Sidel'nikov 수열들 간의 관계

준회원 임 태 형*, 김 영 식**, 정 정 수**, 종신회원 노 종 선**

On the Relationship of Sidel'nikov Sequences

Tae-Hyung Lim*, Young-Sik Kim**, Jung-Soo Chung** ***Associate Members***,
Jong-Seon No** ***Lifelong Member***

요 약

이 논문에서는 서로 다른 원시원과 decimation을 통해서 생성한 M-진 Sidel'nikov 수열들 사이의 관계에 대해서 연구하였다. 이들의 자기상관 함수와 자기상관 분포가 유도되었으며 주어진 주기에 대해서 Sidel'nikov 수열들이 decimation과, 순회 shift, 그리고 상수 곱 하에서 동치라는 것을 증명하였다.

Key Words : Autocorrelation, autocorrelation distribution, decimation, M-ary Sidel'nikov sequences, primitive elements.

ABSTRACT

In this paper, the relationship among M-ary Sidel'nikov sequences generated by different primitive elements and decimation are studied. Their autocorrelation function and autocorrelation distribution are derived. It is proved that Sidel'nikov sequences for a given period are equivalent under the decimation, cyclic shift, and scalar multiplication of the sequence.

Ⅰ. 서 론

전송 표준으로 보통 M-진의 변조 방식을 사용하는 고속 데이터 통신의 수요가 증가하면서 좋은 오류 정정 능력을 갖는 M-진 부호와 좋은 상관 특성을 갖는 M-진 수열을 찾는 것이 점점 더 중요해지고 있다.

소수 p가 있고 p^n-1을 나누는 양의 정수 n과 M이 있다고 할 때, Sidel'nikov는 주기가 p^n-1인 M-진 수열을 만들었다. 이 수열의 자기상관 값의 크기는 4보다 작거나 같다[1].

이 논문에서는 서로 다른 원시원과 decimation을 통해서 생성한 M-진 Sidel'nikov 수열의 자기상관 분포, 다시 말해 자기상관 함수의 각각의 값들의 발생 회수를 유도하였고 M-진 Sidel'nikov 수열들 사이의 관계에 대해서 연구하였다. 또한 주어진 주기에 대해서 Sidel'nikov 수열들이 decimation과, 순회 shift, 그리고 상수 곱 하에서 동치라는 것을 증명하였다.

Ⅱ. 사전지식

$s(t)$가 주기가 N인 M-진 수열이고 ω_M이 1의 M차 복소근인 $\omega_M = e^{j2\pi/M}$라 하자. $s(t)$의 자기상관 함수는 다음과 같이 정의된다.

※ 본 연구는 교육인적자원부, 산업자원부, 노동부의 출연금으로 수행한 최우수실험실 지원사업과 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었습니다.

* 대구경북과학기술원 (THLim@dgist.org)
** 서울대학교 전기컴퓨터공학부 및 뉴미디어통신공동연구소 (kingsi, integer@ccl.snu.ac.kr, jsno@snu.ac.kr)

논문번호: KICS2006-05-223, 접수일자 : 2006년 5월 23일, 최종논문접수일자 : 2006년 6월 16일

$$R(\tau) = \sum_{t=0}^{N-1} \omega_M^{s(t)-s(t+\tau)}$$

여기서 $0 \le \tau \le N-1$이다. Sidel'nikov는 M-진 Sidel'nikov 수열을 다음과 같이 정의하였다 [1].

정의 1: p가 소수이고 α가 p^n개의 원소를 갖는 유한체 F_{p^n}의 원시원이라 하자. 그리고 $M|(p^n-1)$라 하자. 이제 $k=0,1,\cdots,M-1$ 에 대해서 S_k가 다음과 같이 정의되는 F_{p^n}의 서로 겹치지 않는 부분집합들이라 하자.

$$S_k = \{\alpha^{Mi+k}-1 \mid 0 \le i < \frac{p^n-1}{M}\}$$

그러면 주기 p^n-1인 Sidel'nikov 수열 $s_o(t)$는 다음과 같이 정의된다.

$$s_o(t) = \begin{cases} k, \text{ if } \alpha^t \in S_k, 0 \le k \le M-1 \\ k_0, \text{ if } t = \frac{p^n-1}{2} \end{cases}$$

여기서 k_0는 modulo N한 임의의 정수이다.

