 위치한 1을 0으로 바꾼 후 비동기 자기 상관의 절댓값의 최댓값을 구하여 표1과 같이 정리했다. 표 1이 나타낸 바와 같이 비동기 자기 상관 특성이 좋아지는 자리는 $n_1 = (q-1)/2 = 364$로, 단 하나만 존재했으며 이는 정의 3에서 제안된 수열 $\mathbf{t}^+$이다.

이러한 현상은 다른 모든 k진 Sidelnikov 수열들에

표 1. n_1번째 위치에 있는 하나의 1을 0으로 교체했을 때의 상관의 최댓값
Table 1. Max. Correlation when a single 1 on n_1-th position is replaced with 0

n_1	Max Autocorr.	n_1	Max Autocorr.
0	5.950	**364**	**2.000**
28	5.177	392	5.441
56	5.569	420	5.493
84	5.509	448	5.435
112	5.531	476	5.653
140	5.817	504	5.769
168	5.200	532	5.638
196	5.638	560	5.200
224	5.769	588	5.817
252	5.653	616	5.531
280	5.435	644	5.509
308	5.493	672	5.569
336	5.441	700	5.177

서도 나타날 것으로 추측하며, 추후 연구를 통해 밝혀낼 계획이다.

References

[1] P. Z. Fan and M. Darnell, *Sequence design for communications applications,* Exter: John Wiley & Sons Inc., 1996.

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

[3] V. M. Sidelnikov, "Some k-valued pseudo-random sequences and nearly equidistance codes," *Problemy Peredachi Informatsil*, vol. 5, no. 1, pp. 16-22, 1969.

[4] Y.-J. Kim and H.-Y. Song, "Cross correlation of Sidel'nikov sequences and their constant multiples," *IEEE Trans. Inf. Theory*, vol. 53, no. 3, pp. 1220-1224, Mar. 2007.

[5] Y.-S. Kim, J.-S. Chung, J.-S. No, and H. Chung, "New families of M-ary sequences with low correlation constructed from Sidelnikov sequences," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3768-3774, Aug. 2008.

[6] N. Y. Yu and G. Gong, "New construction of M-ary sequence families with low correlation from the structure of Sidelnikov sequences," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 4061-4070, Aug. 2010.

[7] Y.-T. Kim, D. S. Kim, and H.-Y. Song, "New M-ary sequence families with low correlation from the array structure of Sidelnikov sequences," *IEEE Tans. Inf. Theory,* vol. 61, no. 1, pp. 655-670, Jan. 2015.

[8] N. Y. Yu and G. Gong, "Multiplicative characters, the Weil bound, and polyphase sequence families with low correlation," *IEEE Trans. Inf. Theory*, vol. 56, no. 12, pp. 6376-6387, Dec. 2010.

[9] J. H. Kim, S. Y. Kim, M. K. Song, H.-Y. Song, and J. Y. Lee, "A study on correlation properties of sequences from the array structure of Sidelnikov sequences," in *Proc. KICS Symp.*, pp. 446-447, Nov. 2016.

[10] J.-W. Jang, Y.-S. Kim, J.-S. No, and T. Helleseth, "New family of p-ary sequences with optimal correlation property and large linear span," *J. KICS,* vol. 28, no. 9C, pp. 835-842, Sep. 2003.

[11] M. K. Song and H.-Y. Song, "Correlation of column sequences from the arrays of Sidelnikov sequences of different periods," *IEICE Trans. Fundamentals of Electron., Commun. and Comput. Sci.*, vol. E102-A, no. 10, pp. 1333-1339, Oct. 2019.

[12] E I. Krengel, "Some constructions of almost-perfect, odd-perfect and perfect polyphase and almost-polyphase sequences," *SETA 2010*, Sep. 2010.

[13] H. D. Luke and H. D. Schotten, "Odd-perfect, almost binary correlation sequences," *IEEE Trans. Aerospace and Electron. Syst.*, vol. 31, no. 1, Jan. 1995.

[14] A. Ali, E. Ali, A. Habib, Nadim, T. Kusaka, and Y. Nogami, "PseudoRandom ternary sequence and its autocorrelation property over finite field," *Int. J. Comput. Netw. and Info. Secur.*, vol. 11, no. 9, Sep. 2017.

[15] M. K. Song and H-Y. Song, "A generalized Milewski construction for perfect sequences," *SETA 2018*, Oct. 2018.

[16] M. K. Song, G. Kim, and H-Y. Song, "Punctured bent function sequences for watermarked DS-CDMA," *IEEE Comm. Lett.*, vol. 23, no. 7, Jul. 2019.

[17] M. K. Song, H-Y. Song, and J. Y. Lee, "On the Insertion of a watermark in spreading codes," *IPNT 2018*, Nov. 2018.

[18] X. Shi, X. Zhu, X. Huang, and Q. Yue, "A family of M-Ary σ-Sequences with good autocorrelation," *IEEE Commun. Lett.*, vol. 23, no. 7, pp. 1132-1135, May 2019.

이 민 형 (Min Hyung Lee)

2018년 2월 : 연세대학교 전자전자공학부 학사

2018년 3월~현재 : 연세대학교 전자전자공학과 석사과정

<관심분야> 통신공학, 정보이론, 부호이론

[ORCID:0000-0002-0617-8008]

김 강 산 (Gangsan Kim)

2016년 2월 : 연세대학교 전자전자공학부 학사

2016년 3월~현재 : 연세대학교 전자전자공학과 석박사통합과정

<관심분야> 통신공학, 정보이론, 부호이론

[ORCID:0000-0002-3864-5379]

송 홍 엽 (Hong-Yeop Song)

1984년 2월 : 연세대학교 전자공학과 학사

1986년 5월 : University of Southern California Dept. of EE. System 석사

1991년 12월 : University of Southern California Dept. of EE. System 박사

1992년 1월~1993년 12월 : University of Southern California 박사 후 연구원

1994년 1월~1995년 8월 : Qualcomm, San Diego, Senior Engineer

1995년 9월~현재 : 연세대학교 전기전자공학과 전임교수

<관심분야> 통신공학, 정보이론, 부호이론

[ORCID:0000-0001-8764-9424]