□

여기서 $\alpha^{(p^n-1)/2} = -1$, $\cup_{k=0}^{M-1} S_k = F_{p^n} \backslash \{-1\}$이고 $0 \in S_0$ 이다. $k_0 = 0$인 M-진 Sidel'nikov 수열이 균형성을 갖고 있다는 것은 자명하다.

M-진 Sidel'nikov 수열을 아래에서 정의된 지시함수와 F_{p^n} 곱셈의 character를 사용해서 나타낼 수 있다.

정의 2: 지시 함수는 다음과 같이 정의된다.

$$I(x) = \begin{cases} 1, \text{ if } x = 0 \\ 0, \text{ if } x \ne 0 \end{cases}$$

□

정의 3: F_{p^n}의 M차의 곱셈의 character는 다음과 같이 정의된다.

$$\psi_M(\alpha^t) = e^{j2\pi t/M}, \text{ if } \alpha^t \in F_{p^n}^*$$

$$\psi_M(0) = 0$$

여기서 α는 F_{p^n}에서의 원시원이고 $M|(p^n-1)$이고 $0 \le t \le p^n-2$이다.

□

그러면 M-진 Sidel'nikov 수열은 다음과 같이 나타낼 수 있다.

$$\omega_M^{s_o(t)} = \omega_M^{k_0} I(\alpha^t+1) + \psi_M(\alpha^t+1)$$

또한 우리는 M-진 Sidel'nikov 수열을 지시함수와 F_{p^n}에서의 index 함수로 나타낼 수 있다. Index 함수는 다음과 같이 정의된다.

정의 4: 만일 x가 F_{p^n}에서의 0이 아닌 원소라면

$$x = \alpha^i, \quad 0 \le i \le p^n-2$$

를 만족하는 유일한 정수 i를 원시원 α에 대한 x의 index라 부르고 $ind_\alpha x$로 나타낸다.

□

Index들은 로그와 비슷한 역할을 한다. 그러면 M-진 Sidel'nikov 수열은 다음과 같이 나타낼 수 있다.

$$s_o(t) = k_0 I(\alpha^t+1) + ind_\alpha(\alpha^t+1)\bar{I}(\alpha^t+1) \tag{1}$$

여기서 $\bar{I}(x) = 1 - I(x)$이다.

e가 $e > 1$인 정수이고 $p^n = ef+1$이라 하자. 그러면 원분수는 아래와 같이 정의된다.

정의 5: α가 F_{p^n}에서의 원시원이라 하자. F_{p^n}에서의 원분군(cyclotomic class) C_i, $0 \le i \le e-1$,는 다음과 같이 정의된다.

$$C_i = \{\alpha^{es+i} \mid s = 0,1,\cdots,f-1\}$$

여기서 서로 같을 수도 있는 고정된 양의 정수 u와 v에 대해서 원분수 $(u,v)_M$은 $1+z \in C_v$를 만족하는 $z \in C_u$인 원소의 개수와 같다.

□

원분수들 사이의 기본적인 관계들은 [2]와 [4]에서 찾을 수 있다.

Ⅲ. Sidel'nikov 수열의 성질

이 장에서는 Sidel'nikov 수열들 사이의 관계를 살펴볼 것이다. 먼저 원시원을 치환해서 다른 수열

을 생성했을 때와 decimation을 사용해서 다른 수열을 생성했을 경우를 살펴볼 것이다.

3.1 원시원의 치환과 Decimation

M-진 Sidel'nikov 수열에서 서로 다른 원시원으로 치환한다는 것은 정의 1에서 α를 $(c, p^n-1)=1$인 α^c로 치환하는 것을 의미한다.

먼저 $M|(p^n-1)$이고 $p^n-1=Mf$라 하자. 그러면 정의 1을 사용해서 Sidel'nikov 수열 $s_o(t)$를 생성할 수 있다. 만일 α를 α^c로 치환하면 S_k의 정의는 다음과 같이 바뀐다.

$$S_k' = \{\alpha^{cMi+ck}-1 \mid 0 \le i \le f-1\}$$

그리고 원시원 치환을 통해 생성된 M-진 Sidel'nikov 수열은 다음과 같이 주어진다.

$$s_c(t) = \begin{cases} k, & \text{if } \alpha^{ct} \in S_k',\ 0 \le k \le M-1 \\ k_0, & \text{if } ct = \dfrac{p^n-1}{2} \end{cases}$$

여기서 k_0은 modulo M인 어떤 정수이다. Sidel'nikov 수열의 정의로부터 $s_c(t)$ 역시 Sidel'nikov 수열이 된다. 그러나 $s_c(t)$는 본래의 수열 $s_0(t)$와는 다른 특성을 보여준다. 후에 이들 수열들 사이의 관계를 살펴볼 것이다.

그 다음으로 $s_d(t)$로 표현되는 decimation을 통해서 생성된 Sidel'nikov 수열을 살펴보자. 이 논문에서 우리는 $(d, p^n-1)=1$인 decimation factor d를 생각할 것이다. 이것은 S_k의 정의를 바꾸지는 않는다. 그러나 수열의 생성 방법은 다음과 같이 수정된다.

$$s_d(t) = \begin{cases} k, & \text{if } \alpha^{dt} \in S_k,\ 0 \le k \le M-1 \\ k_0, & \text{if } dt = \dfrac{p^n-1}{2} \end{cases}$$

여기서 k_0는 modulo M인 어떤 정수이다. $s_d(t)$의 정의는 Sidel'nikov 수열의 정의와는 다르다. 그래서 Sidel'nikov 수열로 볼 수 없다.

이제 원시원 치환과 decimation을 함께 했을 경우를 살펴보자. $s(t)$가 Sidel'nikov 수열 $s_o(t)$를 d로 decimation을 해 주고 α를 α^c로 치환해준 수열이라 하자. 그러면 수열 $s(t)$는 다음과 같이 나타낼 수 있다.

$$\omega_M^{s(t)} = \omega_M^{k_0} I(\alpha^{cdt}+1) + \psi_M^{c^{-1}}(\alpha^{cdt}+1) \quad (2)$$

3.2 자기상관 함수

이 장에서는 (2)에서 정의된 수열의 자기상환 함수를 살펴볼 것이다. character의 성질을 사용해서 자기상관 함수는 다음과 같은 정리로 유도될 수 있다.

정리 6: $s(t)$가 (2)에서 정의된 수열이라 하자. 그러면 $s(t)$의 자명하지 않은 (다시 말해, $\tau \not\equiv 0 \bmod p^n-1$인) 자기상관 함수는 다음과 같이 주어진다.

$$R(\tau) = \omega_M^{k_0}\overline{\psi}_M^{c^{-1}}(1-\alpha^{cd\tau}) + \omega_M^{-k_0}\psi_M^{c^{-1}}(1-\alpha^{-cd\tau}) - \psi_M^{c^{-1}}(\alpha^{-cd\tau}) - 1$$

증명) $s(t)$와 자기상관 함수의 정의로부터, $s(t)$의 자기상관 함수 $R(\tau)$는 다음과 같이 쓸 수 있다.

$$\begin{aligned} R(\tau) =& \sum_{t=0}^{p^n-2}[(\omega_M^{k_0}I(\alpha^{cdt}+1)+\psi_M^{c^{-1}}(\alpha^{cdt}+1)) \\ &\times(\omega_M^{-k_0}I(\alpha^{cd(t+\tau)}+1)+\overline{\psi}_M^{c^{-1}}(\alpha^{cd(t+\tau)}+1))] \\ =& \sum_{t=2}^{p^n-2}[I(\alpha^{cdt}+1)I(\alpha^{cd(t+\tau)}+1) \\ &+\omega_M^{k_0}I(\alpha^{cdt}+1)\overline{\psi}_M^{c^{-1}}(\alpha^{cd(t+\tau)}+1) \\ &+\psi_M^{c^{-1}}I(\alpha^{cdt}+1)\omega_M^{-k_0}I(\alpha^{cd(t+\tau)}+1) \\ &+\psi_M^{c^{-1}}(\alpha^{cdt}+1)\overline{\psi}_M^{c^{-1}}(\alpha^{cd(t+\tau)}+1)] \end{aligned}$$

분명히 $\tau \not\equiv 0 \bmod p^n-1$에 대해서 $I(\alpha^{cdt}+1) \times I(\alpha^{cd(t+\tau)}+1)=0$가 성립하므로 다음 식을 얻는다.

$$\sum_{t=0}^{p^n-2} I(\alpha^{cdt}+1)\overline{\psi}_M^{c^{-1}}(\alpha^{cd(t+\tau)}+1) = \overline{\psi}_M^{c^{-1}}(-\alpha^{cd\tau}+1)$$

$$\sum_{t=0}^{p^n-2} I(\alpha^{cd(t+\tau)}+1)\psi_M^{c^{-1}}(\alpha^{cdt}+1) = \psi_M^{c^{-1}}(-\alpha^{cd\tau}+1)$$

그래서 다음 식이 성립한다.

$$\begin{aligned} R(\tau) &= \omega_M^{k_0}\overline{\psi}_M^{c^{-1}}(-\alpha^{cd\tau}+1) \\ &+\omega_M^{-k_0}\psi_M^{c^{-1}}(-\alpha^{cd\tau}+1) \\ &+\sum_{t=0}^{N-1}\psi_M^{c^{-1}}(\alpha^{cdt}+1)\overline{\psi}_M^{c^{-1}}(\alpha^{cd(t+\tau)}+1) \end{aligned}$$

곱셈의 character의 성질을 사용하면 다음 식을 얻는다.

$$\begin{aligned} &\sum_{t=0}^{p^n-2}\psi_M^{c^{-1}}(\alpha^{cdt}+1)\overline{\psi}_M^{c^{-1}}(\alpha^{cd(t+\tau)}+1) \\ &= \sum_{t=0,t\neq c^{-1}d^{-1}(q-1)/2-\tau}^{p^n-2}\psi_M^{c^{-1}}\left(\frac{\alpha^{cdt}+1}{\alpha^{cd(t+\tau)}+1}\right) \end{aligned}$$

여기서 t가 $c^{-1}d^{-1}(q-1)/2-\tau$를 제외하고서 0부터 $N-1$까지 변할 때 $(\alpha^{cdt}+1)/(\alpha^{cd(t+\tau)}+1)$은 $F_q\backslash\{1,\alpha^{-cd\tau}\}$의 모든 원소를 갖게 된다. 그러면 다음 식을 얻는다.

$$\begin{aligned} &\sum_{t=0,t\neq c^{-1}d^{-1}(q-1)/2-\tau}^{p^n-2}\psi_M^{c^{-1}}\left(\frac{\alpha^{cdt}+1}{\alpha^{cd(t+\tau)}+1}\right) \\ &= \sum_{x\in F_q}\psi_M^{c^{-1}}(x)-\psi_M^{c^{-1}}(1)-\psi_M^{c^{-1}}(\alpha^{-cd\tau}) \\ &= -\psi_M^{c^{-1}}(\alpha^{-cd\tau})-\psi_M^{c^{-1}}(1) \end{aligned}$$

따라서 정리가 증명되었다.

□

위의 정리에 따르면 (2)에서 정의된 수열의 위상이 다를 때의 자기 상관 특성의 크기가 Sidel'nikov 수열에서처럼 4를 상한을 갖는다는 사실을 알 수 있다.

3.3 자기상관 분포

최근에, Kim, Chung, No, 그리고 Chung은 원분수를 사용해서 Sidel'nikov 수열의 자기 상관 분포를 표현하였다 [3]. 비슷한 방법으로 (2)와 같이 정의된 수열의 자기상관 분포를 유도할 수 있다. 이 논문에서 우리는 먼저 정리 6을 좀 더 유용한 형태로 수정할 것이다.

$F_{p^n}\backslash\{0,1\}$상의 원소를 $y=\alpha^{cd\tau}$로 나타내자. 앞으로 $R(cd\tau)$와 $R(y)$를 상호교환 가능한 표현으로 사용할 것이다.

$$\psi_M^{c^{-1}}(-1)\psi_M^{c^{-1}}\left(\frac{1}{y}\right)=\psi_M^{c^{-1}}\left(\frac{1}{1-y}\right)\psi_M^{c^{-1}}\left(\frac{y-1}{y}\right)$$

를 사용해서 정리 6을 다음과 같은 따름정리로 수정할 수 있다.

따름정리 7: 정리 6에서의 수열의 자기상관 함수는 다음과 같이 수정될 수 있다.

$\psi_M^{c^{-1}}(-1)=1$일 때

$$\begin{aligned} R_{u,v} &= -(\omega_M^{c^{-1}i+k_0}-1)(\omega_M^{c^{-1}j-k_0}-1) \\ &= -(\omega_M^{u}-1)(\omega_M^{v}-1) \end{aligned} \quad (3)$$

로 표현되고 $\psi_M^{c^{-1}}(-1)=-1$일 때 다음과 같이 표현된다.

$$\begin{aligned} R_{u,v} &= (\omega_M^{c^{-1}i+k_0}+1)(\omega_M^{c^{-1}j-k_0}+1)-2 \\ &= (\omega_M^{u}+1)(\omega_M^{v}+1)-2 \end{aligned} \quad (4)$$

여기서 $y\in F_{p^n}\backslash\{0,1\}$는 $\psi_M\left(\frac{1}{1-y}\right)$과 $\psi_M\left(\frac{y-1}{y}\right)$를 만족한다.

□

그 이후의 정리를 유도하기 위해서는 [3]에 있는 다음의 정의와 정리가 필요하다.

정의 8: [3] $A_{i,j}$를 다음과 같이 정의되는 집합 $S_{i,j}$의 크기로 정의한다.

$$\begin{aligned} S_{i,j}=\{y\in F_{p^n}\backslash\{0,1\}\mid \psi_M\left(\frac{1}{1-y}\right)=\omega_M^{i}, \\ \psi_M\left(\frac{y-1}{y}\right)=\omega_M^{j}\} \end{aligned}$$

여기서 $i,j\in\{0,1,2,\cdots,M-1\}$이다.

□

그러면 $A_{i,j}$는 다음의 정리에서처럼 차수가 M인 원분수의 형태로 표현할 수 있다.

정리 9: [3] $A_{i,j}$는 다음과 같이 표현된다.

$$A_{i,j}=(i+j,j)_M$$

□

정리 9를 사용해서 다음과 같이 자기상관 분포를 유도할 수가 있다.

정리 10: $N(R_{u,v})$가 $R(y)=R_{u,v}$를 만족하는 $y \in F_{p^n}\backslash\{0,1\}$의 개수라 하자. 그러면 (2)에서 정의된 수열의 위상이 다를 때의 자기상관 분포는 다음과 같이 주어진다.

만일

$\psi_M^{c^{-1}}(-1)=1$이면

1) $N(0)=\sum_{i=1}^{M-1}((ci,ci+ck_0)_M+(ci,ck_0)_M)$
$+(0,ck_0)_M$

2) $N(R_{k,k})=(2ck,ck+ck_0)_M$, for $1\le k\le M-1$

3) $N(R_{u,v})=(cu+cv,cv+ck_0)_M$
$+(cu+cv,cu+ck_0)_M$, for $1\le u<v\le M-1$

이고, 만일 $\psi_M^{c^{-1}}(-1)=-1$이면,

1) $N(-2)=\sum_{i=0,i\ne\frac{M}{2}}^{M-1}((\frac{cM}{2}+ci,ci+ck_0)_M$
$+(\frac{cM}{2}+ci,\frac{cM}{2}+ck_0)_M)+(0,\frac{cM}{2}+ck_0)_M$

2) $N(R_{k,k})=(2ck,ck+ck_0)_M$, for $0\le k\le M-1$ and $k\ne M/2$

3) $N(R_{u,v})=(cu+cv,cv+ck_0)_M$
$+(cu+cv,cu+ck_0)_M$, for $0\le u<v\le M-1$, $u\ne M/2$, $v\ne M/2$

가 된다.

증명) 만일 $\psi_M(-1)=1$이면

$$
\begin{aligned}
R_{u,v} &= -(\omega_M^{c^{-1}i+k_0}-1)(\omega_M^{c^{-1}j-k_0}-1) \\
&= -(\omega_M^{u}-1)(\omega_M^{v}-1)
\end{aligned}
$$

가 된다.

그래서 다음식이 성립한다.

$$
\begin{aligned}
N(0) &= \sum_{u=0}^{M-1}A_{cu,ck_0}+\sum_{v=0}^{M-1}A_{-ck_0,cv}-A_{-ck_0,ck_0} \\
&= \sum_{i=1}^{M-1}((ci,ci+k_0)_M+(ci,ck_0)_M) \\
&\quad +(0,ck_0)_M
\end{aligned}
$$

마찬가지로 다음 식이 성립한다.

$$
N(R_{k,k})=A_{ck-ck_0,ck+ck_0}=(2ck,ck+ck_0)_M
$$

그리고

$$
\begin{aligned}
N(R_{u,v}) &= A_{cu-ck_0,cv+ck_0}+A_{cv-ck_0,cu+ck_0} \\
&= (cu+cv,cv+ck_0)_M \\
&\quad +(cu+cv,cu+ck_0)_M
\end{aligned}
$$

와 같이 주어진다.

$\psi_M(-1)=-1$인 경우도 마찬가지로 증명할 수 있다.

□

위의 정리에 따르면 M-진 Sidel'nikov 수열의 자기상관 분포가 원시원을 바꾸면 변하지만 decimation을 통해서는 변하지 않는다는 것을 알 수 있다.

Ⅳ. M-진 Sidel'nikov 수열들 간의 관계

(2)에서 정의된 M-진 Sidel'nikov 수열에 대한 수정된 표현을 다음과 같이 얻을 수 있다.

$$
\begin{aligned}
s(t) &= k_0 I(\alpha^{cdt}+1) \\
&\quad + ind_{\alpha^c}(\alpha^{cdt}+1)\bar{I}(\alpha^{cdt}+1)
\end{aligned}
$$

이 장에서는 $s(t)$가 균형성을 갖는, 즉 $k_0=0$인 것으로 가정한다. 그러면 $s(t)$는 다음과 같이 나타낼 수 있다.

$$
s(t)=ind_{\alpha^c}(\alpha^{cdt}+1)\bar{I}(\alpha^{cdt}+1)
$$

이 표현을 사용해서 Sidel'nikov 수열들 사이의 동치 관계를 증명할 수 있다. 일반적으로 만일 $s_1(t)$가 decimation이나 순회 shift 또는 상수 곱을

통해서 수열 $s_2(t)$로부터 얻을 수 있다면 수열 $s_1(t)$과 $s_2(t)$는 동치라고 말한다. 그래서 수열이 원시원의 치환에 대해서 동치라는 것을 보이는 것으로 충분하다.

정리 11: $s(t)$가 (2)에서 정의된 수열이라 하고 $s_o(t)$가 (1)에서 정의된 수열이라 하자. 그러면 $s(t)=c^{-1}s_o(cdt)$는 원시원 치환에 대해서 동치이다.

증명) (2)에서 정의된 $s(t)$는 다음과 같이 나타낼 수 있다.

$$s(t)=ind_{\alpha^c}(\alpha^{cdt}+1)\bar{I}(\alpha^{cdt}+1)$$

그리고 (1)에서 정의된 $s_o(t)$는 다음과 같이 나타낼 수 있다.

$$s_o(t)=ind_{\alpha}(\alpha^{t}+1)\bar{I}(\alpha^{t}+1)$$

이제 cd로 $s_o(t)$를 decimation 하면 다음의 식을 얻는다.

$$s_o(cdt)=ind_{\alpha}(\alpha^{cdt}+1)\bar{I}(\alpha^{cdt}+1) \quad (5)$$

그리고 (5)에 c^{-1}을 곱하면 다음 식을 얻는다.

$$\begin{aligned} c^{-1}s_o(cdt) &= c^{-1}ind_{\alpha}(\alpha^{cdt}+1)\bar{I}(\alpha^{cdt}+1) \\ &= c^{-1}ind_{\alpha}(\alpha^{ind_{\alpha}(\alpha^{cdt}+1)})\bar{I}(\alpha^{cdt}+1) \\ &= c^{-1}ind_{\alpha^c}(\alpha^{cind_{\alpha}(\alpha^{cdt}+1)})\bar{I}(\alpha^{cdt}+1) \\ &= c^{-1}cind_{\alpha^c}(\alpha^{int_{\alpha}(\alpha^{cdt}+1)})\bar{I}(\alpha^{cdt}+1) \\ &= ind_{\alpha^c}(\alpha^{cdt}+1)\bar{I}(\alpha^{cdt}+1) \\ &= s(t) \end{aligned}$$

그러므로 Sidel'nikov 수열은 decimation, 순회 shift, 그리고 상수 곱에 대해서 동치이다.

□

위의 정리에서 원시원 α를 α^c로 치환하거나 d로 decimation을 하는 것은 수열에 상수 c^{-1}을 곱한 후에 cd로 decimation을 하는 것과 같다는 것을 알 수 있다.

참 고 문 헌

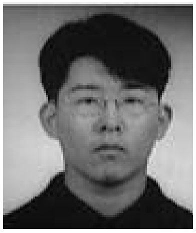
〔1〕 V. M. Sidel'nikov, "Some *k*-valued pseudo-random sequences and nearly equidistant codes," *Probl. Inf. Transm.*, vol. 5, no. 1, pp. 12-16, 1969.

〔2〕 B. C. Berndt, R. J. Evans, and K. S. Williams, Gauss and Jacobi Sums, vol. 21 of Canadian Mathematical Society Series of Monographs and Advanced Text. New York: Wily-Interscience, 1998.

〔3〕 Y.-S. Kim, J.-S. Chung, J.-S. No, and H. Chung, "On the autocorrelatio distributions of Sidel'nikov sequences," IEEE Trans. Inf. Theory, vol. 51, no. 9, pp. 3303-3307, sept. 2005.

〔4〕 T. Storer, *Cyclotomy and Difference Sets, Lectures in Advanced Mathematics*. Chicago, IL: Markham Publishing Company, 1967.

임 태 형 (Tae-Hyung Lim) 준회원



2004년 2월 서울대학교 전기공학부 공학사

2006년 2월 서울대학교 대학원 전기·컴퓨터공학부 공학석사

2006년 2월~현재 대구경북과학기술원 연구원

<관심분야> 시퀀스, 오류정정부호, 디지털통신

김 영 식 (Young-Sik Kim) 준회원

2001년 2월 서울대학교 전기공학부 공학사

2003년 2월 서울대학교 대학원 전기·컴퓨터공학부 공학석사

2003년 3월~현재 서울대학교 대학원 전기·컴퓨터공학부 박사과정

<관심분야> 시퀀스, 오류정정부호, 디지털통신

정 정 수 (Jung-Soo Chung) 준회원

2003년 2월 서울대학교 전기공학부 공학사
2003년 3월~현재 서울대학교 대학원 전기·컴퓨터공학부 석·박사 통합과정
<관심분야> 시퀀스, 오류정정부호, 디지털통신

노 종 선 (Jong-Seon No) 종신회원

1981년 2월 서울대학교 전자공학과 공학사
1984년 2월 서울대학교 대학원 전자공학과 공학석사
1988년 5월 University of Southern California, 전기공학과 공학박사
1988년 2월~1990년 7월 Hughes Network Systems, Senior MTS
1990년 9월~1999년 7월 건국대학교 전자공학과 부교수
1999년 8월~현재 서울대학교 전기·컴퓨터공학부 교수
<관심분야> 시퀀스, 오류정정부호, 시공간부호, 암호학, 이동통신